

An Introduction to Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0505: An Introduction to Sophos Central

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

An Introduction to Sophos Central

In this chapter you will learn what Sophos Central is and the protection it offers.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ There are no pre-requisites for this chapter

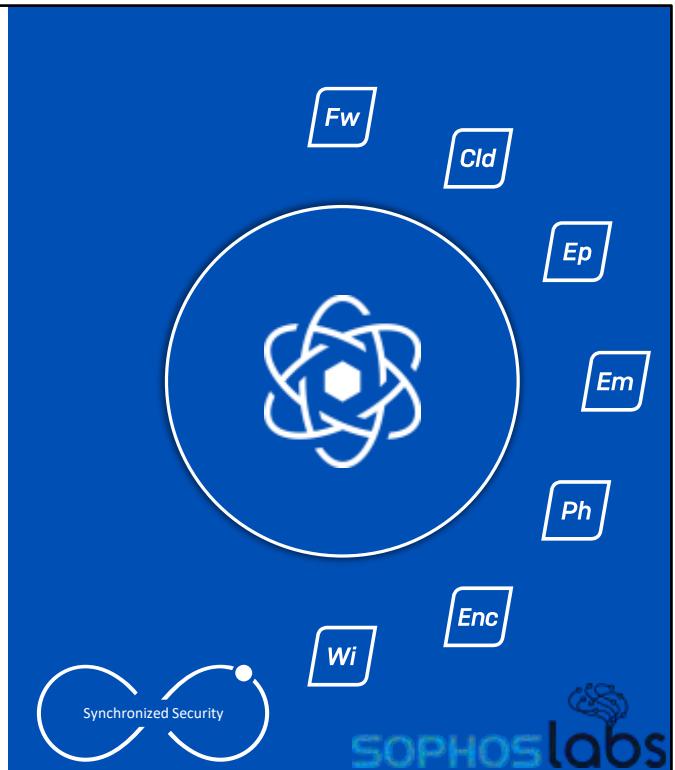
DURATION **5 minutes**

SOPHOS

In this chapter you will learn what Sophos Central is and the protection it offers.

What is Sophos Central?

- A unified cloud-based console used to manage Sophos Central products
- Provides world leading protection
- Reduces complexity of managing multiple protection solutions
- Use of anti-ransomware and anti-exploit technology
- Leverages Synchronized Security to simplify threat investigation and remediation
- Backed by SophosLabs



Sophos Central is a unified cloud-based console that is used to manage Sophos Central products providing world leading protection to keep you, your data, and your organization safe.

Sophos Central reduces the complexity of managing multiple protection solutions that are typically managed through multiple consoles.

It uses anti-ransomware and anti-exploit technology that stops advanced threats and leverages Synchronized Security to simplify threat investigation and remediation which minimizes the impact of threats.

All Sophos protection is backed up by SophosLabs, our global network of threat experts who ensure that you always have the best possible protection.

Web-Based Platform

The screenshot shows the Sophos Central web interface. On the left is a sidebar with navigation links for Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices (which is selected and highlighted in blue), Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for MP Products (Endpoint Protection, Server Protection, Mobile) and Sophos X (also with a 'More' link). The main content area is titled 'WinClient1' and shows the device summary for 'WinClient1'. It includes a device icon with a green checkmark, device details (Windows 10, IP: 172.16.10.70, Last User: administrator, Isolate), and buttons for 'Update now', 'Delete', 'Live Response', and 'More actions...'. At the top of the main content area are tabs for SUMMARY (selected), EVENTS, STATUS, and POLICIES. Below the tabs is a 'Recent Events' section listing five items with timestamps and descriptions. To the right of the main content area is a smartphone displaying the mobile version of the Sophos Central app. The bottom right corner of the main content area has the 'SOPHOS' logo.

Sophos Central is a web-based platform enabling the control and management of all Sophos products from anywhere, at any time. It is automatically updated so that the latest protection is always provided.

Supported Browsers



Google Chrome



Apple Safari (Mac only)



Mozilla FireFox



Microsoft Edge



Additional information in
the notes



As Sophos Central is web-based, we recommend that you are using a supported web browser. Sophos Central supports both the latest and previous versions of all major Internet browsers.

If an unsupported web browser is detected, you will be redirected to a page that lists the currently supported browsers so that you can upgrade.

[Additional Information]

You can view a list of currently supported web browsers here:

<https://docs.sophos.com/central/enterprise/help/en-us/SupportedBrowsers/index.html>



Additional information in
the notes

Sophos Security Framework

The screenshot shows the Sophos Central Security Framework help center. The left sidebar contains links to various security topics like Physical Security, Network Security, and Threat Protection. The main content area has sections for 'About this Help' and 'Want to know what's new?'. A large blue box on the right lists six security measures:

- Physical security
- Network security
- Data security
- Threat protection
- Compliance and external audits
- Customer controls
- Telemetry and data gathering

The Sophos Central security framework document provides a detailed look at Sophos Central.

It covers deployment, development, and maintenance. Additionally, it provides links to information pages providing full details on the data Sophos gathers and stores.

It also details the various measures Sophos takes to provide this secure platform.

[Additional Information]

The security framework document can be found at

<https://docs.sophos.com/central/Framework/security-framework/index.html>

Sophos Central Portals

Sophos ID

- Single Sign-On (SSO) mechanism
- MFA required for admins



Self Service Portal

- Allows users to customize security status and notifications



To access Sophos Central, you will require a Sophos ID. This ID is a single sign-on (SSO) mechanism. Your Sophos ID gives you access to the Sophos Central dashboard as well as other Sophos resources depending on your license. Sophos Central administrators must use multi-factor authentication to login.

The self-service portal (SSP) is available to all users. This allows users to customize their security status and notifications directly. The SSP allows users to enrol devices themselves and provides a console to view quarantined items, and manage device encryption, giving them greater control over their security and data.

Once a user has configured their password, they are able to login to the self-service portal. It is important to note that the self-service portal is only available to users once it has been configured in Sophos Central by an administrator.

Sophos Central Interfaces

Sophos Central Admin Dashboard



Enables IT managers to deploy and manage all their security through a single interface

Enterprise Dashboard (EDB)



Allows Enterprises to manage large, distributed estates

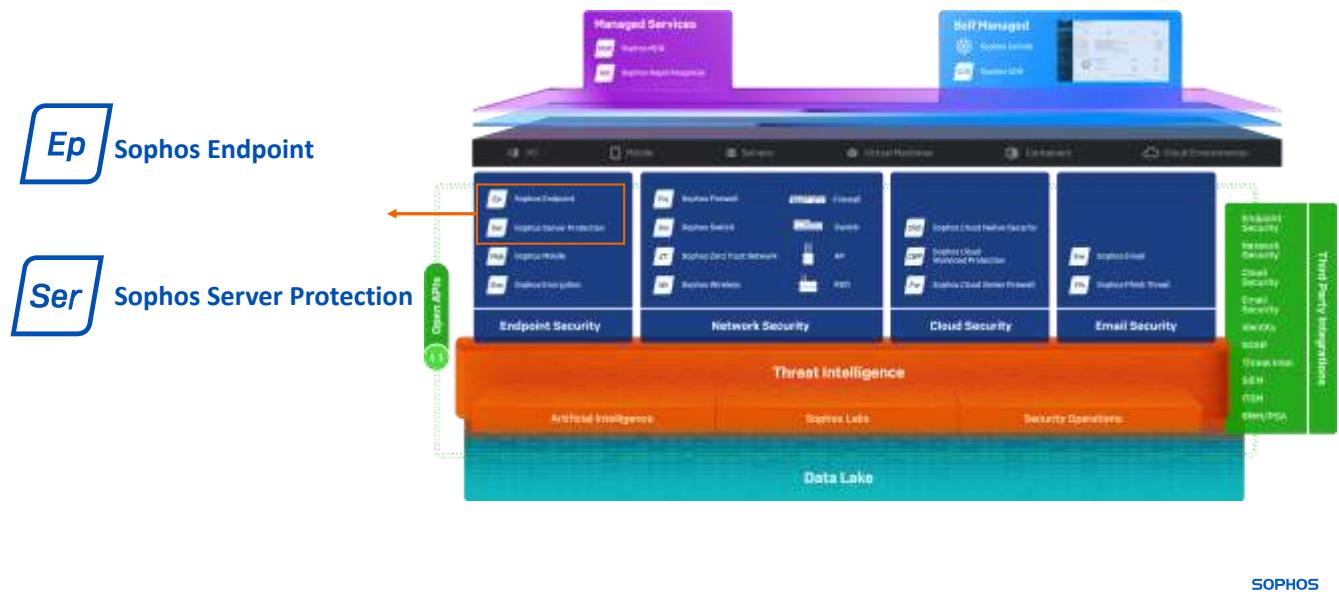
SOPHOS

There are two levels of access to Sophos Central.

Sophos Central Admin Dashboard. This is the administrator interface which is designed to help administrators deploy, manage, and secure an entire organization in one place. This is where an administrator can view multiple products, action alerts, and hunt for possible threats. A summary of the entire estate is displayed on the dashboard providing an overview of security.

The Enterprise Dashboard (EDB). This interface allows administrators to manage the security of large distributed organizations with multiple branches. Sub-estates can be configured with security rules applied to specific sub-estates. Licenses can be shared between sub-estates from one master pool of licenses.

Sophos Adaptive Cybersecurity Ecosystem



It is useful to understand the Sophos Adaptive Cybersecurity Ecosystem, which is shown here.

This course will focus on the Sophos Endpoint and Server Protection available in Sophos Central.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

This course will focus on which Sophos Central products?

Sophos Endpoint

Sophos Firewall

Network Protection

Email Protection

Server Protection

SOPHOS



Question 2 of 2

True or False: In a large distributed organization, specific security rules can be applied to sub-estates.

True

False

SOPHOS

Chapter Review

Sophos Central is a **unified cloud-based console** that is used to manage Sophos Central products.

Sophos Central protection uses **anti-ransomware** and **anti-exploit** technology that **stops advanced threats** and **leverages Synchronized Security** to simplify threat investigation and remediation which minimizes the impact of threats.

The **self-service portal (SSP)** is available to all users, it allows users to **respond to notifications** directly, **view quarantined items** and **protect devices**.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos Central is a unified cloud-based console that is used to manage Sophos Central products.

Sophos Central protection uses anti-ransomware and anti-exploit technology that stops advanced threats and leverages Synchronized Security to simplify threat investigation and remediation which minimizes the impact of threats.

The self-service portal is available to all users, it allows users to respond to notifications directly, view quarantined items, and protect devices.



Sophos Central Protection Overview

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0510: Sophos Central Protection Overview

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central Protection Overview

In this chapter you will learn how Sophos Central endpoint and server protection features work together to protect against cyber attacks.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Sophos Central is

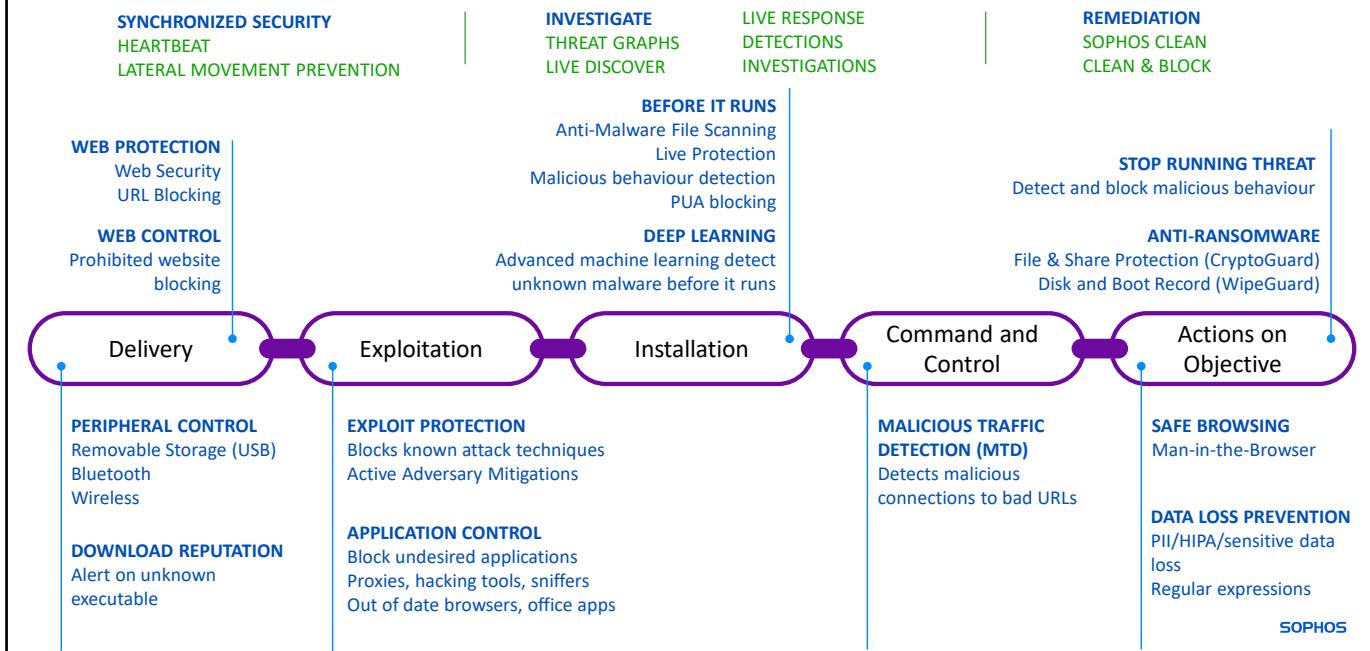
DURATION

18 minutes

SOPHOS

In this chapter you will learn how Sophos Central endpoint and server protection features work together to protect against cyber attacks.

Sophos Central Protection Overview

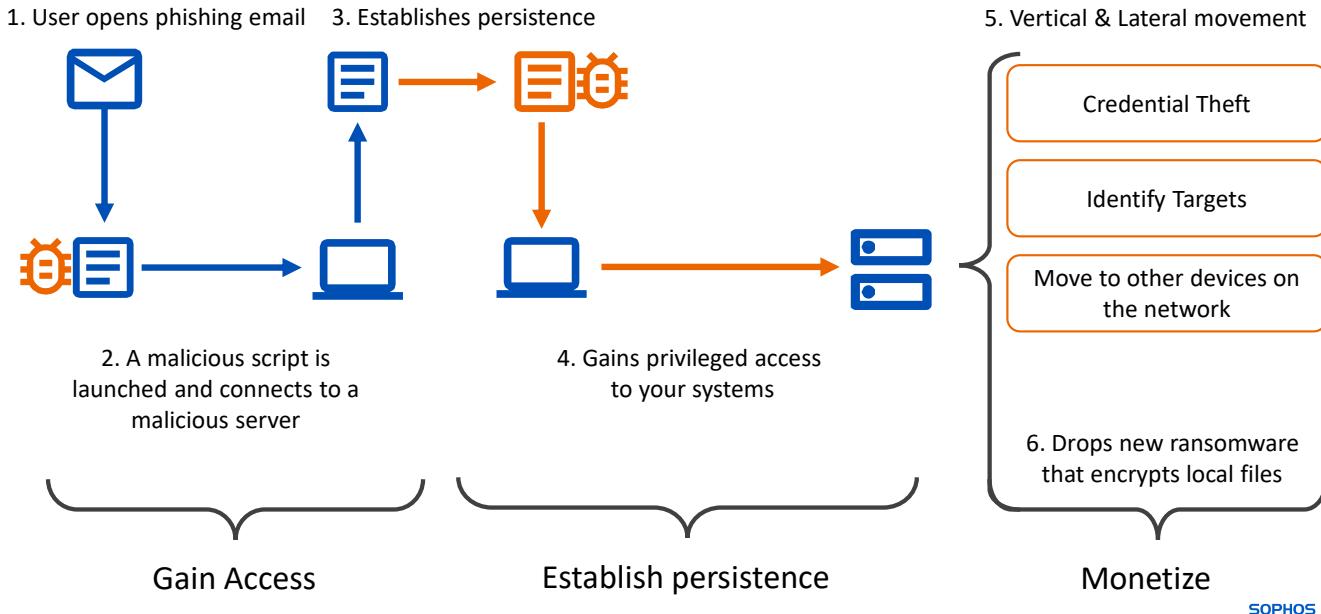


Sophos Central endpoint and server protection consists of multiple layers of protection. We will look at the protection features included by showing adversary tactics and techniques, highlighting how Sophos Central endpoint and server protection is able to prevent them.



Additional information in
the notes

Example Ransomware Attack



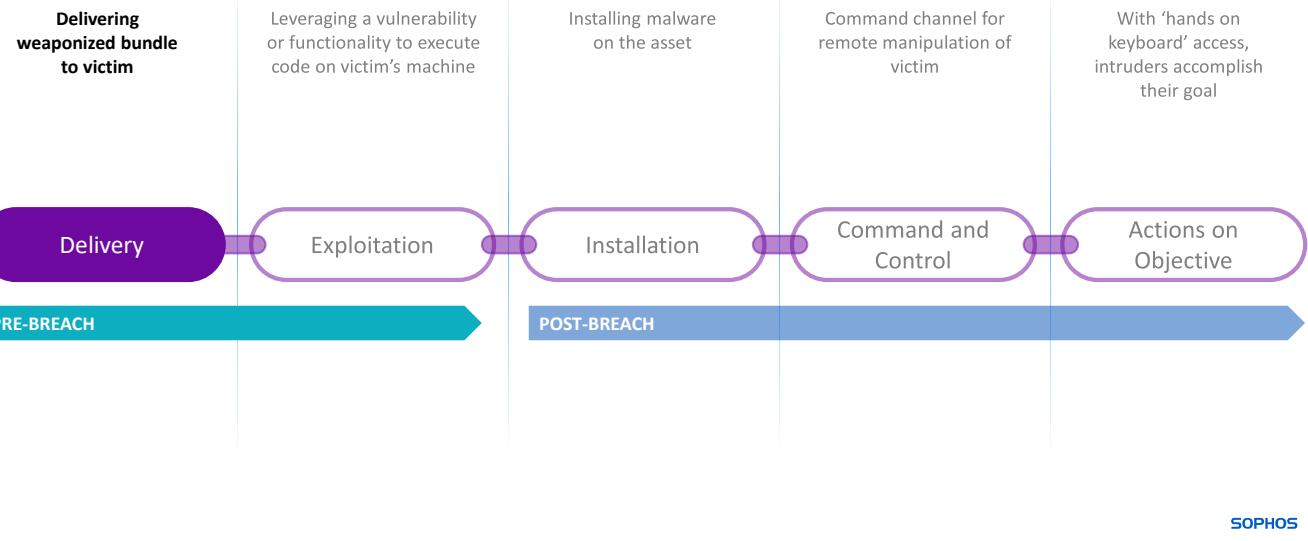
To demonstrate the multiple layers of threat protection offered, let's look at an example ransomware attack.

- A user opens a phishing email which links to a document
- The user opens the document which contains an embedded link to a unique malicious script. The malicious script is executed and communicates to a malicious server
- To establish persistence, the attacker compromises another application on the device that is in constant use. The user closes the document, however, the attacker has now gained access to internal systems
- With this access, the attacker can steal credentials and scan the network to identify targets for movement across the network
- Using the stolen credentials, the attacker moves to other devices on the network
- The attacker can now drop ransomware, encrypt files, and prevent the organization from functioning

[Additional Information]

The Ransomware Threat Intelligence Center provides a collection of Sophos threat research articles and security operations reports related to new or prevalent ransomware groups from 2018 to the present. <https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/>

Anatomy of Attack | Delivery



The first stage of an attack is the delivery of malicious content, for example a file, or a link. There are several techniques used by attackers to deliver malicious content.

Sophos endpoint and server protection provides you with the tools to control which websites users can access, the peripheral devices they can use and the data they can download.

Web Control and Protection

Web Protection

Protects against malicious websites based on URL and IP address reputation

Web Control

Control access to websites based on the website category

SOPHOS

Web protection is used to protect users whilst they are browsing the Internet. It scans the web stream and blocks malicious websites.

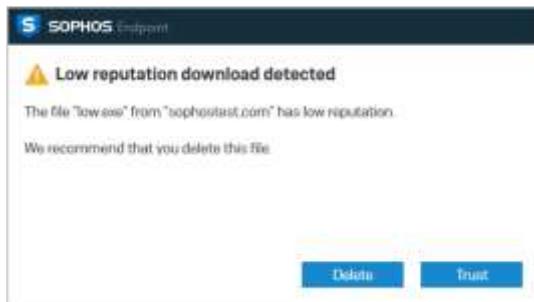
Administrators can also make use of the web control policy which helps to limit the security vulnerabilities introduced by malicious websites. Web control uses category based URL blocking and when configured, checks the category of websites being accessed. If the category of a website is restricted based on the Sophos Central web control policy, the website is blocked.

Download Reputation

Download reputation checks the reputation of files as they are downloaded

A file's reputation is determined by performing a file checksum lookup from the device against known files and their reputation created by SophosLabs

Download reputation is supported on Microsoft Edge, Google Chrome, and Opera



SOPHOS

Download reputation is part of the web protection feature and is enabled by default. It checks the reputation of files as they are downloaded from the Internet. If an unknown or low reputation file is selected for download, the user will be prompted to either delete or trust the file.

A file's reputation is determined by performing a file checksum lookup from the device against known files and their reputation created by SophosLabs. Download reputation is supported on Microsoft Edge, Google Chrome and Opera.

Peripheral Control

Monitor

Collect details of devices in use

Control access

Allow or block by category of device

Add exemptions

By model of device ID

Manage Peripherals - set your peripheral settings below

- Disable peripheral control
- Monitor but do not block (all peripherals will be allowed)
- Control access by peripheral type and add exemptions

The totals listed below include all peripherals detected, whether on endpoint computers or servers:

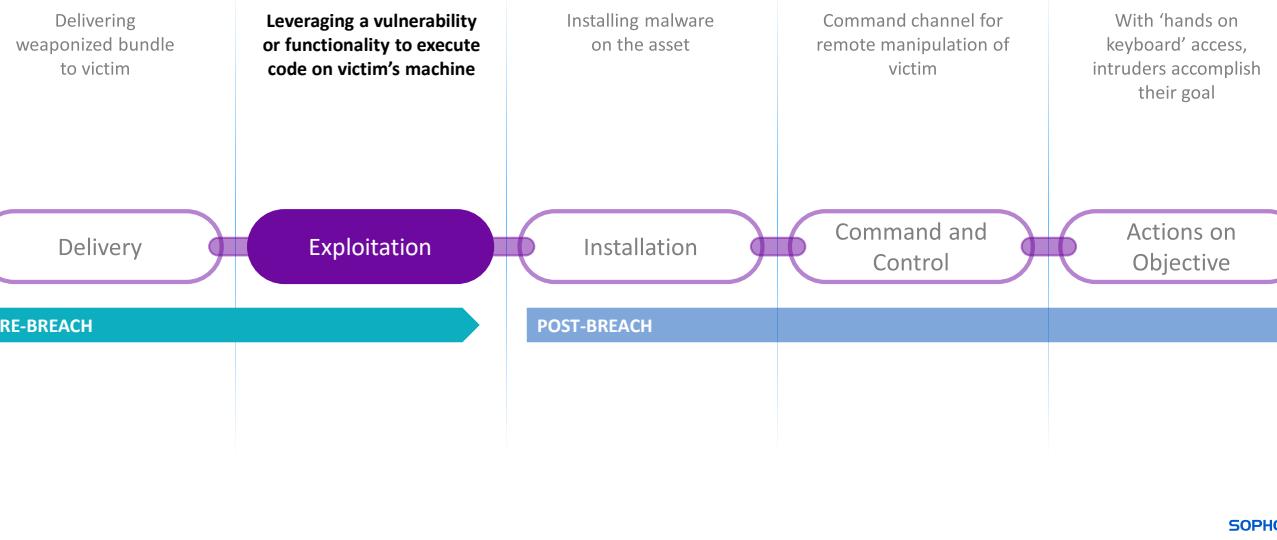
Allow	Bluetooth - 0 detected
Allow	Secure removable storage - 0 detected
Allow	Floppy drive - 0 detected
Allow	Infrared - 0 detected
Allow	Modem - 0 detected
Allow	Optical drive - 0 detected
Allow	Removable storage - 0 detected
Allow	Wireless - 0 detected
Allow	MTP/PTP - 0 detected

SOPHOS

Peripheral control restricts access to external devices such as USB drives. It can be used to prevent the use of untrusted devices that could contain malware. By default, the peripheral control policy is disabled in Sophos Central.

Any peripheral devices detected can be added as an exemption allowing the use of specific trusted devices. Each category of device can be configured to be allowed or blocked. Secure removable storage, floppy disk drives, and optical drives have the option of read-only, allowing users to view the peripheral device but not add or remove data from it.

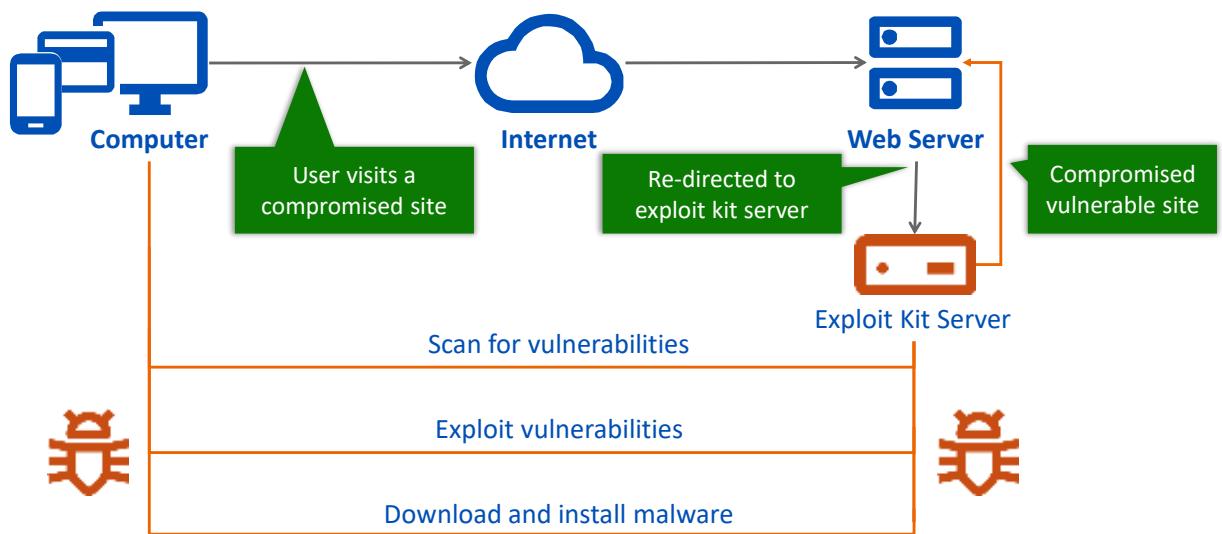
Anatomy of Attack | Exploitation



Once an attacker has gained access to your estate using a delivery technique, they will typically attempt to leverage a vulnerability to execute malicious code.

Attackers are looking to exploit devices; they are looking for a method or a tool that will abuse the vulnerabilities of any software in use. Although exploits can be complex, a cyber-criminal does not need to be skilled to develop them, they can use an exploit kit.

How Exploits Work

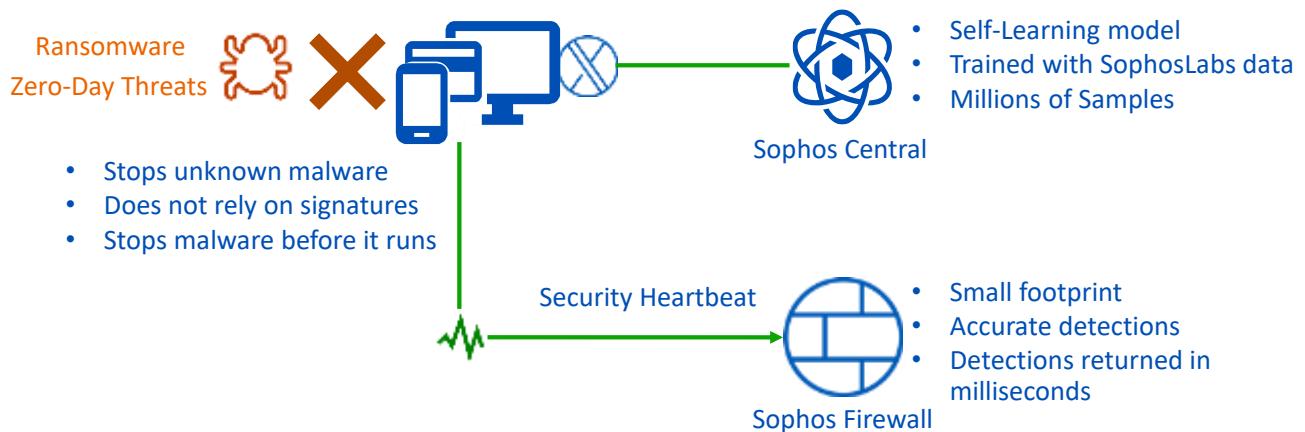


SOPHOS

Exploit kits come with pre-written code and target users running insecure and outdated software applications. In this diagram the user visits a website that has been compromised. As a result, the user is redirected, without their knowledge, to the exploit kit server.

An exploit kit is usually engineered to perform at least two core actions. To scan the system for vulnerabilities, and to exploit those vulnerabilities to download malicious code. Exploit kits can be used online with limited technical knowledge, sometimes kits even come with a user-friendly interface along with technical support!

How Sophos Protects Against Exploits



SOPHOS

Intercept X is used to protect against exploits. This technology protects devices against malicious threats that bypass traditional anti-virus solutions. Typically, these threats are zero-day and ransomware.

Intercept X focuses on identifying the techniques used to compromise a device rather than the threat itself. It denies attackers by blocking the exploits and techniques used to distribute malware, steal credentials, and escape detection. It uses three main methods:

- Exploit prevention blocks known attack techniques
- Machine learning recognizes similarities to known malicious files
- Anti-ransomware protection looks to detect and roll back the damage of a ransomware attack

Intercept X will report any detections to Sophos Central allowing administrators to remotely control all protected devices. If a Sophos Firewall is installed, and Synchronized Security has been enabled, administrators can also block any traffic passing through the firewall from a compromised device, protecting your entire network from the attack.

Application Control

Controlled applications

Select applications to be controlled

Detect applications

When users access them and during scanning

Application request

Request applications to be added by Sophos

SOPHOS

Application control can be used to prevent users from running applications that are considered unsuitable for business use. For example, games or instant messaging applications. It can also improve security by controlling the types of applications allowed, which reduces the attack surface preventing the exploitation of system tools.

The Application control policy can be used to detect applications in use and then to control the access to these applications. Applications that are not included in the application control policy can be requested.

Anatomy of Attack | Installation

Delivering weaponized bundle to victim
Leveraging a vulnerability or functionality to execute code on victim's machine
Installing malware on the asset
Command channel for remote manipulation of victim
With 'hands on keyboard' access, intruders accomplish their goal



The installation stage of an attack is when an attacker will download and install malicious content to run on a compromised device.

SOPHOS



Additional information in
the notes

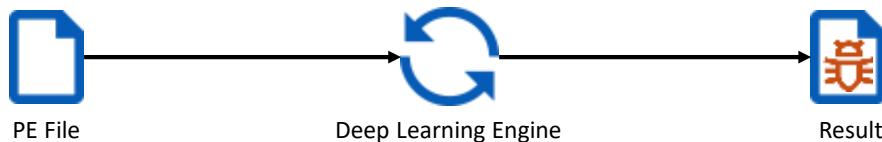
Deep Learning File Scanning

Deep Learning



Enable deep learning

Deep learning scanning is enabled by default
in the Threat Protection policy



SOPHOS

On-access and on-demand file scanning is used by Sophos Central endpoint and server protection. When a user interacts with a file on a protected device, that file is automatically scanned to determine if it is malicious.

If the file is determined to be malicious, it is automatically cleaned up on the device. Sophos uses three pieces of data to determine if a file is malicious or not.

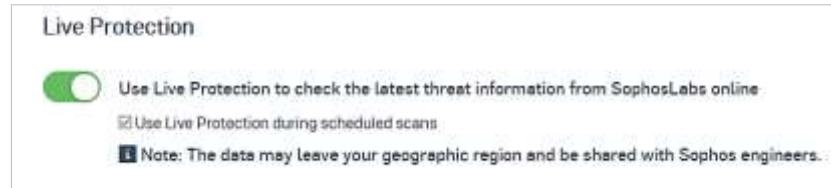
- The AppID which is the application identifier given to an app that sits within a category
- The machine learning score which is a scale between zero and one hundred. If a file has a ML score of over thirty, it will be considered malicious
- The file reputation score which is also scaled between zero and one hundred. Zero indicates a bad reputation, whereas one hundred indicates a clean file. Please note that a file will return a reputation score of one hundred if it has been excluded

[Additional Information]

For more information about the reputation scores for files please see knowledge base article **KB-000037118**. <https://support.sophos.com/support/s/article/KB-000037118>

Live Protection

- ✓ Sends file characteristics, such as checksum to Sophos for checking
- ✓ Performs instant in-the-cloud checking
- ✓ Returns a decision as clean or malicious



SOPHOS

Live protection provides an instant lookup against the very latest known malicious files. Live protection means that virus definition files do not have to be downloaded to a protected device for the latest protection to be in place.

Malicious Behaviour Detection

- ✓ Scans **inbound** and **outbound** network traffic
- ✓ Traffic is scanned and known attacks are recognized
- ✓ Blocks threats before they can infect the OS or an application



Detect malicious behavior



This setting applies to computers running the latest version of Core Agent

SOPHOS

Malicious behaviour detection scans inbound and outbound network traffic for malicious attacks or suspicious behaviour patterns. If an attack is detected for outbound traffic, it is likely that a device is being used to attack other devices on the network.

Inbound traffic is communication coming from a remote device to a device within a network.

Outbound traffic is communication from a network device to a remote device.

Potentially Unwanted Application (PUA) Blocking

PUA

Not malicious but unsuitable for business networks

PUA detection

Enabled by default

Blocked and an event is logged

Scanning exclusions

Applications can be excluded globally or in specific policies

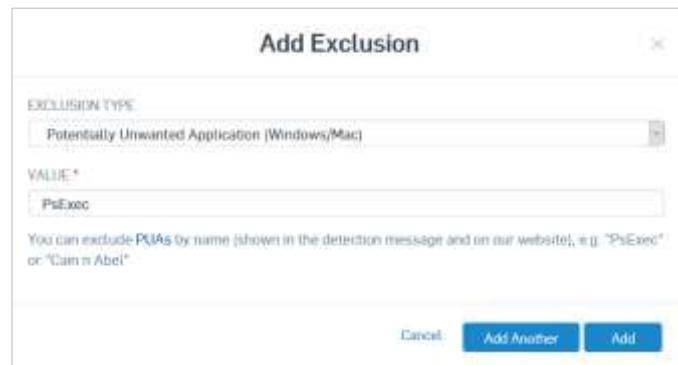
Add Exclusion

EXCLUSION TYPE: Potentially Unwanted Application (Windows/Mac)

VALUE*: PsExec

You can exclude PUAs by name (shown in the detection message and on our website), e.g. "PsExec" or "Cain n Abel"

Cancel Add Another Add

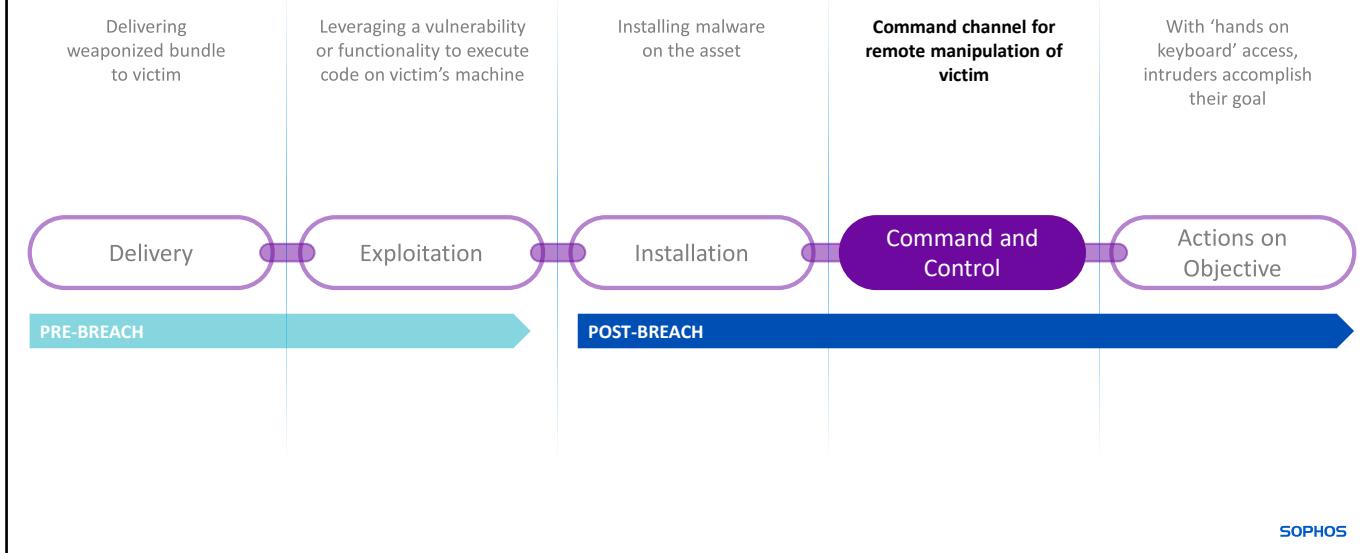


SOPHOS

Potentially unwanted applications, or PUAs, is a term used to describe applications that are generally considered unsuitable for business use. The major PUA classifications are adware, non-malicious spyware, remote administration tools, and hacking tools. Please note that certain applications that are categorized as a PUA may be considered useful by some users.

PUA scanning is enabled by default, any detected applications will be blocked and an event logged in Sophos Central. An administrator can configure either global or policy exceptions for applications where required.

Anatomy of Attack | Command and Control



Once an attacker has gained control of a compromised device, they can establish contact with a command and control server. This server is typically used to send commands that will upload or download malicious code or files.

In a typical scenario, the command and control server communication is a repeated process which allows malware to adapt as more knowledge is collected. Complex malware includes communication to remote servers for further instructions.



Additional information in
the notes

Malicious Traffic Detection (MTD)



Protect network traffic

- Detect malicious connections to command and control servers
- Prevent malicious network traffic with packet inspection (IPS)

This setting applies to computers running the latest version of Core Agent

Malicious traffic detection is enabled by default in the threat protection policy

- Monitors **non-browser** outbound network traffic
- Detects processes which attempt to connect out to known malware sites
- Reports traffic to trigger memory scans
- If this results in a HP/Mal detection, then the threat will be cleaned up

SOPHOS

To detect and prevent the communication from protected devices to suspicious or malicious servers, we use malicious traffic detection. MTD monitors HTTP non-browser application traffic for signs of connectivity to known bad URLs. If the traffic is detected, it is an early indicator that malware may be present on a device.

A command and control server connection is very dangerous as an attacker can use that connection to register devices as part of a botnet which allows them to be used to attack more devices across a network. If a command detection is triggered, a detection signature may not have been created. Sophos can use the detection to collect samples which are submitted to SophosLabs. A specific detection for that traffic is then created.

Malicious traffic detection can also make use of packet inspection (IPS) to scan inbound and outbound network traffic for known attacks. If an attack is detected, it is blocked, which protects against lateral movement as well as external attacks.

[Additional Information]

Sophos provides a test script for malicious traffic detection that can be downloaded from knowledge base article **KB-000035314**. <https://support.sophos.com/support/s/article/KB-000035314>

Anatomy of Attack | Actions on Objective

Delivering weaponized bundle to victim
Leveraging a vulnerability or functionality to execute code on victim's machine
Installing malware on the asset
Command channel for remote manipulation of victim

With 'hands on keyboard' access, intruders accomplish their goal



PRE-BREACH

POST-BREACH

Actions on Objective

SOPHOS

Should an attacker get this far into an attack, they will perform the malicious action they intended to.

This action will depend on the type of malware. For example, a ransomware attack aims to encrypt data whereas spyware tends to log keystrokes to gain access to intellectual property.

Ransomware Behaviour Protection



WipeGuard – Disk & Boot Protection

- Prevents malicious tampering with system areas of disk
- Stops malicious processes
- Proven effective during NotPetya

CryptoGuard – File Protection

- Takes just in time file cache
- Identifies malicious file encryption behavior
- Isolates malicious process
- Automatically rolls back affected files

SOPHOS

Intercept X stops ransomware by intercepting the behaviour. It prevents common file encryption as well as less common ransomware that impacts the disk and master boot record. These attacks are intentionally destructive and can wipe a device.

WipeGuard prevents attacks that target the master boot record and prevents bootkit installation. A bootkit is a variant of a rootkit that infects a device's startup code and can be used to attack full disk encrypted systems.

CryptoGuard protects against remotely run ransomware and file encryption. It does so by monitoring specific file types in specific locations looking for actions that indicate ransomware. One action could be a process that opens and writes to multiple files in a short period of time.

Safe Browsing

Browser exploits are when an attacker targets a vulnerability in either the browser or in an application that the browser calls to process a web request such as Flash Player, Java or Silverlight.

Safe browsing protects against these types of exploits and is enabled by default in the threat protection policy



Protect critical functions in web browsers (Safe Browsing)



- For example, man-in-the-browser (MitB) which infects a web browser by exploiting browser security vulnerabilities
- This allows an attacker to modify web pages, modify transaction content or insert additional transactions



- Safe browsing monitors the crypto, network and presentation DLLs of a browser to detect when another application is interfering.
- Safe browsing only warns the user that the browser compromise was detected.
- The browser session is not terminated but the administrator is provided with event information.

SOPHOS

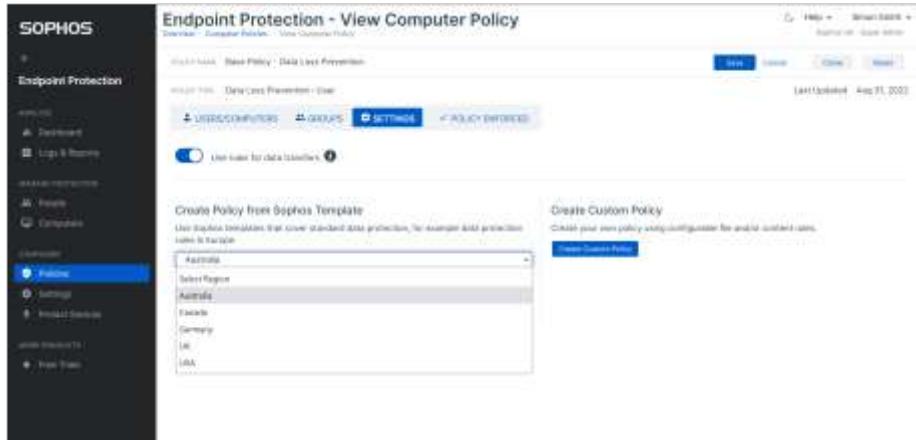
Browser exploits are a class of threat where the attack targets a vulnerability in either the browser or in an application that the browser calls to process a web request, such as Flash Player or Java.

An example of this is a man-in-the-browser attack. A form of Internet threat that infects an Internet browser by taking advantage of vulnerabilities in the browser security. This allows an attacker to modify web pages, transaction content, or insert additional transactions.

Safe Browsing monitors the crypto, network, and presentation DLLs of Internet browsers to detect when another application is interfering. Safe Browsing only warns a user that a browser compromise was detected. It will initiate a scan but will not terminate the browser sessions. The user is alerted that the browser session is potentially compromised, and the administrator is provided with event information to support investigation.

Data Loss Prevention (DLP)

- ✓ Control accidental data loss
- ✓ Monitor and restrict the transfer of sensitive data files
- ✓ Prevent users sending data using common file sharing applications

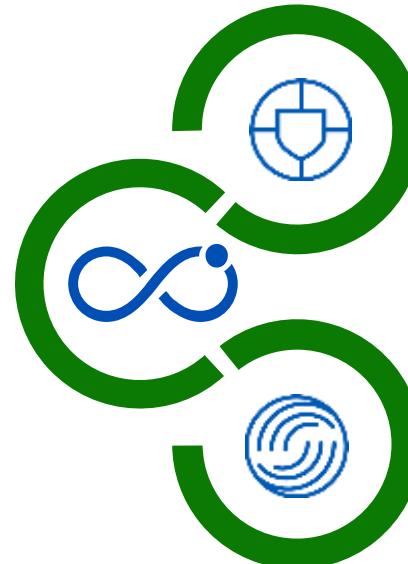


Data Loss Prevention controls accidental data loss and enables administrators to monitor and restrict the transfer of files containing sensitive data. For example, an administrator can prevent users sending sensitive data outside of the organization using web-based email accounts.

DLP uses rules which can be applied through a policy to protected devices. The DLP base policy includes multiple templates that cover standard protection for different regions.

Remediation

Synchronized Security
Heartbeat allows for the network isolation of an infected device



Any malicious files detected are **Quarantined**

Sophos Clean removes any detected files

SOPHOS

If malware is detected, it will be quarantined and automatically removed from the protected device.

The Synchronized Security heartbeat will communicate the device status via Sophos Central. If Synchronized Security is enabled and a Sophos Firewall is in use, the Sophos Firewall can isolate the device so that other devices on the network are not compromised.

Once Sophos Clean has successfully removed the threat, the device's clean status is communicated via Sophos Central. This will remove the device from network isolation.

Investigation and Visibility



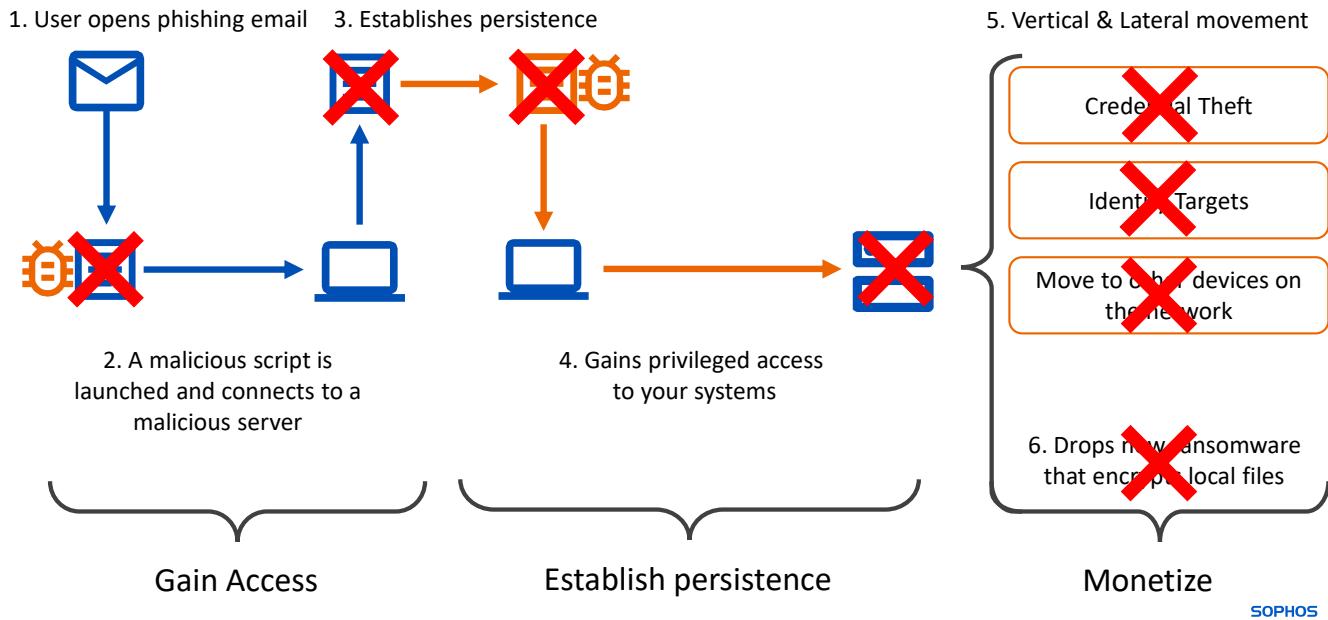
SOPHOS

Sophos Central provides full visibility of your organization. The dashboard displays the health of protected devices and users, along with alerts which are split by severity. This means that critical alerts will be shown immediately.

There are multiple logs and reports that can be customized to suit your requirements and you can use data sharing APIs to connect Sophos Central to third party applications.

The Threat Analysis Center allows you to easily view security incidents. Threat graphs allow you to view how an attack started, which files and systems were impacted and how the threat was responded to. Live Discover allows you to actively hunt malware across your organization and perform IT operational tasks. Live Response allows you to perform tasks remotely on protected and enabled devices.

Example Ransomware Attack



We have seen how an attacker could attack a device and covered the Sophos Central endpoint and server protection features that prevent attacks. To summarise using our previous ransomware attack example.

- To prevent an attacker gaining access to a protected device, Sophos Central implements control over applications, peripheral devices and website access
- It monitors the behaviour of files and prevents communication to malicious servers and bad URLs
- It scans and detects malicious files
- It uses anti-exploit features to prevent vertical and lateral movement across the network
- It prevents an attacker from compromising the boot and disk volumes and prevents ransomware from encrypting files

Knowledge Check

SOPHOS

Take a moment to check your knowledge!

Question 1 of 3

Match the protection feature to the feature description.

Peripheral Control

DROP

Control access to websites based on their category

Application Control

DROP

Block specific applications from running

Data Loss Prevention

DROP

Control removable media device use

Web Control

DROP

Monitor and restrict file transfers

Question 2 of 3

Which 2 of these protection features are used to protect devices when accessing Internet resources?

Web Protection

Live Protection

Malicious Traffic Detection

Web Control



Question 3 of 3

Which of these protection features are not enabled by default?

Live Protection

Download Reputation

Deep Learning

Application Control

SOPHOS

Chapter Review

Sophos Central endpoint and server protection uses **multiple layers of security** to protect against attack.

Sophos Central makes use of **multiple protection techniques** to detect both known and unknown threats .

Threat detection and **protection features** are **enabled by default**. Control features require configuration for use.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos Central endpoint and server protection uses multiple layers of security to protect against attack.

Sophos Central makes use of multiple protection techniques to detect both known and unknown threats.

Threat detection and protection features are enabled by default whereas control features require configuration for use.



An Introduction to Sophos Synchronized Security

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0515: An Introduction to Sophos Synchronized Security

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

An Introduction to Sophos Synchronized Security

In this chapter you will learn how Sophos Synchronized Security allows products to communicate with each other intelligently to respond to threats.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

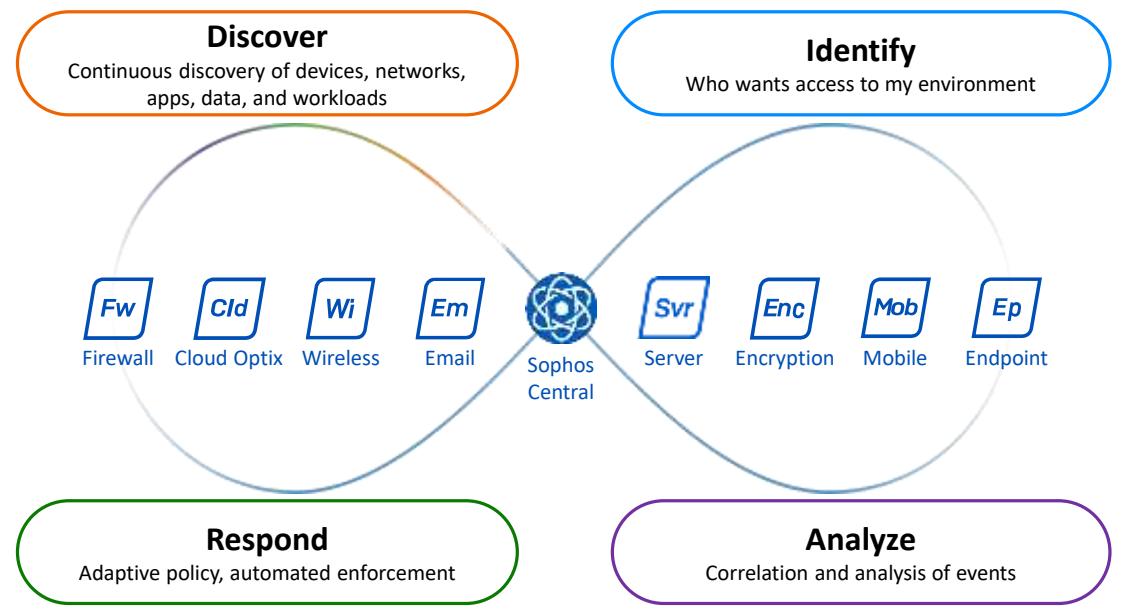
- ✓ What Sophos Central is and the protection features included in endpoint and server protection

DURATION **10 minutes**

SOPHOS

In this chapter you will learn how Sophos Synchronized Security allows products to communicate with each other intelligently to respond to threats.

What is Synchronized Security?



SOPHOS

Sophos Synchronized Security is cybersecurity as a system. Security products working together in real-time.

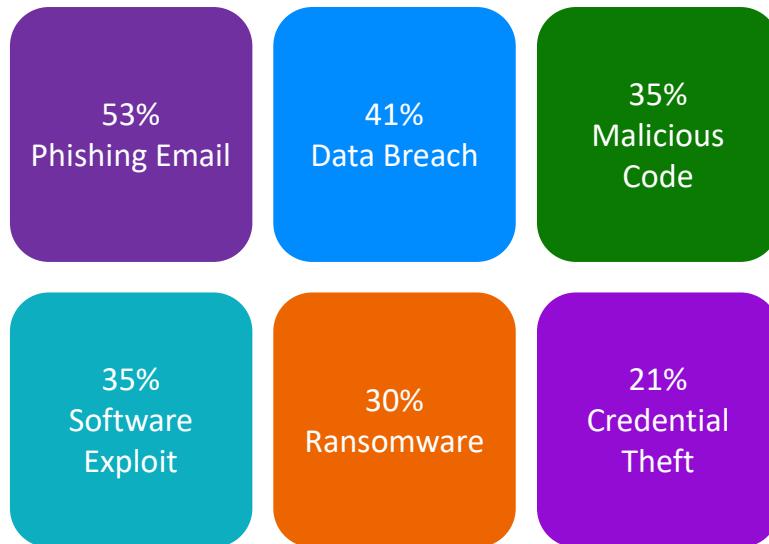
Traditionally, cybersecurity makes use of separate protection products to identify malicious files and to detect and stop malicious traffic. These products work well in isolation, however, are disconnected from each other. This approach results in an IT team manually correlating data between systems which can take time and often means threats are missed.

Sophos Synchronized Security automates detection, isolation, and remediation results which enables attacks to be neutralized quickly. It creates new ways to connect security products that protect your organization.



Additional information in
the notes

Why Synchronized Security?



SOPHOS

Cyber attacks often include multiple elements, for example, a phishing email could install malicious code that takes advantage of a software exploit to install ransomware. To help understand the types of threats being initiated, we asked organizations who had been victims of cyber attacks what types of threats they experienced. The results showed:

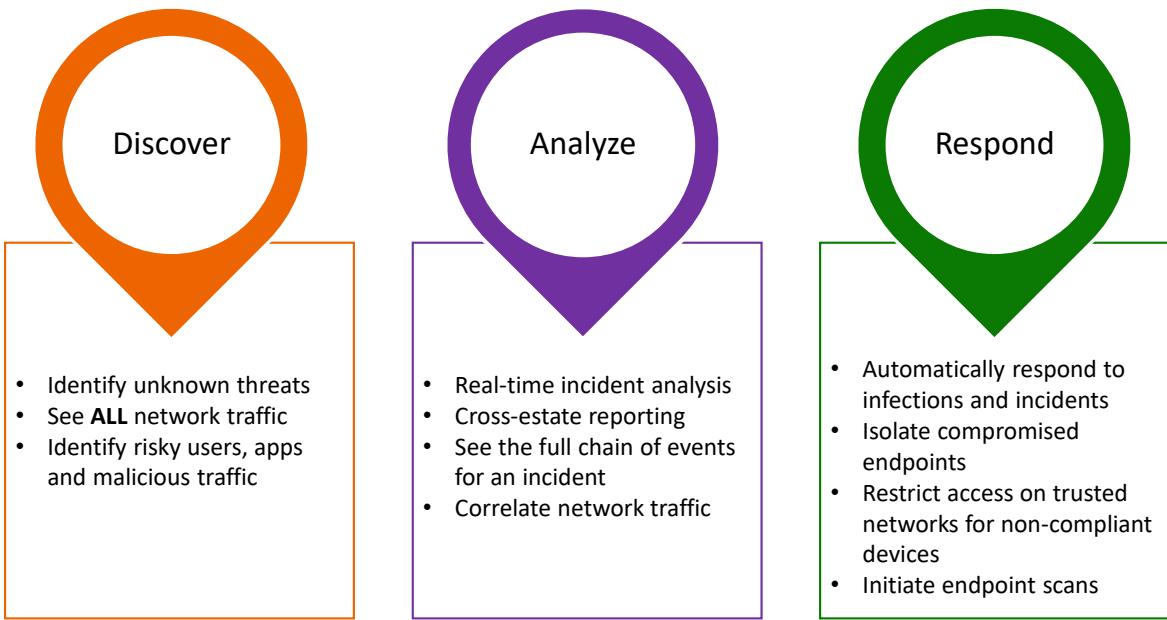
- Over 50% of attacks were introduced using phishing emails
- Over 40% were due to a data breach
- 35% were a result of malicious code or exploits
- 30% were infected with ransomware
- 20% experience credential theft

When added up, these numbers add up to more than 100% which demonstrates that attacks typically use multiple attack elements.

[Additional Information]

This information was taken from our white paper about endpoint security which is available here:
<https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx>

Synchronized Security Overview



SOPHOS

Synchronized Security takes a full system approach. Security products connect with each other in real-time, working together to combat advanced threats.

There are three pillars to the synchronized security system:

Discover. Sophos Central products automatically share information to reveal hidden risks and unknown threats. It enables administrators to see all network traffic, the identification of risky applications, and the correlating behaviour across multiple activities.

Analyze. Real-time incident analysis and cross-estate reporting delivers instant insights. This allows administrators to view the full chain of events for an incident.

Respond. Sophos Central automatically responds to incidents allowing compromised devices to be isolated protecting the entire estate and allowing time for threats to be investigated and remediated.

Synchronized Security Heartbeat

Communication between protected devices and Sophos Central



- A regular heartbeat. A few bytes every 15 seconds
- Event information
- Device health status
- Threat source information

SOPHOS

Communication between Sophos Central products is facilitated by the Sophos Security Heartbeat which creates a secure two-way tunnel of communication.

The Security Heartbeat allows for intelligent communication between Sophos products allowing for a coordinated response to threats. The Security Heartbeat includes:

- A regular heartbeat (a few bytes every 15 seconds) that identifies the device and communicates that the device is active and protected
- Communication of event information
- Communication of the device health status
- Communication of threat information

Security Heartbeat Status



GREEN Endpoint agent is running. No risk and no action required



YELLOW Endpoint agent is running. Medium risk and action may be required



RED Endpoint agent may not be running, and devices may not be protected. High risk and action is required

SOPHOS

Here you can see what each heartbeat status means.

If a computer has a GREEN status, this means that the endpoint agent is running and the computer is protected. No potentially unwanted applications, active or inactive malware has been detected.

If the computer has a YELLOW status, the endpoint agent is running so the computer is protected, however, inactive malware or a PUA has been detected. It can also indicate that the endpoint agent is out of date.

When a computer has a RED status, it can indicate that the endpoint agent may not be running, so the computer may not be protected. Alternatively, it could mean that active malware has been detected or malware has not been cleaned up. It could also mean that malicious network traffic has been detected, or communication to a known bad host has been identified.

Synchronized Security Examples

Sophos **Synchronized Security** integrates with **all** Sophos Central **products**

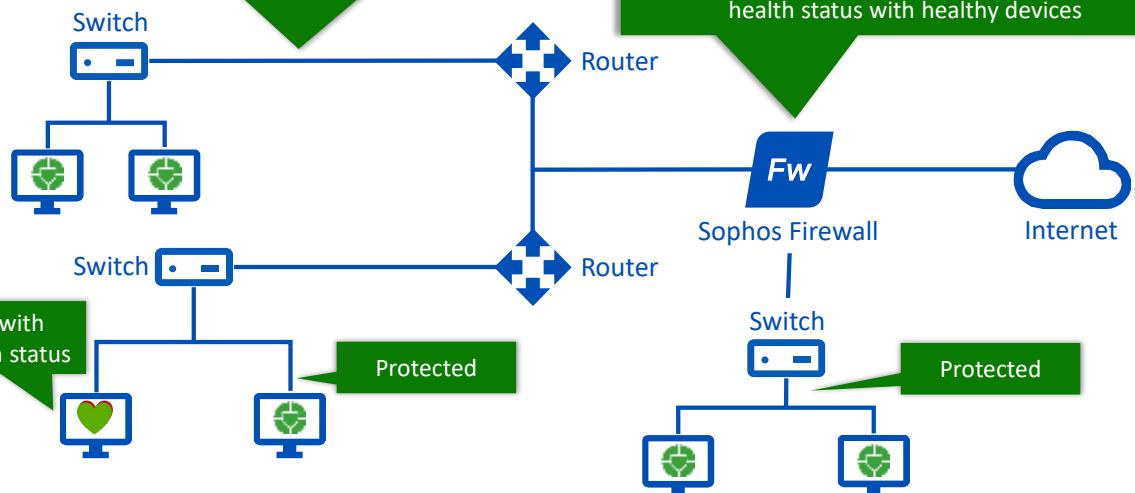
Let's have a look at some examples

SOPHOS

Sophos Synchronized Security integrates with all Sophos Central products, let's have a look at some examples.

Security Heartbeat with Sophos Firewall

Cannot drop traffic based on MAC address and not protected by Sophos Firewall



SOPHOS

What would happen if malware was detected on a device that is part of a network protected with Sophos Firewall and Synchronized Security enabled?

- If malware is detected, the Security Heartbeat sends event information along with the device health status to Sophos Firewall
- Sophos Firewall shares the MAC address of the device with other devices on the network
- Healthy devices drop traffic from the device with the red health status. This will only work on local network segments. If traffic is passing through a router, traffic will not be dropped
- When traffic passes through the Sophos Firewall, the firewall can prevent the device with a red health status from connecting to other devices which protects healthy devices from a possible infection
- Sophos Firewall only blocks the traffic from the red health status device, all other devices will have network access
- Once the endpoint agent has cleaned up malware on the device, the Security Heartbeat sends the updated health status to the Sophos Firewall
- Sophos Firewall allows the device to access hosts and networks as normal
- Sophos Firewall also updates all devices removing the MAC address of the compromised device from the list of devices with a red health status

Endpoint and Sophos Firewall

1. Malware Detection

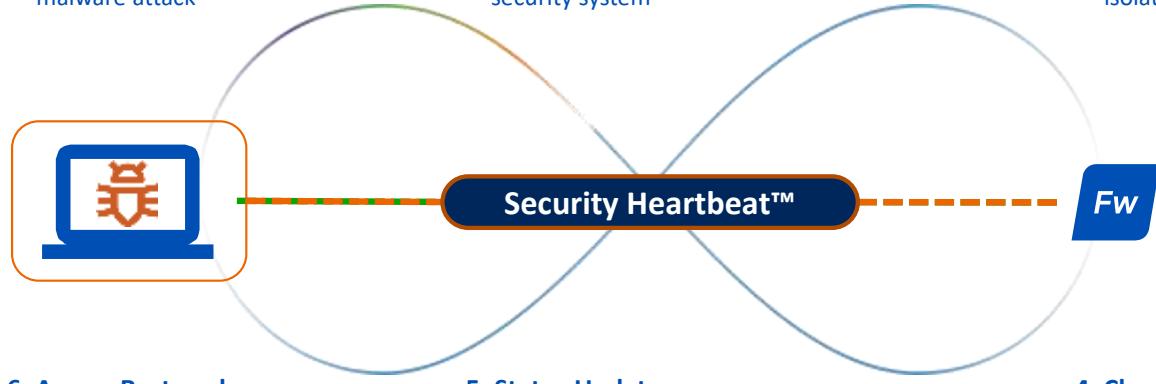
Sophos Endpoint detects a malware attack

2. Cross Estate Communication

Device status shared with the security system

3. Device Isolation

Sophos Firewall isolates the device



6. Access Restored

Sophos Firewall restores network access

5. Status Update

Clean status communicated via Security Heartbeat

4. Clean-up

Automatic clean-up on the device

SOPHOS

This diagram shows what happens when a device is protected with Sophos Central protection and a Sophos Firewall is in use.

1. Endpoint protection detects malware
2. The device health status is communicated via Security Heartbeat with the Sophos Firewall
3. The Sophos Firewall isolates the device on the network
4. Automatic remediation of the device ensures that the threat is cleaned up
5. Once the device is clean, the health status is updated and reported by Security Heartbeat
6. The Sophos Firewall then restores network access

The automatic incident response takes seconds with no human interaction required.

Server and Sophos Firewall

1. Malware Detection

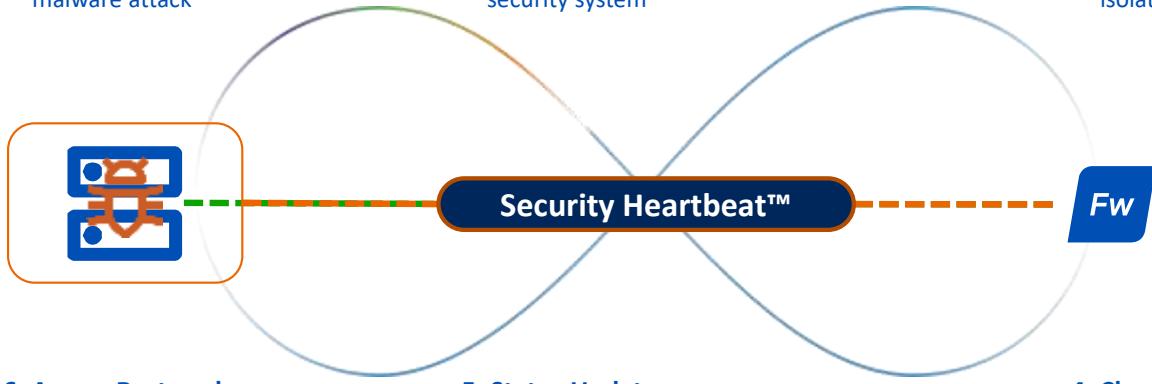
Sophos Server detects a malware attack

2. Cross Estate Communication

Server status shared with the security system

3. Device Isolation

Sophos Firewall isolates the Server



6. Access Restored

Sophos Firewall restores network access

5. Status Update

Clean status communicated via Security Heartbeat

4. Clean-up

Automatic clean-up on the Server

SOPHOS

If the endpoint protection is switched for server protection, the same events will happen should malware be detected on a protected server.

Please note that for servers, an administrator will need to provide approval for any actions taken.

Endpoint Protection and Sophos Email

1. Compromised Mailbox

Sophos Email detects a compromised mailbox

2. Mailbox Isolation

The mailbox is isolated

3. Communication

Isolation status shared with endpoint



Security Heartbeat™



6. Mailbox Restored

Mailbox sender privileges restored

5. Clean-up

The endpoint automatically cleans up the detection

4. Device Scan

The endpoint identifies and scans all known devices to the mailbox 

Here we can see a scenario where a device is using Sophos Email.

1. Sophos Email detects a compromised mailbox which is being used to send outbound spam emails
2. The mailbox is automatically isolated by Sophos Email
3. The status is shared via Security Heartbeat
4. The endpoint protection identifies and scans all known devices associated with the mailbox for malware
5. Endpoint protection automatically cleans up any malware found
6. The mailbox is then restored

Zero-Touch Lateral Movement Protection

1. Threat Detected



2. Cross Estate Communication

Security Heartbeat™



SOPHOS

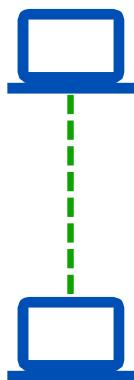
An attacker will typically want to move across your network in order to gain better access to your data. This is called lateral movement.

Synchronized Security provides lateral movement protection.

1. If a protected device detects a threat, the health status of that device is set to red
2. The health status is shared with the Sophos Firewall using Security Heartbeat

Zero-Touch Lateral Movement Protection

1. Threat Detected

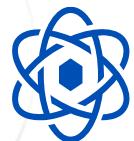


2. Cross Estate Communication



Security Heartbeat™

3. Infection Isolated from the Network and LAN



5. Device health status shared

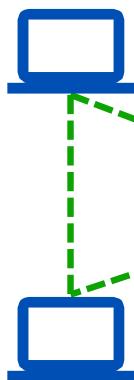
4. Infection Cleaned Up

SOPHOS

3. The Sophos Firewall isolates the device from both the network and the LAN
4. Endpoint protection automatically cleans up the threat
5. The now healthy device shares the updated health status with Sophos Firewall

Zero-Touch Lateral Movement Protection

1. Threat Detected

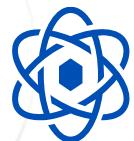


2. Cross Estate Communication

Security Heartbeat™

5. Device health status shared

3. Infection Isolated from the Network and LAN



4. Infection Cleaned Up

6. The connection to the network and the LAN is restored

This process happens in seconds by sharing information and using dynamic policies that respond to incidents and events.

SOPHOS

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

When malware is detected, what device information does Sophos Firewall share with other devices on the network?

MAC Address

IP Address

Host Name

User Information

SOPHOS

Question 2 of 2

What is the interval in seconds between each Security Heartbeat? (enter numerical value)

Chapter Review

Sophos Synchronized Security **automates detections, isolation and remediation** results which enables attacks to be neutralized quickly.

There are **3 pillars** to the Synchronized Security system; **discover, analyze and respond**.

Communication between Sophos Central products is facilitated by the **Sophos Security Heartbeat**.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos Synchronized Security automates detection, isolation and remediation results which enables attacks to be neutralized quickly.

There are three pillars to the Synchronized Security system; discover, analyze and respond.

Communication between Sophos Central products is facilitated by the Sophos Security Heartbeat which creates a secure two-way tunnel of communication.



Getting Started with the Sophos Central Dashboard

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0520: Getting Started with the Sophos Central Dashboard

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Dashboard

In this chapter you will learn how to register for a Sophos Central trial account, and how to access the Sophos Central Dashboard.

It also provides an overview of the Sophos Central Dashboard.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Sophos Central is and the protection it offers

DURATION 8 minutes

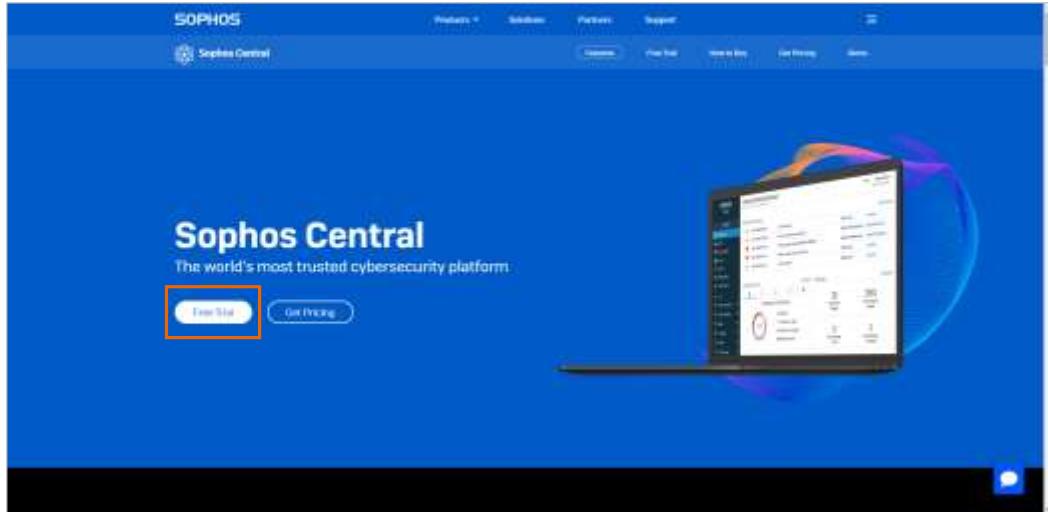
SOPHOS

In this chapter you will learn how to register for a Sophos Central trial account, and how to access the Sophos Central Dashboard.

It also provides an overview of the Sophos Central Dashboard.

How to Register for a Sophos Central Trial

Sign up for a Sophos Central trial at: [sophos.com/central](https://www.sophos.com/central)



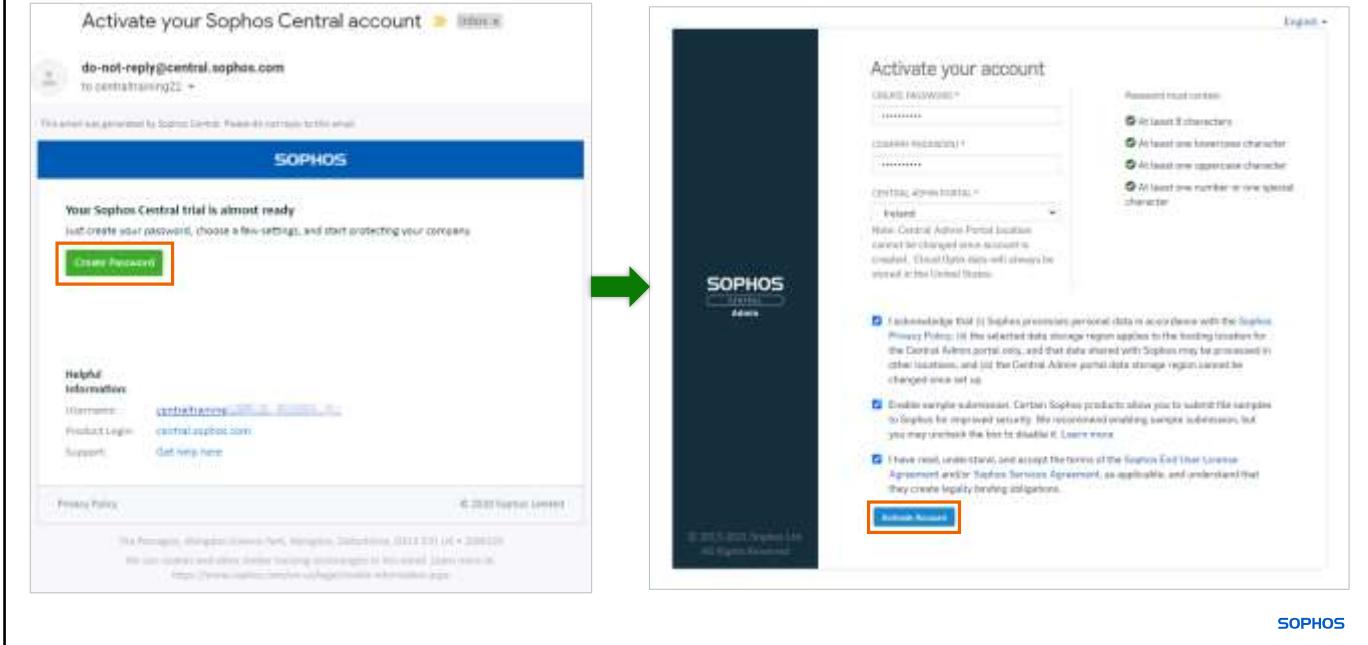
SOPHOS

To get started with Sophos Central, sign up for a trial account via the Sophos website.

After entering your credentials, you will receive an email with the details of how to activate your Sophos Central account. The email is sent to the email address you entered during the registration process.

All trial accounts are valid for thirty days. This period can be extended by contacting your Sophos account team if required.

Activating Sophos Central



The activation email includes the link to create a password for your trial account. You will be prompted to create and confirm a password.

You need to select the Sophos Central Admin Portal from the drop-down menu. Please note that this location cannot be changed once your account has been created.

The privacy policy, sample submission, and the Sophos end user license agreements should be read and accepted.

You can then select **Activate Account**.

Sophos Central Dashboard

<https://central.sophos.com>

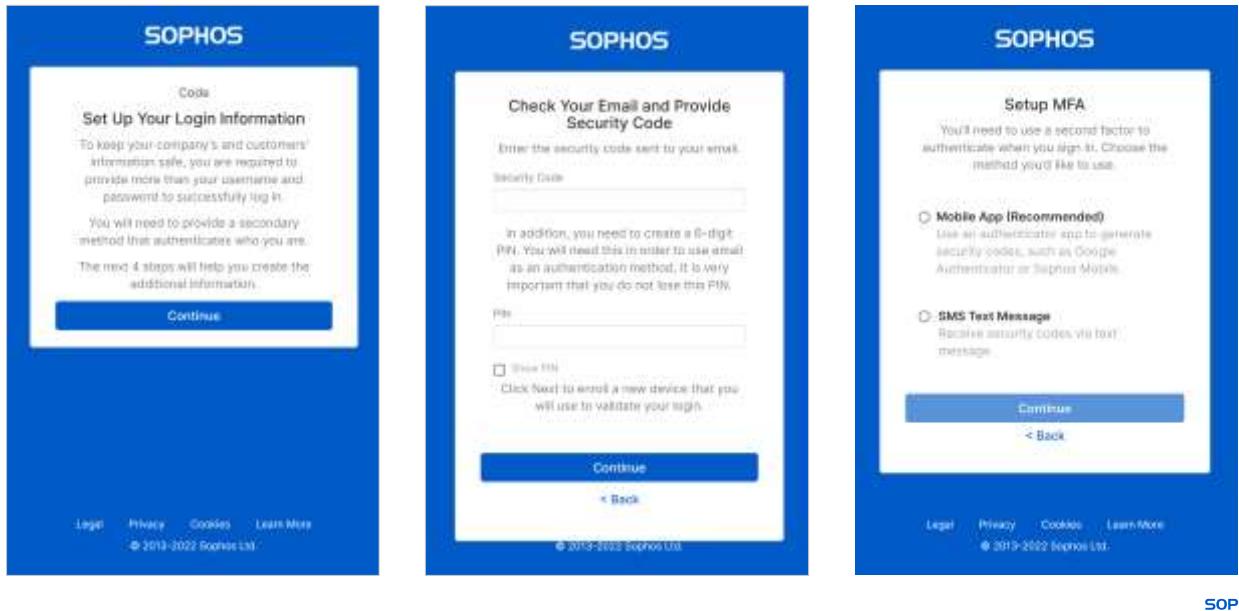


Following the activation of your Sophos Central account, you are automatically logged into your Central Dashboard.

For future access to Sophos Central, navigate to central.sophos.com and enter your Sophos ID. This is the email address you used to register for your Sophos Central account and the password you created when you activated the account.

Multi-factor authentication is required to login to Sophos Central.

Multi-Factor Authentication



Multi-factor authentication needs to be setup when you log back into your Sophos Central account following activation.

Once you have entered your email address and password you will be re-directed to the 'Set Up Your Login Information' page. A security code is sent to the email address you used to register your account. Enter the security code from the email and create a six-digit PIN code.

Select the MFA authentication type, selecting from either SMS text message or a Google or Sophos Authenticator. Once you have selected the authentication type, additional steps will be presented.

If you select SMS text message, you will be prompted for the country and number of the mobile device. You will then be prompted to verify the mobile device by entering the security code sent to that device in a text message.

If you select Google or Sophos Authenticator, scan the QR code that is presented and enter the security code displayed.

Once a security code has been entered, you will be logged into Sophos Central.

Simulation: Registering and Activating Sophos Central



In this simulation you will register for and activate a new Sophos Central trial account

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/RegisteringCentral/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/RegisteringCentral/1/start.html>

Sophos Central Dashboard

The dashboard features a top navigation bar with 'Help', 'Sign In', and 'Logout' links. On the left, a sidebar lists 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Below this is a section for 'My Products' with icons for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Small Business, Firewall Management, Phish Threat, and Cloud Native Security.

The main content area includes:

- Alert Summary:** Shows 2 Total Alerts, 0 High Alerts, 1 Medium Alert, and 1 Low Alert.
- Most Recent Alerts:** Lists two recent events: 'READING03 is out of date.' (Sep 22, 2022 12:08 PM) and 'Firewall connection to Sophos Central has been restored.' (Aug 23, 2022 5:59 PM). Each event has a 'View full details' link.
- Devices and users: summary:** A circular chart showing Endpoint Computer Activity Status with the following data:
 - 3 Active
 - 5 Inactive 2+ Weeks
 - 0 Inactive 2+ Months
 - 0 Not ProtectedA 'See Report' link is provided.
- Web control:** Shows 0 Web Threats Blocked and 45 Policy Violations Blocked. It also shows 0 Policy Warnings Issued and 0 Policy Warnings Processed. A 'See Reports' link is provided.

The Central dashboard is made up of sections, the top section will display the alert summary which collates the number of alerts by severity. In the most recent alerts section, you can select individual alerts to view the full details.

A summary of your protected devices and users is displayed by their active status. Any web pages that have been blocked or a warning message returned will also be displayed on the dashboard.

All summaries include links to the specific pages in Sophos Central that will provide more details.

Sophos Central Dashboard

The screenshot shows the Sophos Central interface. On the left, there's a vertical navigation pane with a dark header containing the Sophos logo and "Sophos Central". Below this are sections for "Dashboard", "Metrics", "Threat Analysis Center", "Logs & Reports", "Devices", "Initial Settings", "3rd-party Connectors", "Protect Device", and "Account Health Check". A red box highlights the "MY PRODUCTS" section, which lists ten products: Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, Phish Threat, Cloud Native Security, and Switches. A hand cursor is hovering over the "Endpoint Protection" item. To the right of the products is a blue callout box with white text: "Your licensed products are listed in the left-hand navigation pane". In the bottom right corner of the main area, the word "SOPHOS" is printed.

Your licensed products are listed in the left-hand navigation pane.

Clicking on a product will take you to that products dashboard. You can then return to the Central Dashboard when required and you will not be logged out during this process.

Sophos Central Dashboard

The screenshot shows the Sophos Central Dashboard with the left-hand menu expanded. The menu includes sections for SOPHOS, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, Account Health Check, and MY PRODUCTS (Endpoint Protection, Server Protection, Mobile). The Alerts section is currently selected, indicated by a blue bar at the top of the menu. The main content area is titled 'Alerts' with the sub-instruction 'Analyze your alerts.' Below this are four summary boxes: 'Total Alerts' (2), 'High Alerts' (0), 'Medium Alerts' (1), and 'Low Alerts' (1). A 'Mark As Acknowledged' button is present. Below these are filtering options ('Filter By: All products', 'All categories') and a 'Ungroup / Group' toggle. A table lists two alerts: 'Firewall connection to Sophos-Central has been restored' (Count: 1) and 'Computer or server out of date' (Count: 1). Actions for each alert include 'Mark As Acknowledged' and 'Reinstall Endpoint Protection'. At the bottom, a pagination indicator shows '1 - 2 of 2'.

The left-hand menu allows you to access key features of Sophos Central.

The **Alerts** page displays a summary of all alerts allowing you to take immediate action if required.

The **Threat Analysis Center** displays the most important threat information. You can view threat graphs, access Live Discover, view detections and perform threat hunting.

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

Sophos Central Dashboard

The screenshot shows the Sophos Central dashboard with the 'People' page selected. The left sidebar includes links for Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People (which is highlighted in blue), and Devices. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'People: Manage your users'. It has tabs for 'Users' (selected) and 'Groups'. Below are buttons for 'Add', 'Email Template', and 'Delete'. A search bar and a 'Set up directory service' link are also present. The main table lists users with columns for Name, Email, Exchange Login, and Last Active. The table shows five users: TRAININGDEMO\anobie, WINCLIENT4\TrainingDemo, Adam Jones, Anne Green, and John Smith. The last user, John Smith, is currently selected. At the bottom, it says '1-101 of 101 users/ 0 selected' and 'Last updated: Sep 26, 2022, 11:12 AM'.

Name	Email	Exchange Login	Last Active
TRAININGDEMO\anobie		Add Exchange Login	Dec 10, 2021 4:11 PM
WINCLIENT4\TrainingDemo		Add Exchange Login	Dec 10, 2021 9:43 AM
Adam Jones	ajones@sophotraining.xyz	ajones	Nov 17, 2021 2:30 PM
Anne Green	agreen@sophotraining.xyz	agreen	Nov 17, 2021 2:30 PM
John Smith	jsmith@sophotraining.xyz	jsmith	Nov 17, 2021 2:30 PM

The **People** page is where you add and manage users and create user groups.

On the **Devices** page you can manage your protected devices. The devices are listed by type on different tabs. The tabs displayed will depend on the features included in your license.

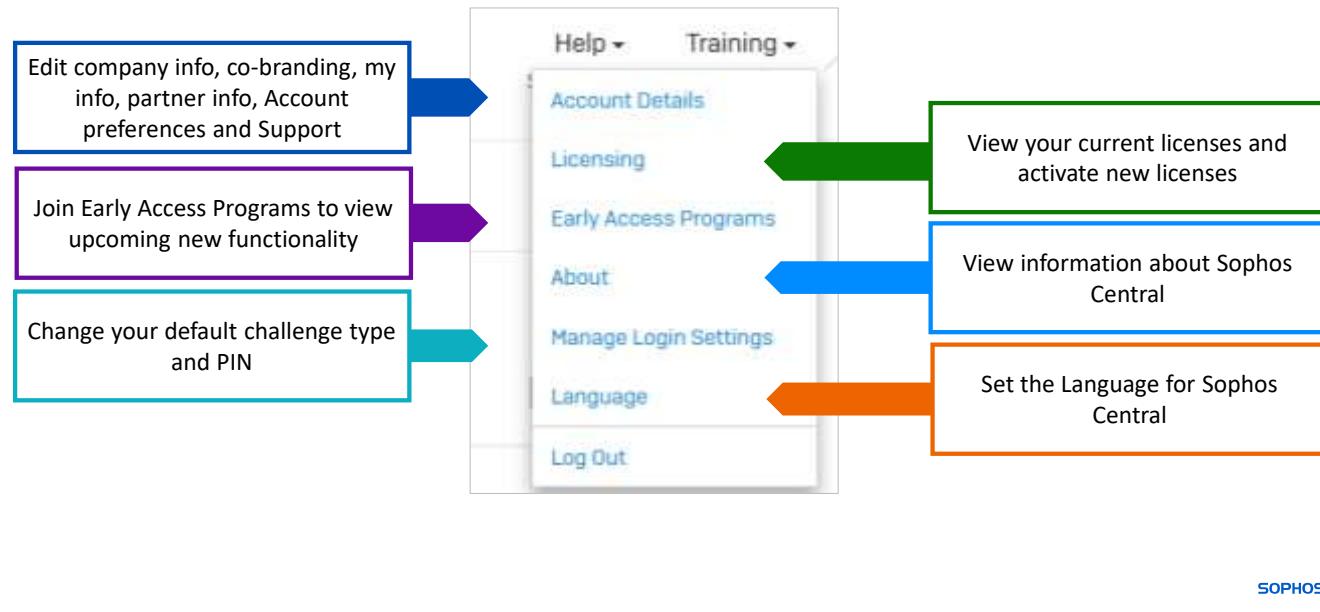
The **Global Settings** page is used to specify security settings that apply to all your users and devices. The pages displayed will depend on the features included in your license.

The **Third-party Connectors** page is where you can add and manage third party connectors. You must have an admin or a super admin user role to add or delete connectors.

The **Protect Devices** page is where you can download Sophos Installers and use them to protect your devices.

The **Account Health Check** page enables you to check that your account has the best protection.

Sophos Central Dashboard



If you click on your username in the top right-hand corner, you will see the toolbar menu. This menu provides links to your account details, licensing, and early access programs.

You can also view information about Sophos Central and set the language of the dashboard.

Manage Login Settings allows you to change your default challenge type and PIN. This menu is also where you log out of Sophos Central.

Sophos Central Dashboard

The screenshot shows the Sophos Central Licensing interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, etc. The main area is titled 'Licensing' with the sub-instruction 'View your license and usage info.' Below this, it says 'License Details:' followed by a table of license information. The table has columns for LICENSE, TYPE, USAGE, LIMIT, STARTS, EXPIRES, and LICENSE #. Each row lists a different product or service. At the top right of the table are two buttons: 'Apply License Key' (which is highlighted with a red box) and 'Contact Partner to Buy'. At the bottom right of the table, there's a link 'Review end-user license agreement'.

LICENSE	TYPE	USAGE	LIMIT	STARTS	EXPIRES	LICENSE #
Phish Threat	Trial	0	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Device Encryption	Trial	0	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Intercept X Advanced with XDR	Trial	4	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Mobile Advanced	Trial	0	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Sophos Intercept X for Mobile	Trial	0	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Intercept X Advanced for Server with XDR	Trial	9	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]
Email Advanced	Trial	0	100	Feb 2, 2022	Feb 1, 2027	LD[REDACTED]

To add a license to Sophos Central, select **Licensing** from the top right-hand menu and select **Apply License Key**.

Sophos Central Dashboard

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, Account Health Check, and several sections for Endpoint Protection, Server Protection, and Mobile. The main area is titled 'Licensing' and contains a sub-section for 'License'. A modal window titled 'Activate License Key' is open in the center. It has a text input field labeled 'LICENSE KEY' with placeholder text 'Enter License Key'. Below it is a checkbox with the text: 'I have read, understand, and accept the terms of the Sophos End User Terms of Use and understand that they create legally binding obligations. I acknowledge that Sophos collects and processes personal data in accordance with the Sophos Group Privacy Notice.' To the right of the checkbox is a note: 'Note: This step is irreversible so please be sure you are applying the License Key to the correct customer. For assistance, contact customer support.' At the bottom of the modal are two buttons: 'Cancel' and 'Apply'. A large green callout box points to the 'Enter your license key to apply any new licenses' text in the modal.

Enter the license key details. Once this is completed, the license status will be updated to show the license details, such as the usage and limit of the license along with the start and expiry date.

Request Assistance

The screenshot shows the Sophos Central interface. On the left sidebar, under 'Sophos Central', there are links for Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, and Wireless. The main content area is titled 'Account Details' with a sub-section 'Add or modify administrator accounts'. A large arrow points from the 'Sophos Support' link in the sidebar to the 'Change Sophos Support settings' section. This section contains two toggle switches: 'Remote Assistance' (which is turned on) and 'Partner Assistance' (which is also turned on). Below each switch is a descriptive note. At the bottom right of the support section is a 'Save' button. The top right corner shows the user's name, Simon Smith, and their role, Super Admin.

Account Details

Add or modify administrator accounts

ACCOUNT DETAILS

- Company Info
- Co-branding
- My Info
- Partner Info
- Account Preferences
- Sophos Support

Change Sophos Support settings.

Remote Assistance

This will give Sophos Support full troubleshooting access to your Sophos Central session for 120 hours. If any of your systems protected by Sophos Central products are part of your PCI Compliance strategy, you are advised to please contact Sophos Support directly prior to granting access due to PCI requirements around vendor access. I also acknowledge that Sophos processes personal data in accordance with the Sophos Group Privacy Notice.

Partner Assistance

Note: This enables your designated partner to access your Sophos Central Admin portal and configure the Sophos Central service on your behalf. If you do not enable partner assistance, your partner will only see high-level reporting information such as services purchased and current usage stats.

The unique ID for this Sophos Central account is: XXXXXXXXXXXXXX [Copy](#)

This account is located in the Ireland region.

The ‘Account Details’ page includes an option to allow Sophos Support to provide remote assistance. It also allows you to enable partner assistance.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Which 2 of these methods are supported for Sophos Central multi-factor authentication?

SMS text message

Google/Sophos
Authenticator

QR Code

Software Token

SOPHOS



Question 2 of 2

True or False: You can add a license to your Central Trial account from Global Settings.

True

False

SOPHOS

Chapter Review

To get started with Sophos Central you must **register for and activate a Sophos Central Trial account**.

You can convert a Sophos Central trial account by entering a **license activation code**.

Remote Sophos and **Partner assistance** can be **enabled** in the **Account Details** page if required.

SOPHOS

Here are the three main things you learned in this chapter.

To get started with Sophos Central you must register for and activate a Sophos Central trial account.

You can convert a Sophos Central trial account by entering a license activation code.

Remote Sophos and Partner assistance can be enabled in the Account Details page if required.



Getting Started with Sophos Central Global Settings

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0525: Getting Started with Sophos Central Global Settings

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Global Settings

In this chapter you will learn about the global settings available in Sophos Central. This chapter covers the most used settings.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

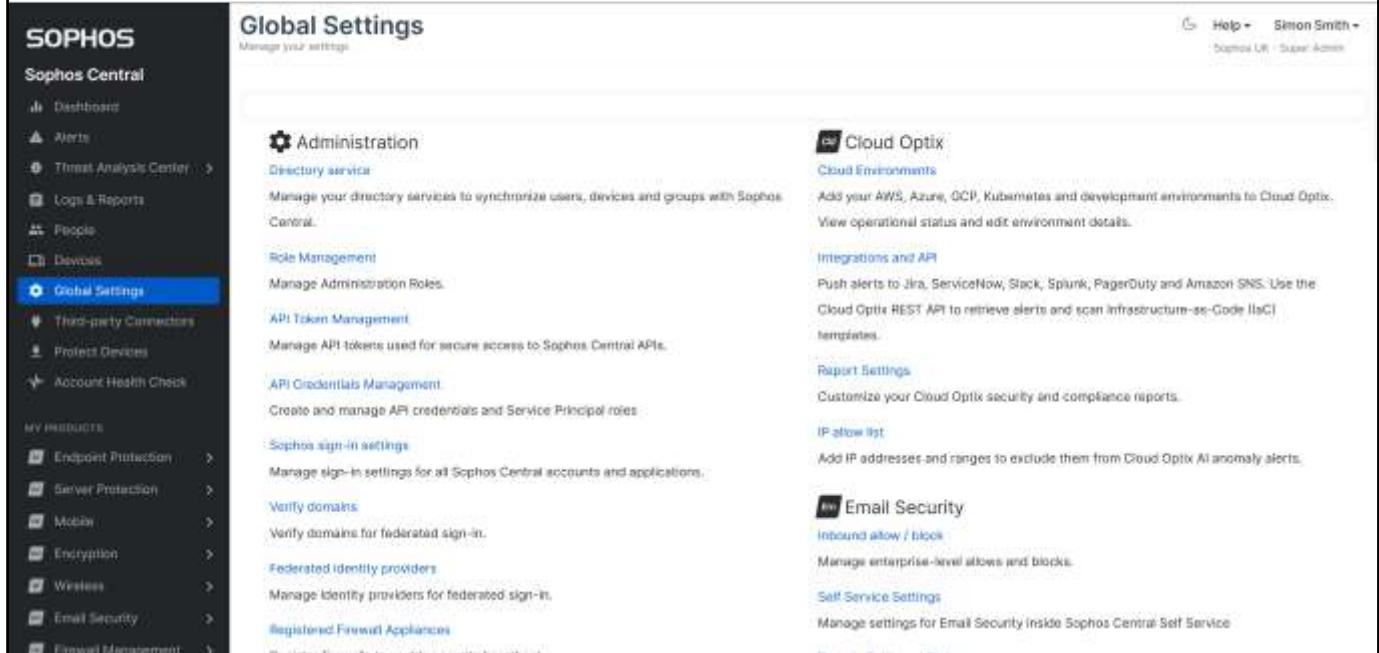
- ✓ What Sophos Central is
- ✓ What features Sophos Central endpoint and server protection offers
- ✓ How to access Sophos Central

DURATION **6 minutes**

SOPHOS

In this chapter you will learn about the global settings available in Sophos Central. This chapter covers the most used settings.

Global Settings Overview



The screenshot shows the Sophos Central interface with the 'Global Settings' page selected in the navigation bar. The left sidebar lists various product categories like Endpoint Protection, Server Protection, and Email Security. The main content area is divided into several sections: 'Administration' (with sub-sections for Directory service, Role Management, API Token Management, API Credentials Management, Sophos sign-in settings, Verify domains, Federated identity providers, and Registered Firewall Appliances), 'Cloud Optix' (with sub-sections for Cloud Environments, Integrations and API, Report Settings, and IP allow list), and 'Email Security' (with sub-sections for Inbound allow / block and Self Service Settings). The top right corner shows user information: Help, Simon Smith - Sophos UK - Super Admin.

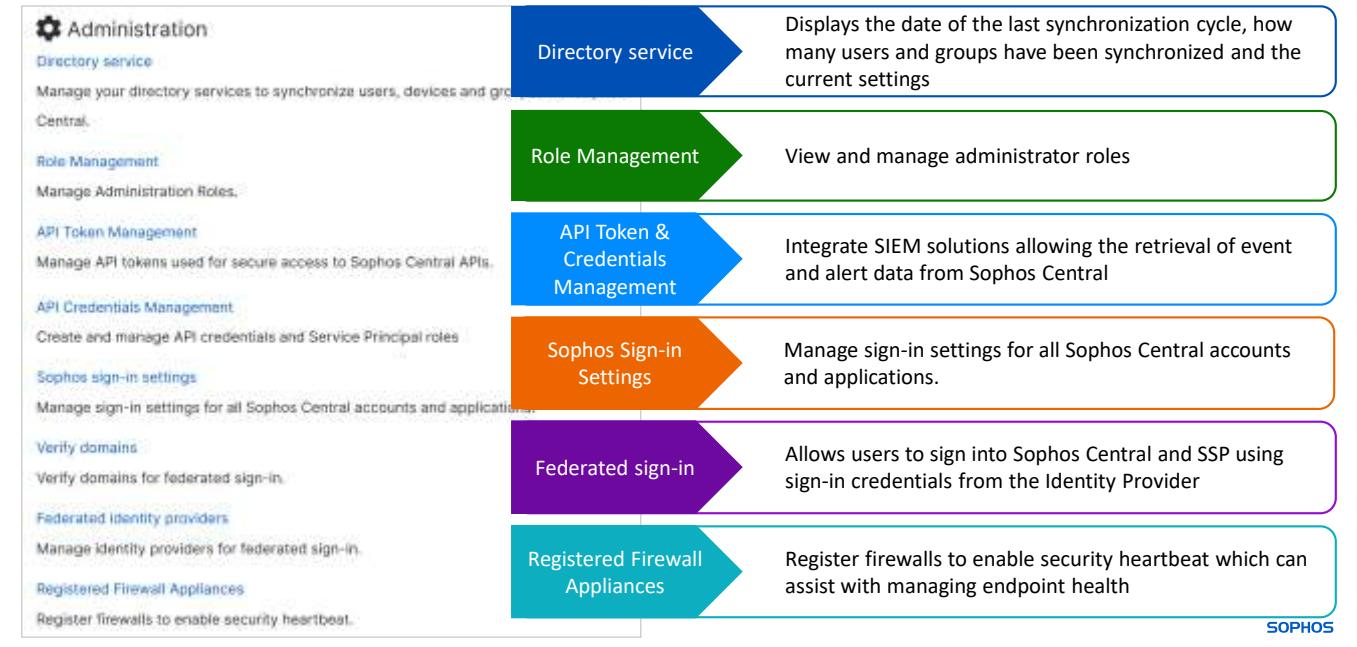
Global settings are used to specify security settings that apply to all users and devices.

The sections displayed will depend on the features included in your license. The 'Administration' and 'General' sections will always be listed followed by your licensed products.

Many of the global settings relate to controlling what your users can access on their protected endpoints and configuring protection for users along with determining bandwidth restrictions and proxy configurations.

Let's have a look at some of the settings in the administration and general sections.

Global Settings - Administration

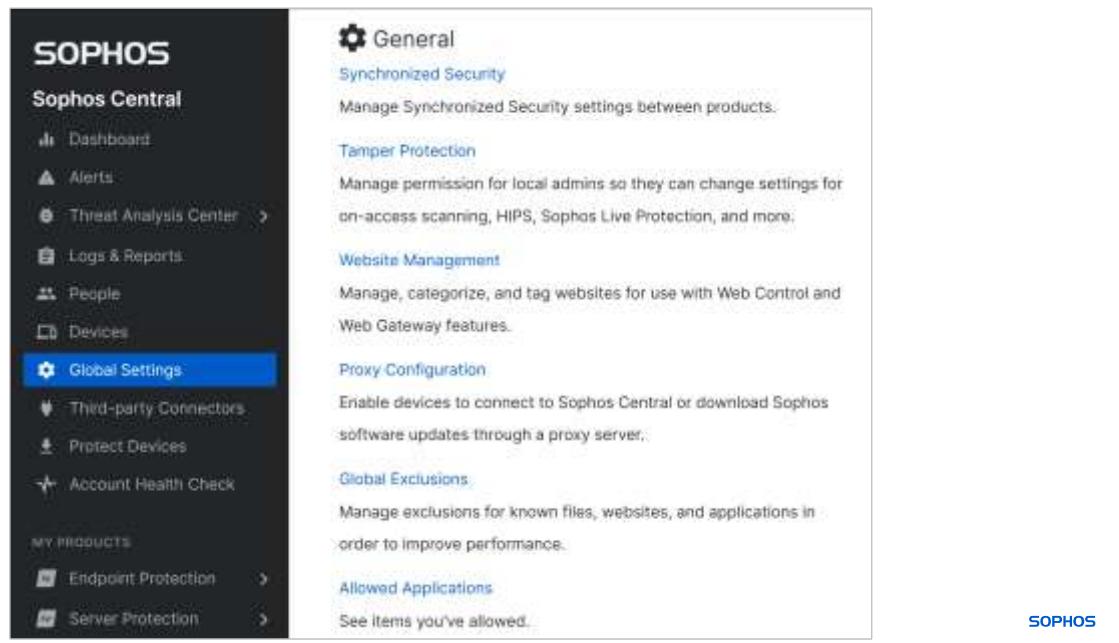


SOPHOS

In the ‘Administration’ section you can:

- Configure and view directory service settings and status
- Manage role-based access
- Configure API tokens and manage API credentials
- Verify, configure, and manage federated sign-in settings
- Register firewall appliances to enable security heartbeat

Global Settings - General



The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected and highlighted in blue), Third-party Connectors, Protect Devices, and Account Health Check. Below that is a section for 'MY PRODUCTS' with Endpoint Protection and Server Protection. The main content area on the right is titled 'General' and contains several sub-sections: 'Synchronized Security' (Manage Synchronized Security settings between products), 'Tamper Protection' (Manage permission for local admins so they can change settings for on-access scanning, HIPS, Sophos Live Protection, and more), 'Website Management' (Manage, categorize, and tag websites for use with Web Control and Web Gateway features), 'Proxy Configuration' (Enable devices to connect to Sophos Central or download Sophos software updates through a proxy server), 'Global Exclusions' (Manage exclusions for known files, websites, and applications in order to improve performance), and 'Allowed Applications' (See items you've allowed). The Sophos logo is in the bottom right corner.

The ‘General’ section includes several global settings; we will look at a few of these.

Global Settings – Synchronized Security

- Monitors outbound email for spam and viruses
- Sophos Endpoint Protection runs an on-demand scan on the devices linked to the mailbox
- Alerts are sent if a sender has been blocked

The screenshot shows the Sophos Central interface. On the left is a dark sidebar with the 'SOPHOS' logo and 'Sophos Central' title, followed by a list of navigation items: Dashboard, Alerts, Threat Analysis Center (with a dropdown arrow), Logs & Reports, People, Devices, and Global Settings (which is highlighted with a blue background). The main content area is titled 'Synchronized Security' under 'Global Settings'. It displays the message 'Manage Synchronized Security settings between different products.' Below this is a toggle switch labeled 'Scan computers that send spam or viruses' with the description 'Automatically scan computers where Email Gateway finds spam or viruses in outbound email'. At the top right of the content area are 'Help', 'Simon Smith', and 'Sophos UK - Sigma Admin' buttons, along with a 'Save' button. The bottom right corner of the main window has the 'SOPHOS' logo.

Sophos email protection is used to protect and manage your email clients, should a virus or spam be sent in an outbound email, this will be detected. When Synchronized Security is enabled it monitors all outbound mail and acts if five or more emails are classified as spam or contain a virus within a 10-minute period.

If this happens, it will identify the originating mailbox that the virus or spam was sent from along with the owner and any devices assigned to that owner. Additionally, that mailbox will be blocked from sending outbound mail for 1 hour which will automatically send an alert to the administrator.

Sophos endpoint protection automatically runs an on-demand scan on devices linked to the identified mailbox.

Global Settings – Alert Email Settings

- Manage which administrators get email alerts
- Configure distribution lists and the frequency of email alerts
- Set custom rules that specify which alerts get sent to which administrators
- Configure exceptions for individual alert types

The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes options like Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices, Global Settings (which is selected), Third-party Connectors, Protect Devices, and Account Health Check. Under My Widgets, there are Endpoint Protection and Server Protection. The main content area is titled 'Configure email alerts' and has tabs for Administrators, Distribution lists, Alerts, Custom rules, and Exceptions. The 'Alerts' tab is active. It contains a section for 'Notification frequency' with a note: 'Choose how often you want to receive email alerts. You can set the frequency depending on severity, product, or alert category, but you can only use one of these.' Below this, there's a radio button group for 'Set by severity' with three options: 'High alert' (selected), 'Medium alert', and 'Info alert'. For each, there's a dropdown for 'Send alert' with options like 'Immediately', 'Hourly', and 'Daily'. A 'Save' button is at the bottom right, and a link 'Review Testbed default settings' is also present.

A user with the super admin role can manage how administrators receive email alerts. You can manage which administrators receive email alerts. Click yes or no to enable or disable the alerts for specific administrators.

You can manage the distribution lists or email addresses that you want to receive email alerts. This option allows you to notify people who do not have access to Sophos Central for specific alerts.

You can control the frequency with which administrators receive email alerts depending on the severity of the alert, the product or the category the alert is in.

Custom rules allow you to set which administrators get which alerts. Please note that using a custom rule will stop any existing recipient settings including distribution lists.

The exceptions list shows the exceptions you have set up. These are set up on an ad-hoc basis in the alerts page.

Global Settings – Proxy Configuration

- Enables devices to connect to Sophos Central or download Sophos agent updates through a proxy server

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected. The main content area is titled 'Proxy Configuration' under 'Global Settings / Proxy Configuration'. A descriptive text at the top states: 'Enable devices to connect to Sophos Central or download Sophos software updates through a proxy server.' Below this is a toggle switch labeled 'Proxy Configuration' which is turned on. A note below the switch says: 'Changes to this setting will take effect for both user devices and servers.' There are four input fields: 'Hostname' (AD.SOPHOSTRAINING.XYZ), 'Port' (3389), 'Username' (Administrator), and 'Password' (redacted). To the right of these fields is a note: 'Windows, Mac and Linux computers and servers will connect to the Internet using the first working attempt:'. Below this is a numbered list: 1. Connect using a Sophos Central message relay; 2. Connect using the proxy configured here; 3. Connect using the default system proxy; 4. Connect using an automatically discovered proxy (WPAD); 5. Connect without using a proxy. At the bottom left is a note: 'Due to security reasons, we cannot retrieve the proxy configuration password. If you click save you may be overwriting the value.' At the top right are 'Save' and 'Cancel' buttons, and a user profile 'Simon Smith - Sophos UK - Super Admin'.

If you need to define an explicit proxy to access the Internet, you can do so here. If the proxy requires authentication you need to provide credentials. Please note that you can only define a single proxy configuration.

Any changes made here will take effect on both computers and servers.

Global Settings – Bandwidth Usage

- Set a custom bandwidth usage limit for endpoints and servers
- The limit is enforced when the endpoints download Sophos software and threat detection updates
- Sophos sets the frequency of data updates to minimize bandwidth usage

The screenshot shows the Sophos Central interface. On the left, the navigation menu is visible with 'Global Settings' selected. The main content area is titled 'Bandwidth Usage' under 'Global Settings'. It contains a section for 'Bandwidth Limit (Windows Only)' with a note about enforcing limits for software and threat detection updates. A dropdown menu for 'BANDWIDTH LIMIT' shows '256 Kbps (Sophos Default)'. Below this is a 'Data Updates' section with a note about Intercept X and Sophos Linux protection, and a checked checkbox for 'Use default frequency'.

SOPHOS

You can configure the bandwidth used for updating the Sophos agent software on Windows devices.

Currently the default bandwidth limit is 256 Kbps. You can specify a custom bandwidth limit or unlimited bandwidth. This limit will be enforced as computers download Sophos software and threat detection updates.

By default, Sophos sets the frequency of data updates in Sophos Central to an average of once a week. This helps reduce network bandwidth while ensuring devices are updated to changes in the threat landscape.



Additional information in
the notes

Global Settings – Device Migration

- To migrate computers, the user must have the Admin role in both Sophos Central accounts
- API credentials with the Service Principal Super Admin credentials are required in both Sophos Central accounts
- Only allow migrations for a limited time period

The screenshot shows the Sophos Central interface. On the left, there's a dark sidebar with various menu items like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is highlighted in blue), and Third-party Connectors. The main content area is titled 'Device Migration' under 'Global Settings'. It contains a note about migrating devices via APIs. There are two radio buttons for migration settings: 'Allow device migration' (selected) and 'Allow migration until a set time' (also selected). A date and time input field shows '2022-10-03 15:25'. At the bottom right of the main area, there are 'Save' and 'Cancel' buttons.

You can migrate computers from one Sophos Central account to another.

To migrate computers, the user must be assigned the admin role in both Sophos Central accounts. You will also need API credentials for both accounts that have the **Service Principal Super Admin** role.

We recommend that you only allow migrations for a limited time period. To migrate computers, use our Endpoint API and follow the instructions in the help guide. A link to the guide is available in the notes of the student handout.

[Additional Information]

<https://docs.sophos.com/central/Customer/helpenus/ManageYourProducts/GlobalSettings/DeviceMigration/index.html#use-endpoint-api>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

True or False: The global setting for bandwidth usage only applies to Windows devices.

True

False

SOPHOS



Question 2 of 2

Which of these options allows you to send email notifications for specific alerts to people who do not have access to Sophos Central?

Distribution Lists

Custom Rules

Exceptions

Admin Only

SOPHOS

Chapter Review

Global Settings are used to specify security settings that **apply to all users and devices**.

The sections displayed will depend on the features included in the license. **'Administration'** and **'General'** sections will **always** be listed.

A user with the **Super Admin** role can **manage how administrators receive email alerts**. Distribution lists can be created to **send alerts to users without access** to Sophos Central.

SOPHOS

Here are the three main things you learned in this chapter.

Global settings are used to specify security settings that apply to all users and devices.

The sections displayed will depend on the features included in the license. The **'Administration'** and **'General'** sections will always be listed.

A user with the super admin role can manage how administrators receive email alerts. Distribution lists can be created to send alerts to users without access to Sophos Central.



Sophos Central Protection Licenses and Requirements

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE0530: Sophos Central Protection Licenses and Requirements

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central Protection Features and Requirements

In this chapter you will learn about the server and endpoint protection features available per license, along with the specific system requirements for both servers and endpoints.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Sophos Central is and how to access it
- ✓ Understand the security features of Sophos endpoint and server protection
- ✓ How to view and apply Sophos Central licenses

DURATION **9 minutes**

SOPHOS

In this chapter you will learn about the server and endpoint protection features available per license along with the specific system requirements for both servers and endpoints.

Endpoint Protection

The screenshot shows the Sophos Endpoint Protection - Computers dashboard. On the left, there's a sidebar with sections like ANALYZE, MANAGE PROTECTION (highlighted), and CONFIGURE. Under MANAGE PROTECTION, 'Computers' is selected. The main area displays a table of 8 computers, each with a name, IP, OS, and protection status. A column labeled 'Protection' shows that all 8 computers are protected by 'Intercept X Advanced with XDR'. This column is highlighted with a red border. The table also includes columns for 'Encryption' and 'Last scan'.

Name	IP	OS	Protection	Encryption	Last scan
WinClient5	192.168.1.100	Windows 10 Pro	✓ Intercept X Advanced with XDR	+ Training	1 day ago
MN-5035A1148	192.168.1.101	macOS Monterey 12.5	✓ Intercept X Advanced with XDR	✓ robillywi	1 day ago
Training-W10	192.168.1.102	Windows 10 Enterprise	✓ Intercept X Advanced with XDR	+ Administ	1 day ago
WinClient1	192.168.1.103	Windows 10 Pro	✓ Intercept X Advanced with XDR	+ administ	1 day ago
WinClient4	192.168.1.104	Windows 10 Pro	✓ Intercept X Advanced with XDR	+ administ	1 day ago
WinClient2	192.168.1.105	Windows 10 Pro	✓ Intercept X Advanced with XDR	+ administ	1 day ago
WinClient3	192.168.1.106	Windows 10 Pro	✓ Intercept X Advanced with XDR	+ administ	1 day ago

The threat protection features you benefit from will depend on the license that you apply to your endpoints. This environment shows that all endpoints (Windows and macOS) are protected by Intercept X Advanced with XDR.

Let's look at the licensing options and view which features are included.



Additional information in
the notes

Endpoint Protection Licenses

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
ATTACK SURFACE REDUCTION Web Security, Download Reputation, Web, Peripheral, and Application Control	✓	✓	✓	✓
PRE-EXECUTION PROTECTION Deep learning malware detection, Anti-malware file scanning, Live Protection, Pre-execution Behaviour Analysis, PUA blocking, IPS	✓	✓	✓	✓
STOP RUNNING THREATS DLP, Runtime behaviour analysis, AMSI, MTD, Exploit prevention, active adversary mitigations, CryptoGuard, WipeGuard, Safe Browsing, Enhanced App lockdown	✓	✓	✓	✓

SOPHOS

We will start by looking at the features that are available for endpoints.

All available endpoint protection licenses provide web security and control, download reputation, and the optional controls for peripheral devices and applications. They also include anti-malware scanning, live protection, behaviour analysis, data loss prevention, and potentially unwanted application blocking.

To prevent threats from running, all licenses include AMSI, runtime behaviour analysis, deep learning malware detection, exploit prevention, advanced mitigation protection, CryptoGuard, WipeGuard, safe browsing, and malicious traffic detection.

[Additional Information]

For more information about the features included with each license see: <https://www.sophos.com/en-us/products/endpoint-antivirus/tech-specs.aspx>



Additional information in
the notes

Endpoint Protection Licenses

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
DETECT Live Discover, SQL Query library, suspicious events detection and prioritization, fast access on-disk storage, cross-product data sources and querying, scheduled queries and Data Lake cloud storage (30 days)		✓	✓	✓
INVESTIGATE Threat graphs (root cause analysis) Deep learning malware analysis, Advanced on-demand SophosLabs threat intelligence, forensic data export	✓	✓	✓	✓
REMEDIATE Automated malware removal, Synchronized Security Heartbeat, Sophos Clean Live Response, on-demand endpoint isolation, single click 'Clean and Block'	✓	✓	✓	✓

SOPHOS

Intercept X Advanced with XDR plus MTR Standard and Advanced licenses add to the protection offered by including a wider range of investigative and remediation tools including cross estate threat searching, endpoint isolation, Live Discover, and the Live Response command line interface. They also provide a single-click clean and block feature.

The XDR licenses include Data Lake cloud storage for up to thirty days, which allows you to query endpoints that are offline.

[Additional Information]

For more information about XDR see: <https://www.sophos.com/en-us/mediabinary/PDFs/factsheets/intercept-x-edr.pdf>



Additional information in
the notes

Endpoint Protection Licenses

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
HUMAN-LED THREAT HUNTING AND RESPONSE 24/7 lead-driven threat hunting, security health checks, data retention, activity reporting, adversarial detections, threat neutralization and remediation			✓	✓
24/7 lead-less threat hunting, threat response team lead, direct call-in support, proactive security posture management				✓

SOPHOS

Managed Threat Response (MTR) licenses add an around the clock threat hunting detection and response service that's delivered by a team of Sophos experts.

Sophos analysts respond to potential threats, look for indicators of compromise and provide detailed analysis on events including what happened, when, and where it happened. Additionally, they will investigate how it happened and why.

The same licenses are available for macOS and Windows endpoints.

[Additional Information]

For more information about the features included with each license see: <https://www.sophos.com/en-us/mediabinary/PDFs/factsheets/sophos-intercept-x-mac-ds.pdf>



Additional information in
the notes

Endpoint System Requirements

Platforms	Endpoint Protection	Managed Threat Detection	Intercept X	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with XDR and MTR
Windows 7, 8, 8.1, 10, and 11						
Free disk space	2 GB	4 GB	2 GB	4 GB	8 GB	8 GB
RAM	2 GB	4 GB	2 GB	4 GB	4 GB	4 GB
Cores	2	2	2	2	2	2
MacOS 10.15, 11.12, 11.12 (native), Intel-based MAC (64-bit), Apple Silicon M Series (ARM)						
Free disk space	2 GB	2 GB	2 GB	2 GB	2 GB	2 GB
RAM	2 GB	2 GB	2 GB	2 GB	2 GB	2 GB

SOPHOS

Before you protect your endpoints, you should ensure they meet the system requirements.

This table details the supported platforms and the free disk space and memory required. For Windows endpoints, this changes depending on the license that is applied.

[Additional Information]

A list of all Windows system requirements can be found in knowledge base article [KB-000035144](#).

<https://support.sophos.com/support/s/article/KB-000035144>

The list of the recommended system requirements for MacOS can be found in knowledge base article

[KB-000034670](#). <https://support.sophos.com/support/s/article/KB-000034670>

Server Protection

Server Protection Provides:

- Exclusions for common server roles
- Process exclusions
- Environmental variables
- Server specific policies

The screenshot shows the Sophos Central web interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices' (which is selected and highlighted in blue), 'Global Settings', 'Third-party Connectors', 'Printed Devices', and 'Account Health Check'. The main content area is titled 'Servers' with the sub-header 'View and manage your servers'. It features tabs for 'Computers', 'Mobile devices', 'Servers' (which is selected and highlighted in blue), and 'Unmanaged devices'. Below the tabs are buttons for 'Manage Endpoint Software', 'Add Server', 'Reset health status', and 'Delete', along with an 'Export to CSV' link. A search bar and filter dropdowns for 'Name', 'IP', 'OS', 'Protection', 'Last activity', 'Status', and 'Lockdown status' are present. The main table lists two servers: 'winserver1' (Windows Server 2019 Standard) and 'linact1' (Ubuntu 20.04 LTS). The 'winserver1' row has a red box around it, highlighting the 'Windows Server 2019 Standard' entry. The table includes columns for Name, IP, OS, Protection, Last activity, Status, and Lockdown status. At the bottom, a footer note says 'Last updated: Jun 17, 2022, 3:57 PM'.

Name	IP	OS	Protection	Last activity	Status	Lockdown status
winserver1	172.16.18.10	Windows Server 2019 Standard	Intercept X Advanced for Server with XDR	Jun 17, 2022, 2:33 PM	Training	N/A (available)
linact1	172.38.18.130	Ubuntu 20.04 LTS	Server Protection	Mar 29, 2022, 3:28 AM	Normal	Lock Down

Server protection is designed specifically for servers. Exclusions for common server roles are automatically applied. Process exclusions and environmental variables can be added to server policies which provide a greater level of control for protected server security.

Server protection is available for Windows and Linux servers. It also includes virtual environment protection for VMWare ESXi and Microsoft Hyper-V, as well as support for servers hosted by Amazon Web Services (AWS) and Microsoft Azure.

Server Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
MANAGEMENT Multiple policies, controlled updates		✓	✓	✓	✓	✓
ATTACK SURFACE REDUCTION Application, peripheral and web control, application whitelisting		✓	✓	✓	✓	✓
Download reputation, web security	✓	✓	✓	✓	✓	✓
PRE-EXECUTION PROTECTION Deep learning malware detection, anti-malware file scanning, Live Protection, behaviour analysis, PUA blocking, IPS	✓	✓	✓	✓	✓	✓

SOPHOS

All server protection licenses include standard malware detection, file scanning protection and live protection. The advanced licenses include controlled updates, policy control, web protection, control policies for peripherals, applications, web, and application whitelisting.

The features supported on Linux Servers are highlighted in blue in the tables shown.

Currently Linux has two deployment options:

- Sophos Server Protection for Linux gives access to the features highlighted in the table
- Sophos Anti-Virus for Linux is a legacy product

Please note that the two deployment options cannot be used together.

Server Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
STOP RUNNING THREATS DLP		✓	✓	✓	✓	✓
Behaviour analysis, AMSI, MTD, Exploit prevention, Active Adversary mitigations, CryptoGuard, WipeGuard, Safe Browsing, Enhanced Application Lockdown	✓	✓	✓	✓	✓	✓
DETECT Live Discover, SQL Query library, on-disk data storage, cross product data sources, prioritised detection lists, Sophos Data lake, scheduled queries, container runtime visibility and detections			✓	✓	✓	✓

SOPHOS

All server protection licenses include the threat protection features that detect and stop active threats from running. Please note that data loss prevention is included in all advanced server licenses.

The investigative detection features including Live Discover, on-disk data storage, Sophos Data Lake and container running visibility and detection are included in licenses that include XDR and MTR.

Server Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
INVESTIGATE Threat Graph (Root cause analysis)		✓	✓	✓	✓	✓
Deep learning malware analysis, advanced on-demand SophosLabs threat intelligence, forensic data export, AI-guided investigation			✓	✓	✓	✓
REMEDIATE Automated malware removal, Synchronized Security Heartbeat, Sophos Clean	✓	✓	✓	✓	✓	✓
Live Response , Server isolation, single-click 'clean and block', Container runtime visibility and detections			✓	✓	✓	✓

SOPHOS

All licenses include the automated removal of detected threats, please note that some features are platform specific.

We recommend that you check the licensing guides available. As an example, the XDR features supported by Server Protection for Linux are not available for Sophos Anti-Virus for Linux.



Additional information in
the notes

Server Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
CONTROL Synchronized Application Control, Update Cache and Message Relay, Automatic Scanning Exclusions	✓	✓	✓	✓	✓	✓
File Integrity Monitoring			✓	✓	✓	✓

SOPHOS

The control features are included in all licenses with the exception of File Integrity Monitoring which is included in licenses that include XDR and MTR.

[Additional Information]

For more information about the server licenses available and the features that come with each license please view the following documents. https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/Server_protection_licensing_guide-na.pdf

Workload Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
CLOUD ENVIRONMENTS						
Monitoring (AWS, Azure, GCP, Kubernetes, IaC and Docker Hub registries)		One per provider	One per provider	Unlimited	One per provider	On per provider
Security monitoring		Daily scans	Daily scans	Scheduled, daily and on-demand scans	Daily scans	Daily scan
Asset inventory, advanced search capabilities, AI-powered anomaly detection, SophosLabs Intelix malicious traffic alerts, email alerts, AWS and Azure Native Service Integrations, Sophos Intercept X agent discovery, automatic Sophos agent removal	✓	✓	✓	✓	✓	✓

SOPHOS

The server protection licenses can be applied to cloud environments. This table shows the features that are included in each license for cloud environments.

Workload Protection Licenses

Features	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Compliance policies and reports		CIS Benchmarks	CIS Benchmarks	CIS Benchmarks, ISO 27001, EBU R 143, REDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, Sophos best practices	CIS Benchmarks	CIS Benchmarks
Custom policies				✓		
Network visualization, IAM visualization, spend monitor, alert management, SIEM integrations, Rest API, Infrastructure as code template scanning, environment access control, Container image scanning		✓	✓	✓	✓	✓

SOPHOS

This table shows the features that are included in each license for cloud environments.



Additional information in
the notes

Linux Protection Licenses

Features	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Linux Protection Agent Including malware scanning, exploit prevention, and file scanning	✓	✓	✓
Linux Sensor Integrate Linux and container runtime threat detections with your existing threat response tools via API		✓	✓
Cloud Infrastructure Security Monitor cloud security posture to prevent security and compliance risks	✓	✓	✓
XDR Extended detection and response		✓	✓
Managed Threat Response 24/7/365 threat hunting and response service			✓

SOPHOS

As well as acting as a protection agent Linux protection can also be installed as a sensor. Sophos Linux Sensor uses APIs to integrate runtime threat detections, in host or container environments, with your existing threat response tools. This provides a wider range of detections, control to create custom rule sets, and configuration options to tune host resource utilization.

[Additional Information]

For more information about the versions of Central Server for Linux see: <https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/central-server-for-linux.pdf>

For more information about installation of Linux Sensor see:

<https://docs.sophos.com/esg/sls/help/en-us/gettingStarted/installSensor/index.html>

Managed Threat Response

Features	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
24/7 lead-driven threat hunting, security health checks, data retention, activity reporting, adversarial detections, threat neutralization and remediation	✓	✓
24/7 lead-less threat hunting, threat response team lead, direct call-in support, proactive security posture management, ransomware file protection,		✓

SOPHOS

Sophos Managed Threat Response (MTR) provides around the clock threat hunting, detection, and response delivered by an expert team as a fully managed service.

This table displays the features that are included for standard and advanced MTR licenses.



Additional information in
the notes

Server System Requirements

Platforms	Server Protection	Managed Threat Detection	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with XDR and MTR
Windows Server 2008 R2, SBS 2011, 2012, 2012 R2, 2016, 2019, and 2022					
Free disk space	5 GB	8 GB	8 GB	10 GB	10 GB
RAM	4 GB	8 GB	8 GB	8 GB	8 GB
Cores	2	2	2	2	2
Amazon Linux, Debian 9 and 10, Oracle Linux 7 and 8, Red Hat Enterprise Linux 7, 8 and 9, SUSE Linux Enterprise Server 12 and 15, Ubuntu 18, 20.04 and 22.04 LTS					
Free disk space	2 GB	2 GB	2 GB	2 GB	2 GB
RAM	2 GB	2 GB	2 GB	2 GB	2 GB

SOPHOS

Before you protect servers, you should ensure they meet the system requirements.

This table details the supported platforms and the free disk space and memory required. For Windows operating systems, this changes depending on the license that is applied.

We recommend viewing the system requirements regularly as these will change over time.

[Additional Information]

Windows system requirements **KB-000034920**. <https://support.sophos.com/support/s/article/KB-000034920>

Recommended system requirements for SAV for Linux **KB-000033389**.

<https://support.sophos.com/support/s/article/KB-000033389>

Recommended system requirements for SPL **KB-000039161**.

<https://support.sophos.com/support/s/article/KB-000039161>



Additional information in
the notes

Intercept X Essentials

Aimed at small organizations that want the best protection but don't require full control and management capabilities

Includes the most powerful features from Intercept X such as deep learning AI, anti-ransomware and anti-exploit techniques

Only provides access to base policies. No app control, web control, peripheral control, DLP, threat cases or controlled updates

Essentials and Advanced/EDR licenses are not permitted in the same estate

SOPHOS

Sophos also offers Intercept X Essentials and Intercept X Essentials for Server.

These products are aimed at small organizations that want the best protection but don't require full control and management capabilities. They include the most powerful defensive features from Intercept X such as deep learning, anti-ransomware, and anti-exploit techniques. However, these licenses do not include application control, web control, peripheral control, data loss prevention, threat graphs or controlled updates.

If you require multiple, configurable policies or control capabilities, the Intercept X Advanced for Server license or higher should be used. Please note that a mixture of Intercept X Essentials and Intercept X Advanced licenses are not permitted in the same estate.

[Additional Information]

For information about Intercept X Essentials please view the FAQ here: <https://www.sophos.com/en-us/mediabinary/pdfs/factsheets/sophos-intercept-x-essentials-faq.pdf>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of these features are only available with Intercept X Advanced with XDR?

Endpoint Isolation

CryptoGuard

Root Cause Analysis

Malicious Traffic Detection

Live Response

Data Lake

SOPHOS

Question 2 of 3

What are the minimum hardware requirements to install Intercept X Advanced with XDR Server Protection on Windows?

Disk space: 8 GB
RAM: 4 GB
Cores: 2

Disk space: 8 GB
RAM: 8 GB
Cores: 2

Disk space: 10 GB
RAM: 8 GB
Cores: 2

Disk space: 10 GB
RAM: 8 GB
Cores: 4



Question 3 of 3

True or False: Intercept X Essentials only provides access to Base Policies.

True

False

SOPHOS

Chapter Review

The **threat protection features** you benefit from will **depend on the license** that you apply to your endpoints and servers.

Server Protection is designed specifically for servers. Process exclusions and environmental variables can be added to server policies which provide a greater level of control.

Intercept X Essentials is aimed at small organizations that want the **best protection** but don't require full control and management capabilities.

SOPHOS

Here are the three main things you learned in this chapter.

The threat protection features you benefit from will depend on the license that you apply to your endpoints and servers.

Server protection is designed specifically for servers. Process exclusions and environmental variables can be added to server policies which provide a greater level of control.

Intercept X Essentials and Intercept X Essentials for Server are aimed at small organizations that want the best protection but don't require full control and management capabilities.



An Introduction to Users in Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE1005: An Introduction to Users in Sophos Central

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Introduction to Users in Sophos Central

In this chapter you will learn how users can be added to Sophos Central, and how they are used for endpoint and server protection.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Know what Sophos Central is and how to login

DURATION **6 minutes**

SOPHOS

In this chapter you will learn how users can be added to Sophos Central, and how they are used for endpoint and server protection.



Additional information in
the notes

Sophos Central Users

Policies and Devices

Devices are assigned to users

Policies are assigned to users
and applied to their devices

Administration

Users can be assigned
administrative roles to manage
selected aspects of Sophos
Central

SOPHOS

People are a key element of management in Sophos Central endpoint and server protection.

For endpoint protection, policies are assigned to users and not devices. When a user logs into a device, the device is assigned to them, and their user policies are applied.

Users are also used for managing administration in Sophos Central, delegating access to selected aspects of the Sophos Central Admin console.

[Additional Information]

<https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/index.html>

Methods for Adding Users

Add users **manually**

Import users from a **CSV file**

Synchronize users from a **directory service**

The **current user** is added during the device installation

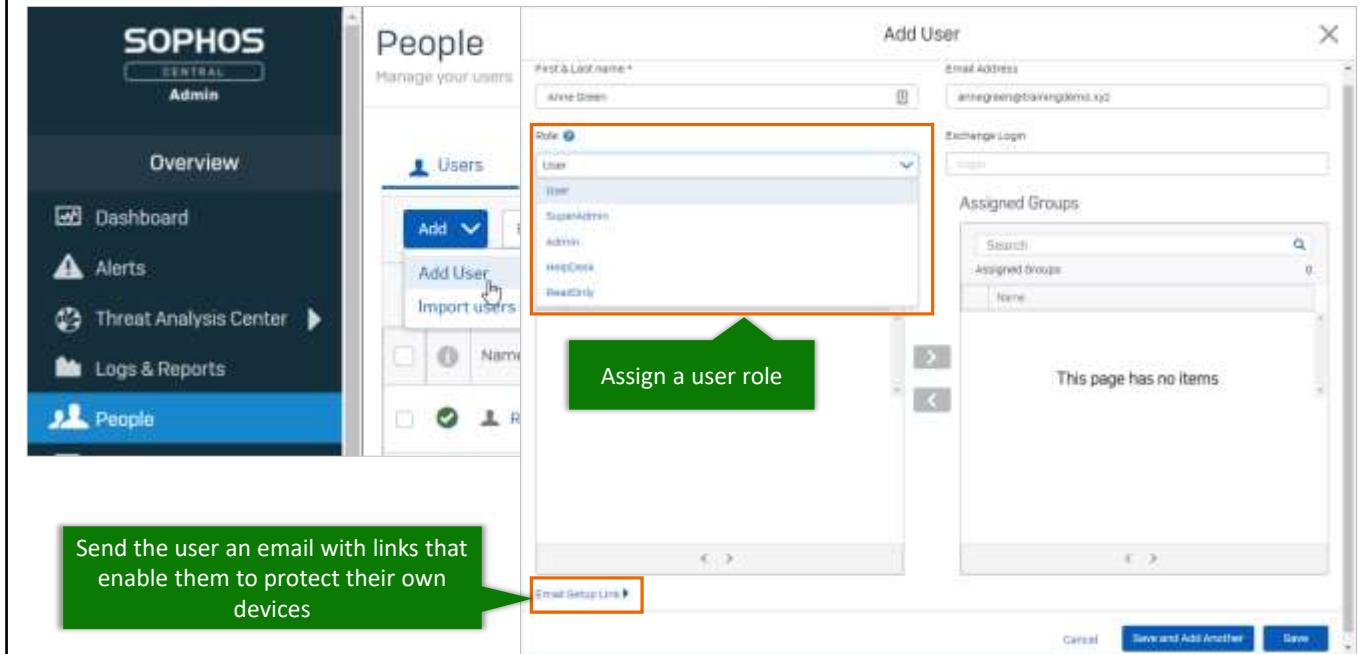
When a **new user** logs into a managed device

SOPHOS

There are five ways users can be added to Sophos Central; they are:

- Creating users manually
- Importing users using a CSV file
- Synchronizing users from a directory service, either Active Directory or Azure Active Directory
- Users are created automatically during a device installation
- Users are created automatically when a user logs into a managed device

Adding Users Manually



Let's start by looking at how to manually add a user to Sophos Central.

Users are managed in the **People** section of the admin console. Here, you can add an individual user and protect them by selecting **Add > Add User**.

Enter the users first and last name along with their email address and then select an administration role for the user. The default role assigned will always be 'user'. Next you can select to enter the 'Exchange Login' details for the user you are adding. These details can be used to configure email access on mobile devices.

If you have groups configured, you can optionally select which groups you would like to add the user to. To enable users to protect their own devices, click **Email Setup Link**. When a user downloads and installs the software, their device is automatically associated with them as a user.

Once the user is saved, they will appear in the 'People' list.

Importing Users from a CSV file

The screenshot shows the 'Import users from CSV' dialog box. On the left, there is a text area with instructions and examples. A green callout box points to two links: 'Blank template with header' and 'Template with example data'. On the right, there are fields for 'CSV File*', a 'Browse' button, and several checkboxes. One checkbox is checked ('Create new groups'). Another checkbox is unchecked ('Give users access to Sophos Central Self Service'). Below these are notes about file size and encoding. At the bottom are 'Cancel' and 'Add' buttons, and a 'SOPHOS' logo.

The csv to import new users requires setting of 'name' and 'email'.
As optional fields you can add 'manager email', 'exchange login' and 'group'.
If you have users who are in several groups you can add additional 'group' fields followed by a number. For example 'group1' and 'group2'.
As a formatting example you can have a look at the following examples:

- Blank template with header
- Template with example data

To view formatting examples, use the templates provided

CSV File*

Create new groups

Give users access to Sophos Central Self Service.
Users will get an email that tells them how to sign in.

Max file size is 2MB
CSV file should be utf-8 encoded

SOPHOS

Importing users using a CSV file allows you to add users in bulk. To import users from a CSV file, navigate to **People** then click **Add > Import users from CSV**.

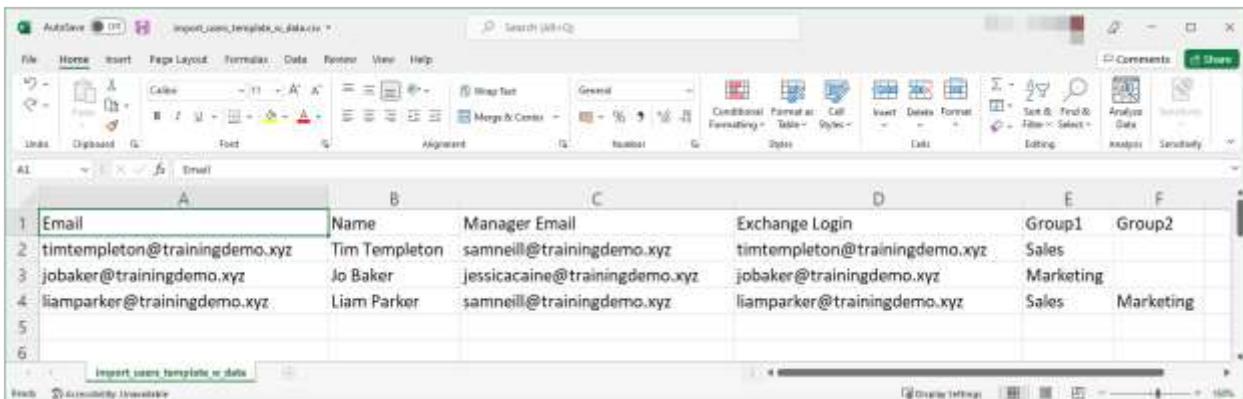
To ensure you include the correct details for your users you can download a template. There are two versions of the template, a blank template with only the header information, and a template with an example.

The 'Create new groups' tick box can be selected if you are including user groups in the CSV file that are not yet created in Sophos Central.

The 'Give users access to Sophos Central Self Service' tick box will send a registration email for the Sophos Central self-service portal to each imported user.

Click **Browse** to select your CSV file and click **Add**.

Importing Users from a CSV file



	Email	Name	Manager Email	Exchange Login	Group1	Group2
1	timtempleton@trainingdemo.xyz	Tim Templeton	samneill@trainingdemo.xyz	timtempleton@trainingdemo.xyz	Sales	
2	jobaker@trainingdemo.xyz	Jo Baker	jessicacaine@trainingdemo.xyz	jobaker@trainingdemo.xyz	Marketing	
3	liamparker@trainingdemo.xyz	Liam Parker	samneill@trainingdemo.xyz	liamparker@trainingdemo.xyz	Sales	Marketing
4						
5						
6						

SOPHOS

Here is an example of a CSV file with some example users.

Your CSV file can include the email address of the manager for each of your users. If there is a manager who is not already a user in Sophos Central, a user is created. This means the number of users imported may exceed the number of rows in the file.

If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in the imported file. However, if the existing user in Sophos Central is managed through a directory service, the user is skipped during import, and no changes are made to the user account.

Simulation: Creating Users in Sophos Central



In this simulation you will manually create users in Sophos Central and upload users using a CSV file.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/CreatingUsers/1/start.html>

SOPHOS

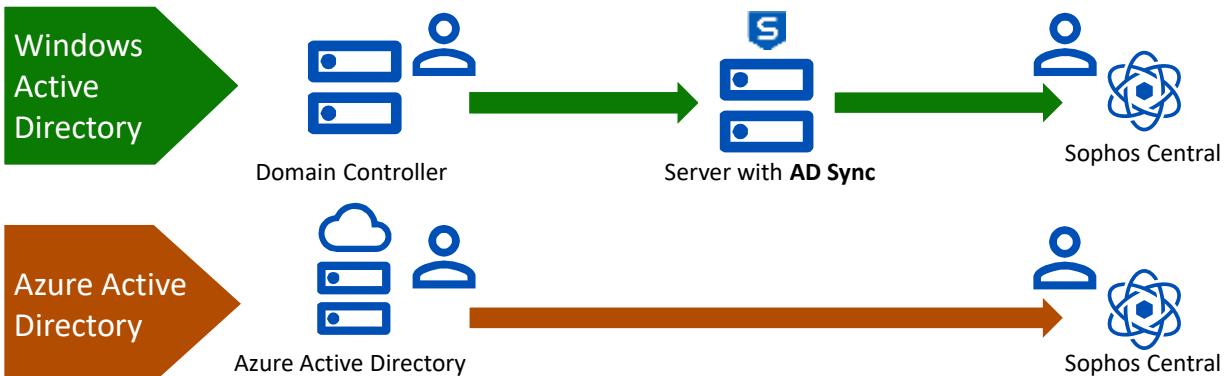
Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/CreatingUsers/1/start.html>

Synchronizing from a Directory Service



We recommend installing and configuring the directory service before you start deploying protection

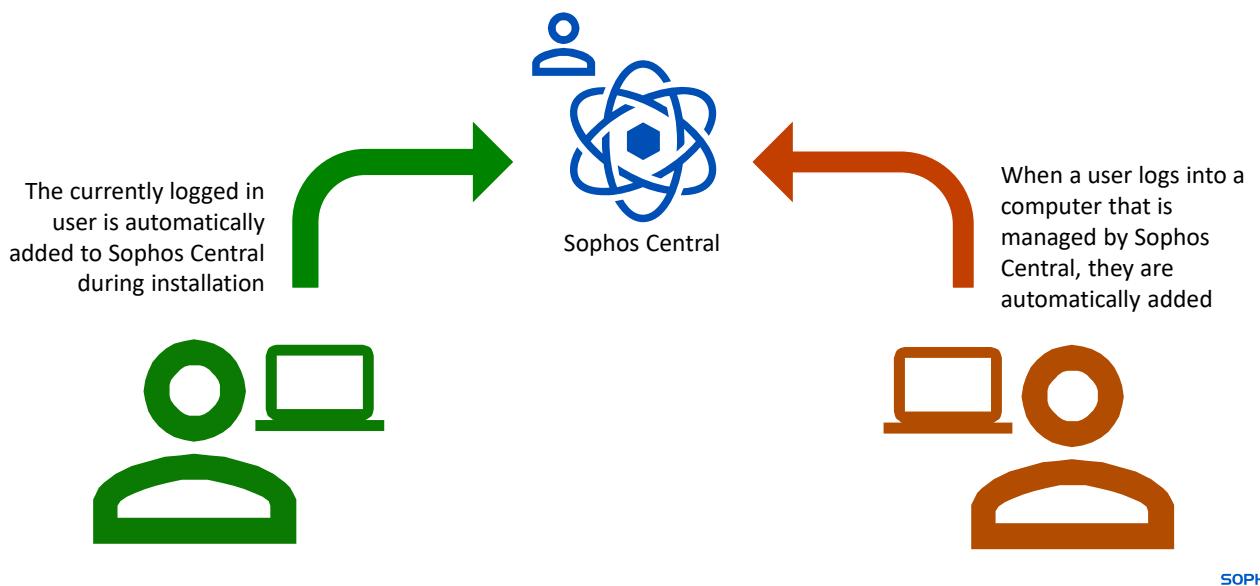
SOPHOS

You can automate the adding and removing of users and groups in Sophos Central if you are using either Windows Active Directory or Azure Active Directory. Sophos Central can be configured to perform a regular one-way synchronization, from the directory service to Sophos Central. This ensures that users in Sophos Central match those configured in your organization's directory.

We recommend installing and configuring your selected directory service tool before you start deploying Sophos protection to any devices, so that you can preconfigure policies and apply them to users and groups.

Please note that other directory services such as OpenLDAP and eDirectory are not currently supported.

Adding Users Automatically



Users will be automatically added to Sophos Central in two scenarios. First, during the installation of the Sophos agent on a device if a user is logged onto that device. Second, when a new user logs onto a device that is already protected by Sophos Central.

Video Demo: Automatic Users



In this short demo you will see how users are added automatically to Sophos Central.

LAUNCH DEMONSTRATION

CONTINUE

<https://training.sophos.com/ce/demo/AutomaticUsers/1/play.html>

SOPHOS

Please watch this video demonstration.

Click **Launch Demonstration** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/demo/AutomaticUsers/1/play.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of the following directory services are supported by Sophos Central?

Azure Active Directory

OpenLDAP

eDirectory

Windows Active Directory

SOPHOS



Question 2 of 3

In Sophos Central Endpoint Protection, what do you apply policies applied to?

Users

Computers

SOPHOS

Question 3 of 3

You have created a CSV to bulk upload users, shown below. If these are the first users you are adding to Sophos Central, how many users will be created by importing this CSV file? (enter your answer numerically)

1. Email	Name	Manager Email	Exchange Login	Group1	Group2
timtempleton@trainingdemo.xyz	Tim Templeton	samneill@trainingdemo.xyz	timtempleton@trainingdemo.xyz	Sales	
jobaker@trainingdemo.xyz	Jo Baker	jessicacaine@trainingdemo.xyz	jobaker@trainingdemo.xyz	Marketing	
liamparker@trainingdemo.xyz	Liam Parker	samneill@trainingdemo.xyz	liamparker@trainingdemo.xyz	Sales	Marketing

Chapter Review

Sophos Central **endpoint** policies are assigned to **users**, and for **administration**, users have access assigned to selected parts of the **console**.

You can **manually** create users, **import** them using a CSV file, **synchronize** users from a directory service, or they are added **automatically** during installation or when a new user logs into a managed endpoint.

Sophos Central supports synchronizing users from **Windows Active Directory** and **Azure Active Directory**.

SOPHOS

Here are the main things you learned in this chapter.

Sophos Central endpoint policies are assigned to users, and for administration, users have access assigned to selected parts of the console.

You can manually create users, import them using a CSV file, synchronize users from a directory service, or they are added automatically during installation or when a new user logs into a managed endpoint.

Sophos Central supports synchronizing users from Windows Active Directory and Azure Active Directory.



Getting Started with Sophos Central User Management

Sophos Central Endpoint and Service Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE1010: Getting Started with Sophos Central User Management

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central User Management

In this chapter you will learn how to manage users in Sophos Central using groups, how to setup and manage your multi-factor authentication settings, and how to create API credentials.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to login to Sophos Central
- ✓ How users are added to Sophos Central

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how to manage users in Sophos Central using groups, how to setup and manage your multi-factor authentication settings, and how to create API credentials.

People

The screenshot shows the Sophos Central 'People' management interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People' (which is selected and highlighted in blue), 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Under 'MY PRODUCTS', there are links for 'Endpoint Protection', 'Server Protection', and 'Mobile'. The main content area is titled 'People' with the subtitle 'Manage your users'. It features a navigation bar with 'Users' (selected) and 'Groups', and buttons for 'Add', 'Import Setup Link', 'Delete', 'Set up directory service', and 'Export to CSV'. A search bar is also present. The main list displays users with columns for 'Name', 'Email', 'Exchange Login', and 'Last Active'. A tooltip 'Synchronized from a directory' points to the row for 'Lucy Fox', which has a blue circular icon with a white refresh symbol next to it. Another tooltip 'Central-managed' points to the row for 'Help Desk', which has a green circular icon with a white person symbol next to it. The list shows entries for Lucy Fox, John Smith, Josh Noble, Help Desk, and Ed Korsgaard.

Name	Email	Exchange Login	Last Active
Lucy Fox	lfox@sophostraining.xyz	lfox	Nov 17, 2021 2:30 PM
John Smith	jsmith@sophostraining.xyz	jsmith	Nov 17, 2021 2:30 PM
Josh Noble	jnoble@ad.sophostraining.xyz	jnoble@ad.sophostraining.xyz	Nov 29, 2020 4:10 PM
Help Desk		Add Exchange Login	Nov 9, 2020 10:10 AM
Ed Korsgaard	e.korsgaard@sophostraining.xyz	Add Exchange Login	

Once users have been added to Sophos Central, they will be listed on the 'People' page.

You will notice that there are two different icons for users, one to indicate that the user is synchronized from a directory, and the other for Central-managed users that have been added manually or automatically.

User Details Summary

The screenshot shows the Sophos Central interface for managing users. On the left, a dark sidebar lists various management categories like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People (which is selected), Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under MY PRODUCTS, there are links for Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'WINCLIENT2\Sophos' under 'Users / WINCLIENT2\Sophos'. It displays a user profile icon with a green checkmark, the name 'WINCLIENT2\Sophos', and options to 'Edit' or 'Delete User'. Below this, it shows 'Exchange Login' status as 'None'. A navigation bar at the top right includes 'Help', 'UK Training', and 'Sophos UK - Super Admin'. The main content is divided into four tabs: SUMMARY (selected), DEVICES (1), EVENTS, and POLICIES. The SUMMARY tab shows a section for 'Recent Events' with five entries from November 14, 2022, detailing updates and URL blocks. It also shows a summary for 'Devices (1)' with one entry for 'WinClient2' running Windows 10, along with an 'Actions' button and a 'Mailboxes' link.

Clicking on a user will open the details page for that user; this is split into four tabs; summary, devices, events, and policies.

The **SUMMARY** tab contains an overview of recent events, devices, mailboxes, groups and logins.

User Details Devices

The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People' (which is selected), 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Under 'MY PRODUCTS', options like 'Endpoint Protection', 'Server Protection', 'Mobile', 'Encryption', 'Wireless', 'Email Security', and 'Firewall Management' are listed. The main content area is titled 'WINCLIENT2\Sophos' and shows a summary for the user 'WINCLIENT2\Sophos'. It displays a green checkmark icon next to a user profile icon, a computer monitor icon with a green checkmark, and the text 'WinClient2 Windows 10'. Below this, there are links for 'Change Sigin' and 'Edit / Delete User'. A message at the bottom says 'You can protect additional devices for WINCLIENT2\Sophos from the Protect Devices page.' At the top right, there are 'Help', 'UK Training', and 'Sophos UK - Super Admin' links. A 'Actions' dropdown menu on the right contains 'Update Now', 'Scan Now', 'Diagnose', and 'Delete' options.

The **DEVICES** tab displays all the devices the user has associated to them. It allows you to perform actions on the devices.

For example, on an endpoint you can initiate a scan or update, gather troubleshooting information, or delete the device.

User Details Events

The screenshot shows the Sophos Central interface for managing users. On the left, a sidebar lists various management categories like Dashboard, Alerts, Threat Analysis Center, and People. The 'People' section is currently selected. The main area displays user details for 'WINCLIENT2\Sophos'. Below this, a table lists '72 Events' from Nov 14, 2022, to Nov 3, 2022. The events are categorized by device (e.g., WinClient2) and include types such as 'Update succeeded', 'blocked due to category', and 'Policy in compliance'.

SEV	TYPE	DATE	EVENT	device
1	Info	Nov 14, 2022 10:31 AM	Update succeeded	WinClient2
1	Info	Nov 14, 2022 10:26 AM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.171.37 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 4, 2022 5:17 PM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 4, 2022 5:17 PM	https://13.107.42.16/ blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 4, 2022 1:15 PM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 4, 2022 9:57 AM	Policy in compliance: Exploit Detection	WinClient2
⚠	Warning	Nov 4, 2022 9:30 AM	Policy non-compliance: Exploit Detection	WinClient2
1	Info	Nov 4, 2022 3:15 AM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 4, 2022 2:51 AM	Update succeeded	WinClient2
1	Info	Nov 3, 2022 4:14 PM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 3, 2022 8:15 AM	https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	WinClient2
1	Info	Nov 3, 2022 2:51 AM	Update succeeded	WinClient2

The **EVENTS** tab displays all the events logged for the user and their devices. These can be filtered by time.

User Details Policies

The screenshot shows the Sophos Central interface. On the left, the navigation menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', **People**, 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Under 'MY PRODUCTS', there are links for 'Endpoint Protection', 'Server Protection', 'Mobile', 'Encryption', 'Wireless', 'Email Security', and 'Firewall Management'. The main content area is titled 'WINCLIENT2\Sophos' and shows a user profile for 'WINCLIENT2\Sophos'. Below the profile are buttons for 'Change login name' and 'Edit / Delete user'. At the top right are links for 'Help', 'UK Training', and 'Sophos UK - Super Admin'. The top navigation bar has tabs for 'SUMMARY', 'DEVICES (1)', 'EVENTS', and 'POLICIES'. The 'POLICIES' tab is selected, displaying a table of policies applied to the user. The table has two columns: 'TYPE' and 'NAME'. The policies listed are:

TYPE	NAME
Email Security: Email Security	Base Policy - Email Security
Email Security: Data control	Base Policy - Data control
Encryption: Device Encryption	Base Policy - Device Encryption
Endpoint Protection: Application Control	Base Policy - Application Control
Endpoint Protection: Data Loss Prevention	Base Policy - Data Loss Prevention
Endpoint Protection: Windows Firewall	Base Policy - Windows Firewall
Endpoint Protection: Peripheral Control	Base Policy - Peripheral Control
Endpoint Protection: Threat Protection	Example 1
Endpoint Protection: Update Management	Base Policy - Update Management
Endpoint Protection: Web Control	Base Policy - Web Control

The **POLICIES** tab displays the policies that apply to the user.

People Groups

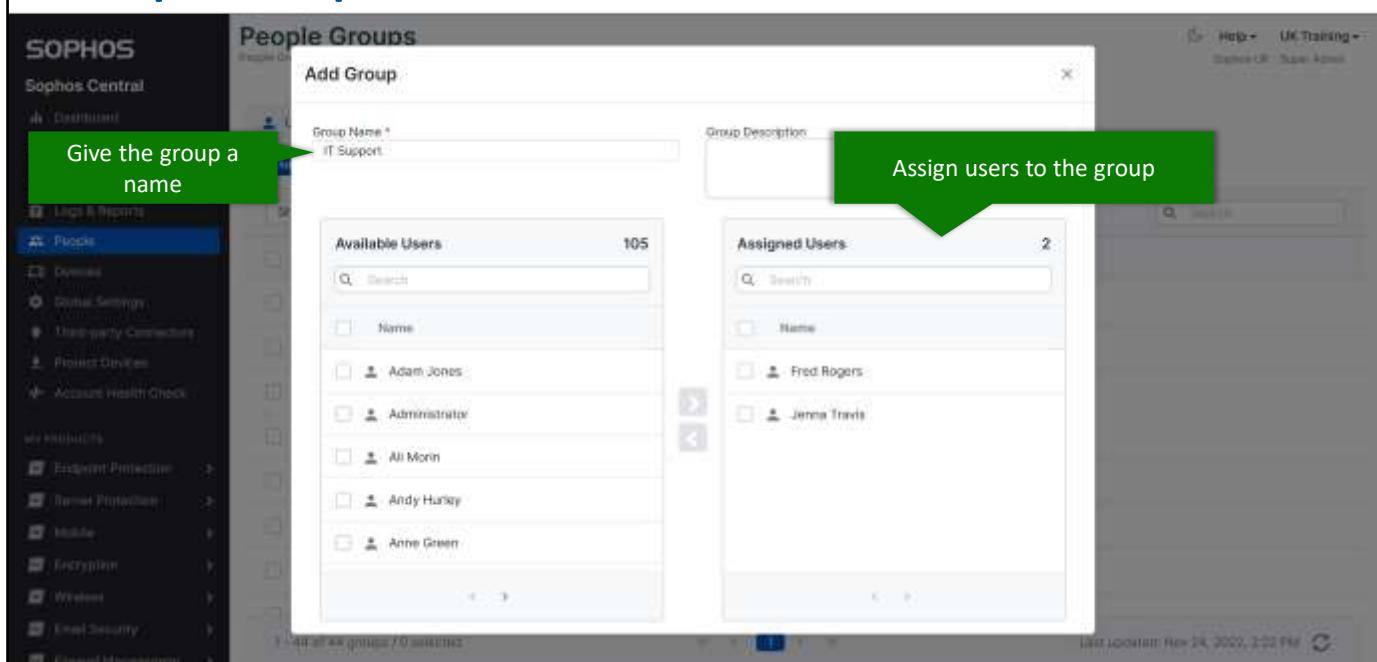
The screenshot shows the 'People Groups' section of the Sophos Central interface. On the left, a sidebar lists various management categories like Endpoint Protection, Server Protection, and Email Security. The 'People' category is selected. The main area is titled 'People Groups' and contains a filter dropdown labeled 'Show all groups' with options: 'Show all groups', 'Show Sophos Central-managed groups', and 'Show Active Directory groups'. Below the filter are two sections: 'Central managed' (with a green icon) containing 'Managers (SOPHOS) [6]' and 'Active Workers [1]' (highlighted with a green box); and 'Synchronized from a directory' (with a blue icon) containing 'Protected Users (SOPHO STRA)' and 'Head-only Domain Controllers'. A green arrow points from the 'Central managed' section to the 'Active Workers' group. A blue arrow points from the 'Synchronized from a directory' section to the 'Protected Users' group. A green callout box labeled 'Filter user groups' points to the filter dropdown. A blue callout box labeled 'Central managed' points to the 'Central managed' section. A blue callout box labeled 'Synchronized from a directory' points to the 'Synchronized from a directory' section.

People groups simplify applying policies to users with the same requirements. Groups can be manually created in Sophos Central or synchronized from an active directory service. As with users, groups have different icons to indicate how they are being managed.

At the top of the page, you can filter the user groups to show all groups, or only Central-managed groups or Active Directory groups.

Users can be a member of multiple groups.

People Groups

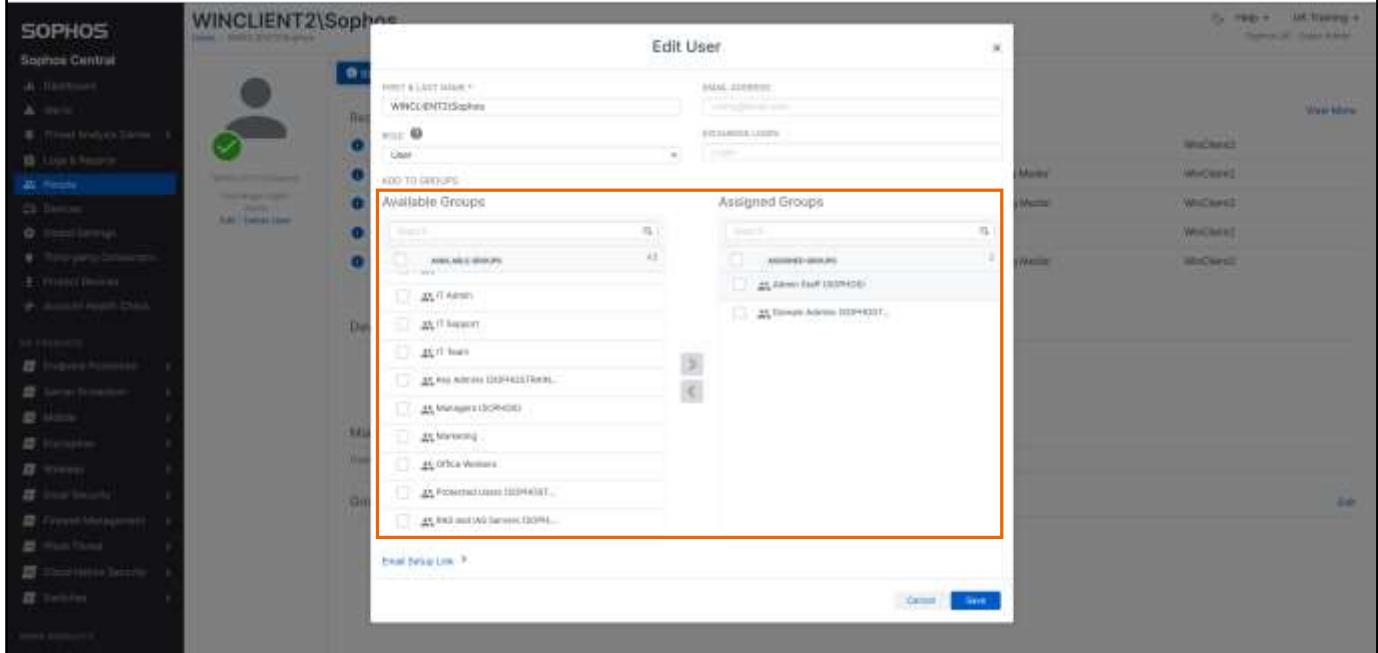


To create a new Central managed group, navigate to **People > Groups > Add Group**.

Enter the group name and optionally a description for the group.

Move any users you wish to be a member of the group from the 'Available Users' list to the 'Assigned Users' list and click **Save**.

Edit User

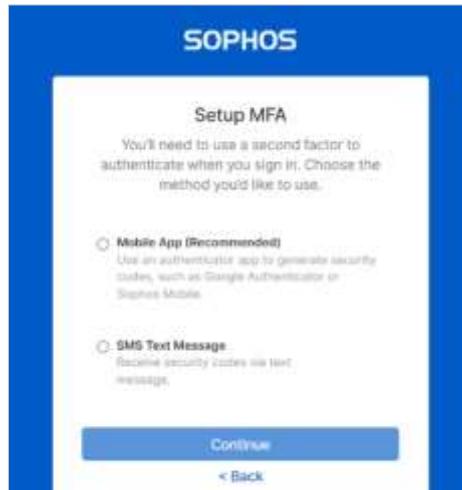


You can modify the groups a user is assigned to by editing the user.

Select the user from the **People > Users** list. Under the username click **Edit**. You can assign the user to multiple groups.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) improves authentication security by requiring two or more factors of authentication.



MFA is required for all administrators in Sophos Central

Multi-factor authentication, or MFA, improves security by requiring two or more factors of authentication to login to Sophos Central. Multi-factor authentication is required for all administrators in Sophos Central.

Your username and password are required for authentication, this is information you know. As a second factor of authentication, you need to use something you have. This can be a phone, which is proven by entering a one-time code that is sent via an SMS text message or an electronic token, which is proven by entering a one-time code from an authenticator app.

If you lose your phone or the authenticator app, you can use your email address with a PIN code as a backup authentication method; however, the primary authentication method must be either SMS or an authenticator app.

How to Manage your MFA Settings

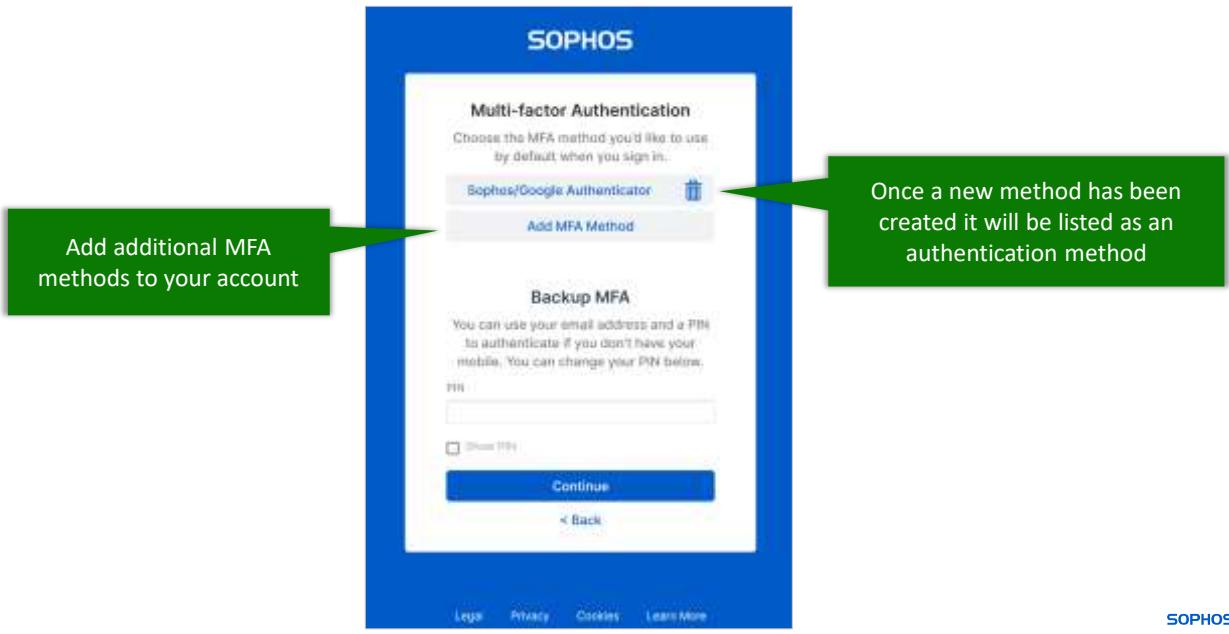
The screenshot shows the Sophos Central Admin console interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People (which is selected and highlighted in blue), and Devices. Below that, under 'MY PRODUCTS', are Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'People' and 'Manage your users'. It has tabs for 'Users' (selected) and 'Groups'. Below these are buttons for 'Add', 'Email Template', and 'Delete'. A search bar and a dropdown for filtering users ('All users') are also present. The main list displays several user entries with columns for Name, Email, Exchange Login status, and Last updated date. One entry, 'TRAININGDEMO\administrator', has a yellow warning icon next to it. At the bottom, it says '1-107 of 107 users / 0 selected' and shows a page navigation bar. In the top right corner, there's a user menu with options like Help, Account Details, Licensing, Early Access Programs, About, and Log Out. The 'Manage Login Settings' option is highlighted with a red box.

Name	Email	Exchange Login	Last updated
TRAININGDEMO\administrator		Add Exchange Login	Nov 14, 2022 1:
TRAININGDEMO\administrator		Add Exchange Login	Nov 14, 2022 1:
WINCLIENT5\TrainingDemo		Add Exchange Login	Nov 14, 2022 1:
TRAINING-W10\Administrator		Add Exchange Login	Nov 2, 2022 8:
DESKTOP-CRQDC8A\dan		Add Exchange Login	Oct 12, 2022 5:

You can update your multi-factor authentication settings from the user menu in the top-right of the admin console.

Select **Manage Login Settings**.

How to Change MFA Type



Here you can see the multi-factor authentication methods you have configured, add new methods, remove old devices, or update the PIN used for the email backup authentication.

Adding new authentication methods follows the same process as the initial multi-factor authentication configuration.

Simulation: Configuring MFA



In this simulation you will configure multi-factor authentication for a new Sophos Central account, then add another authentication method.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/MFA/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/MFA/1/start.html>

API Credentials

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected. The main content area is titled 'API Credentials Management' and displays a table of existing credentials. The table columns are 'NAME', 'CREDENTIAL ID', 'ROLE', and 'CREATED ON'. The table data includes:

NAME	CREDENTIAL ID	ROLE	CREATED ON
ADSyncUtil	dc72aa68-ca09-aaaa-a672-1f22311c8caa	Service Principal Super Admin	Apr 17, 2020
Rob	29997626-9603-4392-9ed7-e43b604324d0	Service Principal Super Admin	Aug 07, 2020
AD Sync	0e136742-600c-4a75-9a63-d96a321f982c	Service Principal Super Admin	Mar 10, 2021
xdr api	24644f57-4653-4016-aa40-6cfbed939174	Service Principal Super Admin	May 05, 2021
AD Synchronization	5b250345-9994-4483-a107-29e0339a09948	Service Principal Super Admin	Dec 01, 2021
ad sync test	166bb07e-2e07-4c16-9bbd-3a60c07791a84	Service Principal Directory Sync	Dec 22, 2021
Data Lake	6f79e388d-fef2-47a9-8589-51ca39a9f538	Service Principal Super Admin	Aug 28, 2022

A note at the bottom of the table states: 'Note: You may create up to 10 credentials.' A blue 'Add Credential' button is located in the top right corner of the table header.

Super admin permissions are required to create API credentials

To use the Sophos Central APIs and the Windows Active Directory Sync tool, you need to create a set of API credentials. These are separate to users in Sophos Central.

API credentials have a credential ID and secret that work like a username and password, as well as a role to manage the permissions and an expiry date.

Only administrators with the super admin role can add and manage API credentials in Sophos Central. API credentials are managed in **Global Settings > API Credentials Management**.

You can have up to 10 API credentials in Sophos Central.

API Credentials

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected. The main content area displays the 'API Credentials Management' screen, specifically the 'Add credential' dialog. The dialog has fields for 'Credential name*' (set to 'Active Directory Sync'), 'Description' (empty), and a dropdown for 'Role*' which is currently set to 'Service Principal Super Admin'. A green callout box points to this role selection with the text 'Select the role for the API credential permissions'. In the background, a list of existing credentials is visible, each with a name, role, and creation date.

Role	Created On
Super Admin	Apr 17, 2020
Super Admin	Aug 07, 2020
Super Admin	Mar 10, 2021
Super Admin	May 05, 2021
Super Admin	Dec 01, 2021
Super Admin	Dec 22, 2021
Super Admin	Aug 26, 2022

Creating API credentials is easy, you just need to enter a name, optionally you can add a description, then select the role you want to use, which will determine the permissions the API credential is given.

API Credentials

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected in the sidebar. The main content area displays the 'Active Directory Sync' API credential summary. The summary includes fields: Name (Active Directory Sync), Created on (Nov 24, 2023), Expires on (Nov 23, 2025), Description (empty), Client ID (71fa878@5e10-4ec1-8549-9064fb5c1496), Client Secret (a long, complex string of characters), and Role (Service Principal Super Admin). A green callout box points to the Client Secret field with the text: 'The client secret is only shown once when the API credential is created'. Below the summary, a note states: 'Note: For security reasons, the Client Secret will only be shown one time. Click the Show Client Secret link only when you are ready to implement it.' A blue bar at the bottom of the page also contains the text: 'The client secret will only be displayed ONCE'.

API credential summary	
Name	Active Directory Sync
Created on	Nov 24, 2023
Expires on	Nov 23, 2025
Description	
Client ID	71fa878@5e10-4ec1-8549-9064fb5c1496
Client Secret	8596711a3f0e05f0a423e69301983a400308842a3c093e95e056108f03-009fe0a2c2931277479e020eef4f4f725e0f0e09cb601d
Role	Service Principal Super Admin

The client secret is only shown **once** when the API credential is created

Note: For security reasons, the Client Secret will only be shown one time. Click the Show Client Secret link only when you are ready to implement it.

The client secret will only be displayed **ONCE**

Once you have created a set of API credentials the details for the credential information will be displayed.

It is important to note that the client secret will only be displayed once, so you should only choose to display it when you are ready to use it.

API Credential Roles

The screenshot shows the Sophos Central API Credentials Management interface. On the left, there's a navigation sidebar with sections like Sophos Central, Global Settings (which is selected), and My Products. The main area is titled 'API Credentials Management' and has tabs for 'Credentials' and 'Roles'. The 'Roles' tab is active, displaying a list of roles:

Name	# Role Members	Type	Description
Service Principal Directory Sync	1	Service Principal	Used for Active Directory Synchronization: Limited to AD sync capability
Service Principal Firewall	0		
Service Principal Forensics	0		
Service Principal Super Admin	6		
Service Principal Management	0		
Service Principal ReadOnly	0		

A modal window is open for the 'Service Principal Directory Sync' role, showing its details. The modal has a title 'Service Principal Directory Sync' and includes fields for 'Description' (which notes it's for AD sync), 'API Permissions' (with options for 'An' and 'Alerts'), and sections for 'Directory Objects', 'Directory Synchronization', 'Endpoint', 'Endpoint Settings', 'Firewall Management', and 'Fileshare'. A 'Role Members' section on the right lists one member: 'Service Principal Sync'.

On the **Roles** tab you can see descriptions for each of the roles.

By clicking on a role, you can see the API permissions given to that role and the API credentials that are assigned.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 4

How can you easily tell if a user or group is synchronized with a directory service or Central-managed?

Type column

Icon

Mouse-over tooltip

User's summary page

SOPHOS



Question 2 of 4

True or False: You can enable and disable MFA for selected administrators?

True

False

SOPHOS



Question 3 of 4

Which forms of multi-factor authentication does Sophos Central support?

Hardware tokens

SMS

Authenticator app

Biometrics

SOPHOS



Question 4 of 4

How many API credentials can you have in Sophos Central? (enter a numerical value)

SOPHOS

Chapter Review

Users and groups can either be **synchronized** from an Active Directory or **Central-managed**, this is indicated by the icon. In the user details you can see the user's **devices**, **events**, and **policies**. Users can be a member of more than one group.

Multi-factor authentication is **required** for all administrators in Sophos Central. Sophos Central supports **SMS** and **authenticator apps**, with **email** and **PIN code** as a **backup**. You can **add** and **remove** authentication methods and **modify** the email PIN through the **user menu** in the top-right.

Credentials for accessing the Sophos Central APIs require **super admin** access to create and manage. You can have up to **10** API credentials, and each set have a **role** to manage permissions. The secret for API credentials is only shown **once**.

SOPHOS

Here are the three main things you learned in this chapter.

Users and groups can either be synchronized from an Active Directory or Centrally-managed, this is indicated by the icon. In the user details you can see the user's devices, events, and policies. Users can be a member of more than one group.

Multi-factor authentication is required for all administrators in Sophos Central. Sophos Central supports SMS and authenticator apps, with email and a PIN code as a backup. You can add and remove authentication methods and modify the email PIN through the user menu in the top-right.

Credentials for accessing the Sophos Central APIs require super admin access to create and manage. You can have up to 10 API credentials, and each set have a role to manage permissions. The secret for API credentials is only shown once.



Getting Started with Directory Synchronization in Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE1020: Getting Started with Directory Synchronization in Sophos Central

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Directory Synchronization in Sophos Central

In this chapter you will learn how to get started using directory synchronization with Windows and Azure Active Directories.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

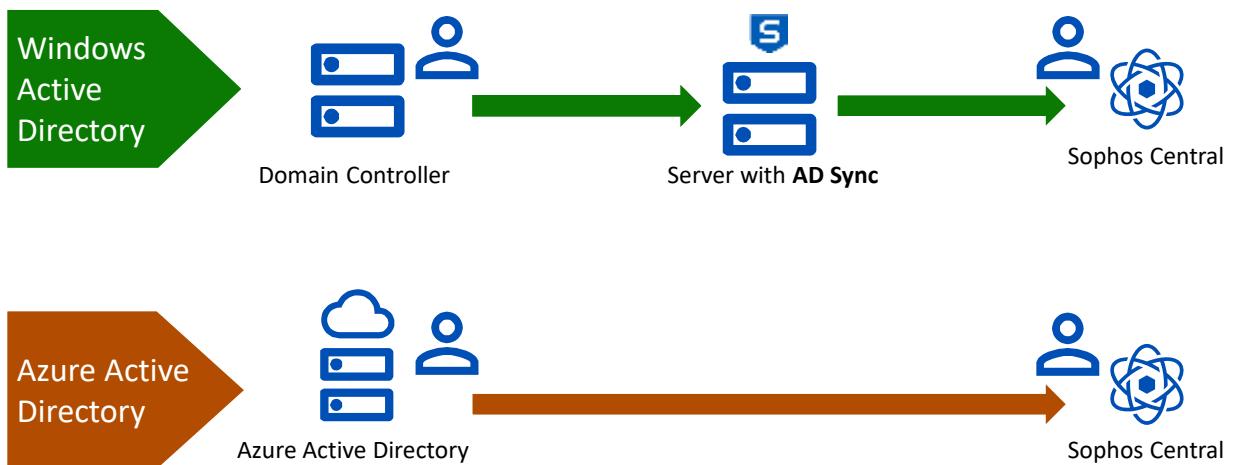
- ✓ How to add and manage users in Sophos Central

DURATION **11 minutes**

SOPHOS

In this chapter you will learn how to get started using directory synchronization with Windows and Azure Active Directories.

Sophos Central Directory Synchronization



SOPHOS

Sophos Central supports one-way synchronization of users and groups from Microsoft Windows Active Directory and Azure Active Directory.

For Windows Active Directory synchronization a small tool is installed on a server that can connect to the domain controller.

For Azure Active Directory synchronization, Sophos Central is the synchronization tool and will connect directly to Azure to perform synchronization.

Directory Synchronization

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is currently selected). Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, and Mobile. The main content area is titled "Directory service" under "Global Settings". It contains a brief description about synchronizing users and groups with either Azure Active Directory or Active Directory. Two buttons are visible: "Add Azure AD" and "Download AD Sync installer". A large blue callout box points from the text "Configuration options" to a list of three items: "Synchronize multiple Azure directory domains", "Synchronize device and device groups from a Windows AD and users and user groups from an Azure AD for the same domain", and "Synchronize Windows AD for different domains in the same forest". The top right corner shows "Help", "Active Directory", and the user "Sophos - Super Admin".

You can synchronize users and groups from multiple sources as well as synchronize devices, device groups, public folders, and mailboxes from AD.

You can synchronize multiple Azure AD domains to Sophos Central as well as:

- Synchronize devices and device groups from a Windows Active Directory and users and user groups from an Azure Directory for the same domain
- Synchronize Windows Active Directory for different domains in the same forest, selecting multiple child domains in a single forest

Directory Synchronization

Restrictions

- ✗ Synchronize users or email addresses to multiple Sophos Central admin accounts. Users and email addresses must be unique in each Sophos Central account
- ✗ Synchronize multiple Active Directory sources for the same domain
- ✗ Synchronize users using both Windows Active Directory and Azure directory from the same domain
- ✗ Synchronize from more than 25 sources

SOPHOS

There are a few restrictions when synchronizing a directory. You are unable to:

- Synchronize users or email addresses to multiple Sophos Central admin accounts. Users and email addresses must be unique in each Sophos Central account
- Synchronize multiple Active Directory sources for the same domain
- Synchronize users using both Windows Active Directory and Azure directory from the same domain
- Synchronize from more than 25 sources

Windows Active Directory Synchronization

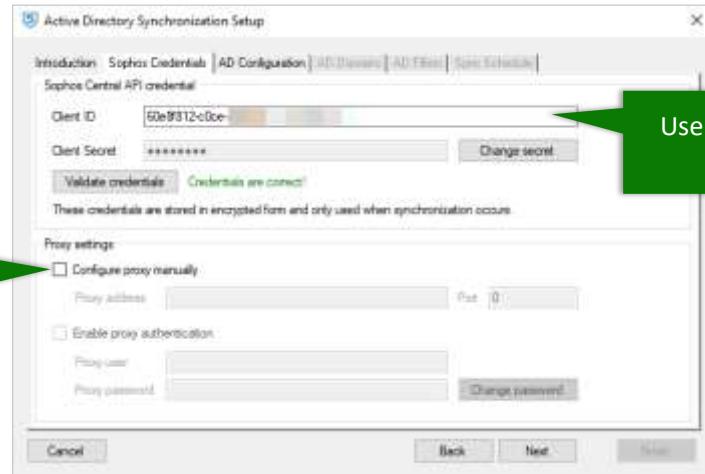
The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices', and 'Global Settings' (which is selected). Under 'MY PRODUCTS', there are links for 'Endpoint Protection', 'Server Protection', and 'Mobile'. The main content area is titled 'Directory service' under 'Global Settings'. It contains a brief description about synchronizing users and groups with either Azure Active Directory or Active Directory. Two buttons are present: 'Add Azure AD' and 'Download AD Sync installer'. A green callout box highlights the 'Download AD Sync installer' button. Below these buttons, a message states 'You don't currently have any directory services set up.' There are two 'Synchronize' buttons followed by 'Add Azure AD' and 'Download AD Sync installer' buttons.

We will start by looking at Windows Active Directory synchronization. To configure this, navigate to **Global Settings > Directory service** and select **Download AD Sync installer**.

The AD Sync Utility uses a small background service installed on a Windows device in your organization's domain. This service performs regular one-way synchronization to pull selected users and groups from your Active Directory and synchronize them to Sophos Central.

The AD Sync Utility can be installed on a Domain Controller, but alternatively it can be installed onto any Windows server or computer that is part of the domain and can connect to a Domain Controller.

Sophos Credentials



Optional configuration
a proxy manually

Use the API credentials to
configure AD Sync

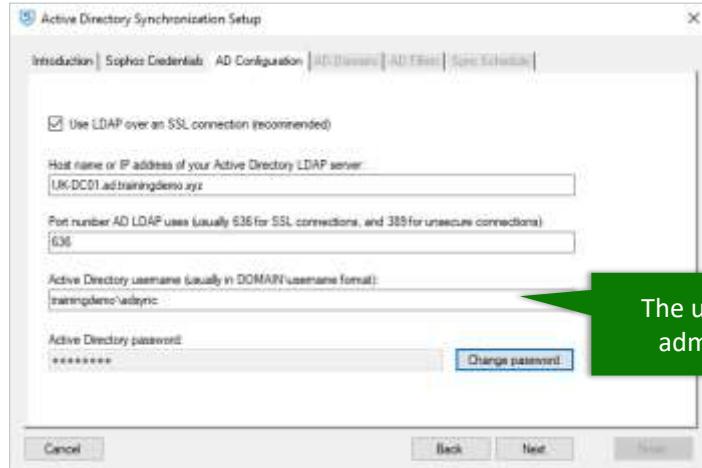
Once the installer has been downloaded and run, the configuration utility will automatically be launched.

The first step is to setup the connection to your Sophos Central account. This is done using API credentials with the 'Service Principle Directory Sync' role.

Optionally, you can also configure a proxy if this is required.

SOPHOS

AD Configuration



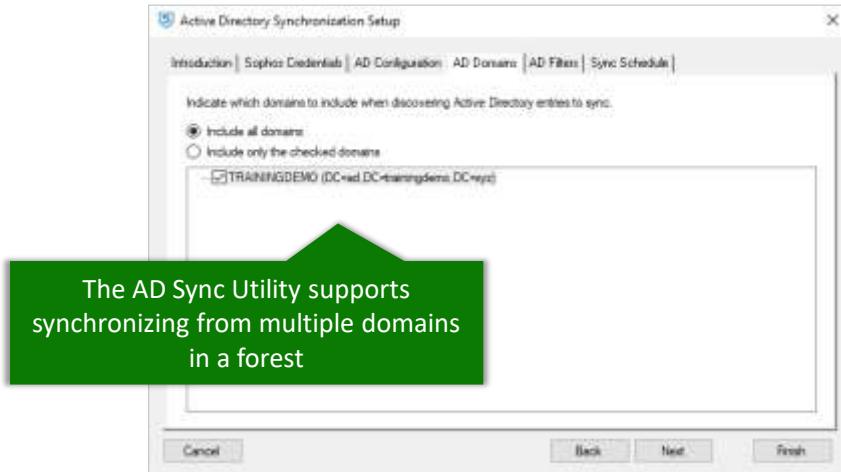
SOPHOS

The next step is to configure the connection to your Active Directory. We strongly recommend using a secure LDAP connection to the Domain Controller.

You will need to provide the hostname or IP address of the Domain Controller, the port number, which will be prepopulated but can be edited, and user credentials.

The user does not need administrative rights, any domain user that can read the directory will be sufficient.

AD Domains

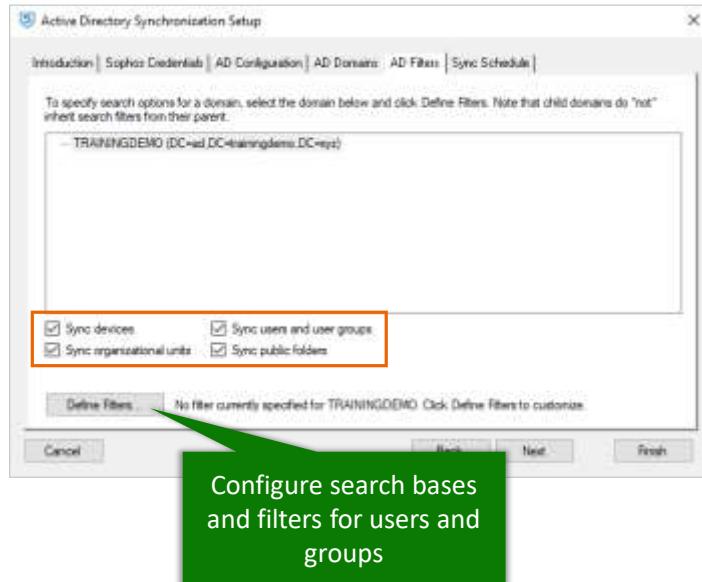


SOPHOS

AD Sync Utility can gather and synchronize information from multiple domains within a forest however, as you can only configure a single set of credentials, you cannot synchronize from unrelated domains.

If you do need to synchronize data from unrelated domains, you will need to install the AD sync utility tool on a device in each domain.

AD Filters



SOPHOS

By default, the AD sync utility will search the entire domain and synchronize everything.

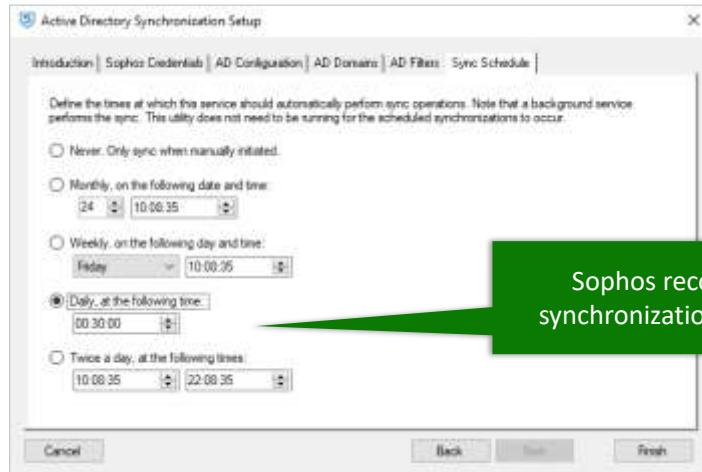
You can control the types of object that are synchronized using the four checkboxes highlighted here.

The options are:

- Sync devices
- Sync organization units
- Sync users and groups
- Sync public folders

This can be managed by configuring search bases and filters for users and groups. This can be particularly useful if you are working with a large domain. This is done by clicking **Define Filters...**

Schedule



SOPHOS

In the majority of environments Sophos recommends that you configure the AD Sync Utility to synchronize daily; however, you may want to ensure that any filters and settings work as expected before enabling the schedule.



Additional information in
the notes

Reviewing Changes

Sophos Central AD Sync Utility - Pending Changes

The following 15 users will be added to Sophos Central

Name	Email	Distinguished Name
AD Connect Service		CN=AD Connect Service,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
Administrator		CN=Administrator,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
ADSync		CN=ADSsync,DU=Service Accounts,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
Anne Green		CN=Anne Green,OU=Marketing,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
Fred Rogers		CN=Fred Rogers,OU=Support,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
IME_ADMIN		CN=IME_ADMIN,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
IME_USER		CN=IME_USER,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
Jane Doe		CN=Jane Doe,OU=Sales,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
Jo Brown		CN=Jo Brown,OU=HR,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
John Smith		CN=John Smith,OU=Sales,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
Lucy Fox		CN=Lucy Fox,OU=IT,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
MSOL_257b1ef13193		CN=MSOL_257b1ef13193,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
OktaService		CN=OktaService,CN=Users,DC=ad,DC=trainingdemo,DC=xyz
Sara Baker		CN=Sara Baker,OU=Training,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
STAS		CN=STAS,OU=Service Accounts,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz

When you manually synchronize you can review and approve changes

Approve Changes and Continue | Reject Changes and Stop

When you complete the configuration of the AD Sync Utility, or if you choose to perform a manual synchronization, you can review all the changes that will be made before committing them. This allows you to confirm that your configuration is working as expected.

Simulation: AD Sync Utility



In this simulation you will install and configure AD Sync Utility.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/ADSync/1/start.html>

SOPHOS

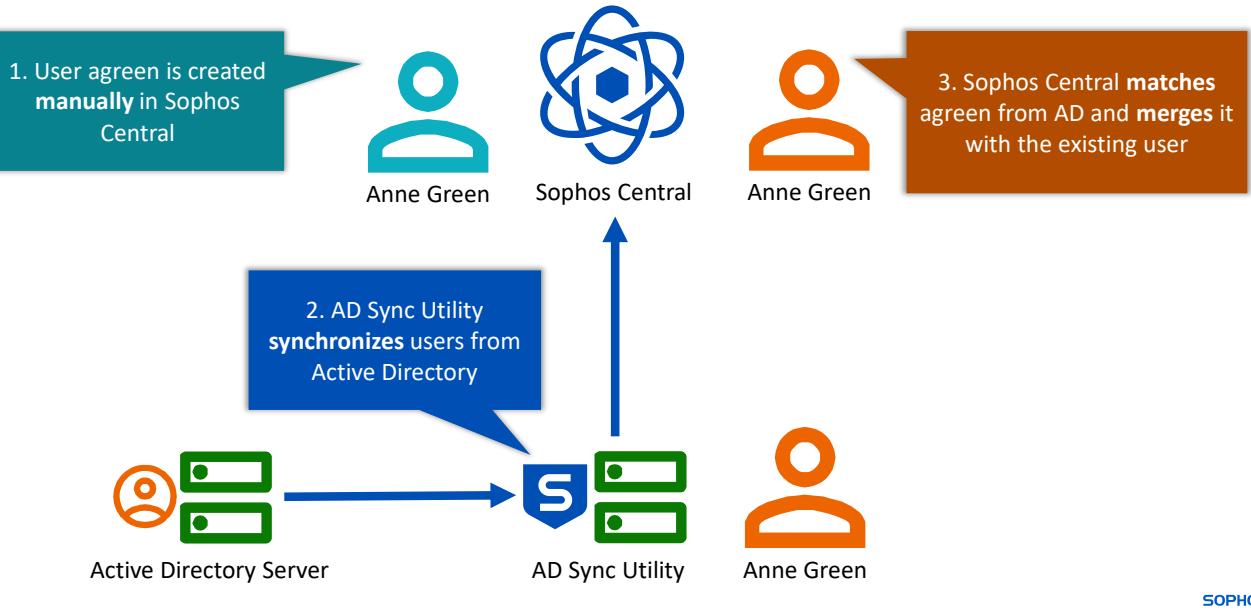
Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/ADSync/1/start.html>

Merging Users



In some cases, AD Sync Utility may be setup after some users have been created manually; for example, users that were created during an evaluation or pilot phase.

In this case, AD Sync Utility will merge the users from AD with existing users if their email addresses match. This will also apply to users that are created automatically when a domain name and logon name of the user matches.

For example, the user Anne Green in Sophos Central is merged with the user Anne Green from Active Directory.

Azure Active Directory Synchronization

The screenshot shows the Sophos Central interface. On the left, a sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected), Third-party Connectors, Protect Devices, and Account Health Check. Under MY PRODUCTS, there are Endpoint Protection, Server Protection, and Mobile options. The main content area is titled "Azure Config" under "Global Settings / Directory service / Azure Config". It shows a "Directory type: Azure active directory" and a "Turn on" button. Below this, there are "Settings" and "Preview" tabs, and a "Configure a synchronization schedule" callout pointing to a red-bordered section. This section contains fields for "Name" (set to "Sophos Training") and "Description", and a "Synchronization schedule" section where "Hourly" is selected, set to "Every 6 hours starting at 02 AM". Other options like Daily, Weekly, Monthly, and None are also available.

Let's look at getting started if you have chosen to use an Azure directory in Sophos Central.

The top of the page provides a synchronization schedule allowing you to determine how often the directory will be synchronized with Sophos Central.

Azure Active Directory Synchronization



Additional information in
the notes

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected. In the main content area, there is a configuration section for Azure Active Directory synchronization. It includes fields for 'Client ID', 'Domain', 'Client secret', and 'Client secret expiration'. A green callout box highlights this section with the text: 'How to configure an app in Azure Active Directory so Sophos Central can connect to synchronize'.

In the configuration section, you can view the instructions on how to configure an app in Azure Active Directory so that Sophos Central can connect to your Azure directory. We will cover these steps in a moment.

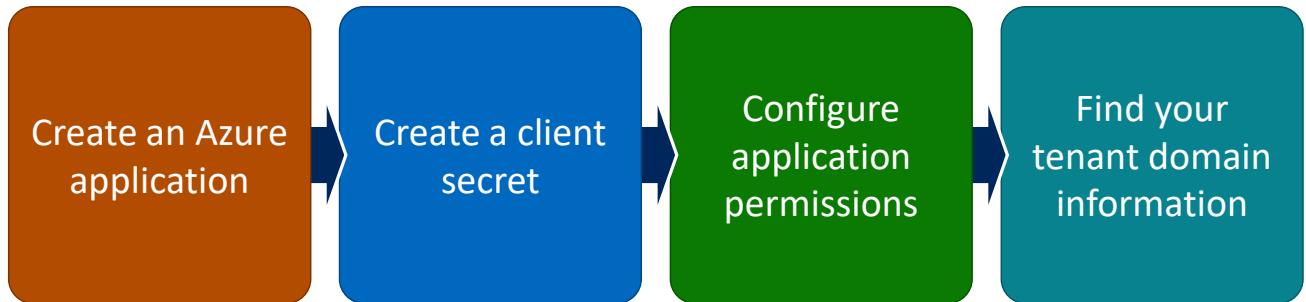
Once you have configured Azure Active Directory you will have four pieces of information. These are required to allow Sophos Central to connect:

- Client ID
- Client secret
- Tenant domain
- Client/Application secret expiration date

[Additional Information]

<https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithAzureAD/AddAzureApplication/index.html>

Setup an Azure Application



SOPHOS

The Azure Active Directory configuration is completed in four steps:

- Create an Azure application
- Create a client secret
- Configure application permissions
- Find your tenant domain information

All these steps take place within the Azure Active Directory.

Create an Azure Application

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The 'Name' field contains 'Central AD Sync'. The 'Supported account types' section has a radio button selected for 'Accounts in this organizational directory only' (Single tenant). The 'Redirect URI (optional)' section shows a 'Web' dropdown set to 'https://central.sophos.com'.

* Name
The user-facing display name for this application (this can be changed later).
Central AD Sync

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multi-tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multi-tenant) and personal Microsoft accounts (e.g. Skype, XBox)
 Personal Microsoft accounts only
Help me choose...

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web https://central.sophos.com

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies.

The first step is to create, or register, an application in Azure Active Directory.

This can be done in **App registrations** by clicking **New registration**.

Configure the account types as **Accounts in this organization directory only**.

In the 'Redirect URI' section add a **Web URI** for **https://central.sophos.com**.

Create a Client Secret

The screenshot shows the Microsoft Azure portal interface for 'Central AD Sync'. The left sidebar has 'Certificates & secrets' selected. The main area shows a table for client secrets with one entry: 'Password' (uploaded on 11 Jan 2023, expires 8/24/2023, value: WugjQ, secret ID: 666cbc94). A green callout box points to the 'Value' column with the text 'You need the value (secret) and expiry date'. A red box highlights the 'New client secret' button.

In the app registration you created, select **Certificates & secrets**, then click **New client secret**.

Select how long the secret will be valid and click **Add**.

You need the value of the secret and the expiry date. Make a note of these and keep them safe. The secret value is only shown once when you create it and cannot be shown again.

Configure Application Permissions

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb trail shows 'Home > Sophos Training Demo > Central AD Sync'. The main title is 'Central AD Sync | API permissions'. On the left, a sidebar menu under 'Manage' has 'API permissions' selected. The main content area is titled 'Configured permissions' with a note about admin consent requirements. It shows a table with one row for 'Microsoft Graph (B2C)'. A red box highlights the 'Grant admin consent for...' button in the 'Actions' column for this row. The table columns are 'API / Permission name', 'Type', 'Description', 'Admin consent requ...', and 'Status'.

API / Permission name	Type	Description	Admin consent requ...	Status
Microsoft Graph (B2C)	Application	Read directory data	Yes	Granted for Sophos Tra...

You then need to configure the permissions for your app registration.

Select **API permissions** in the left-hand menu.

You will see a default permission here; this can be removed.

You need to add the **Application** permission for **Microsoft Graph > Directory.Read.All**, then click **Grant admin consent for your Azure AD**.

Find Your Tenant Domain Information

The screenshot shows two side-by-side views of the Microsoft Azure portal. The left view is for 'Central AD Sync' and the right view is for 'Sophos Training Demo | Overview'. Both views are under the 'Azure Active Directory' section.

Central AD Sync Overview:

- Shows the 'Application (client) ID' as `f71e0aa2-0000-0000-0000-000000000000`.
- Shows the 'Object ID' as `18751106-0000-0000-0000-000000000000`.
- Shows the 'Directory (tenant) ID' as `4bc1d8f4-0000-0000-0000-000000000000`.
- Shows the 'Supported account types' as 'My organization'.

Sophos Training Demo | Overview:

- Shows the 'Name' as 'Sophos Training Demo'.
- Shows the 'Tenant ID' as `4bc5d07d-0000-0000-0000-000000000000`.
- Shows the 'Primary domain' as `trainingdemo.epr`.
- Shows the 'Users' count as 14.
- Shows the 'Groups' count as +.
- Shows the 'Applications' count as 0.

Finally, you need to locate two further pieces of information. First, the 'Application (client) ID' of your app registration, and second the primary domain, which can be found on the overview page of your Azure AD.

Azure Active Directory Synchronization

The screenshot shows the Sophos Central Global Settings page under the 'Azure Active Directory Synchronization' section. It includes fields for Client ID (77c982c09d33ad3xyz-44), Domain (trainingdemo.xyz), Client secret (redacted), and Client secret expiration (Jul. 25 2024). A green callout box points to the user and group selection section below, stating: 'Optionally configure filters for users and groups'. Other options shown include 'All users and groups' (selected), 'Add users by group ID', 'Add users by group filter', and 'Add users by user filter'.

Using this information, you can configure your Azure AD in Sophos Central.

Enter the required details then click **Test Connection** to validate the details entered.

You can optionally filter the users and groups that will be synchronized.

To finish, **Turn On** at the top of the page to save and turn on the source. You can select **Save** which will save the configuration changes but not apply them.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

What permissions does the user AD Sync Utility connects to the domain with require?

Domain Admin

Read Access

Auditor Access

Enterprise Admin

SOPHOS



Question 2 of 3

What are the 4 steps required to configure Azure Active Directory so that Sophos Central can synchronize users and groups?

Add an app role

Create an app registration

Find your tenant domain information

Create a client secret

Create a token

Configure API permissions

SOPHOS

Question 3 of 3

How often does Sophos recommend to schedule the AD Sync Utility tool to synchronize with Sophos Central?

Hourly

Daily

Weekly

Monthly

Chapter Review

To synchronize from Windows Active Directory, you need to install the AD Sync Utility on either a domain controller or another Windows device that is a member of the domain. AD Sync Utility needs API credentials to connect to Sophos Central and a user to connect to the domain

To synchronize from Azure Active Directory, you need to create an app registration in Azure AD. In the app registration you need to add a client secret and configure the API permissions with Microsoft Graph Directory.Read.All application permissions

Existing users that have an email address that matches a user being synchronized will be merged. You can change the directory type, in which case synchronized data in Sophos Central will be kept, but no new data will be accepted from the previous directory

SOPHOS

Here are the three main things you learned in this chapter.

To synchronize from Windows Active Directory, you need to install the AD Sync Utility on either a domain controller or another Windows device that is a member of the domain. AD Sync Utility needs API credentials to connect to Sophos Central and a user to connect to the domain.

To synchronize from Azure Active Directory, you need to create an app registration in Azure AD. In the app registration you need to add a client secret and configure the API permissions with Microsoft Graph Directory.Read.All application permissions.

Existing users that have an email address that matches a user being synchronized will be merged. You can change the directory type, in which case synchronized data in Sophos Central will be kept, but no new data will be accepted from the previous directory.



Getting Started with Sophos Central Agent Deployment

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE1505: Getting Started with Sophos Central Agent Deployment

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Agent Deployment

In this chapter you will learn how to install the Sophos Central Endpoint agent on Windows, macOS, and Linux.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Be able to login to Sophos Central and navigate the console
- ✓ Experience using Windows, macOS, and Linux devices

DURATION **9 minutes**

SOPHOS

In this chapter you will learn how to install the Sophos Central Endpoint agent on Windows, macOS, and Linux.



Additional information in
the notes

Deployment Options



Download the Installer



Email a setup link



Bulk deployment using a script



Include the agent in an image

SOPHOS

There are four ways to deploy the Sophos Central Endpoint agent to your devices; these are:

- Downloading the installer directly from Sophos Central to the device
- Emailing the setup link to the device owner
- Using a script to deploy the agent to multiple devices
- Including the Sophos Central agent in an image

[Additional Information]

For more information about software deployment methods, please see knowledge base article **KB-000034831**. <https://support.sophos.com/support/s/article/KB-000034831>

Download the Installer

The screenshot shows the Sophos Central interface. On the left, a sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, and Protect Devices, which is highlighted with a blue border. Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, and Email Security. The main content area is titled 'Protect Devices' and has a sub-section 'How do I use the installers for endpoints and servers?'. It contains two main sections: 'Endpoint Protection' and 'Unified Endpoint Management and Sophos Intercept X for Mobile'. Under Endpoint Protection, there's a description of full malware protection and more, followed by links to 'Download Complete Windows Installer' (with 'Choose Components...' option), 'Download Complete macOS Installer' (with 'Choose Components...' option), and a checkbox for 'Send Installers to Users!'. The Unified Endpoint Management section includes a link to 'Use the enrollment wizard to manage and/or protect a device'.

To download the installer from Sophos Central, navigate to **Protect Devices** in the left-hand menu.

The download page is divided into sections for each product. In the ‘Endpoint Protection’ section you can see there are download options for both Windows and macOS, and there are options to either download the complete installer or to **Choose Components**.

For Endpoint and Server Protection, the installer that is downloaded is the same. When the installer runs it detects whether it is running on an endpoint or server and installs the appropriate packages.

There are also ‘Protect Devices’ pages within the product sections of Sophos Central that will only display the downloads available for that product. This means that if you are in the ‘Endpoint Protection’ section of Sophos Central you do not need to come back to the dashboard to access the downloads.

Agent Download

The screenshot shows the Sophos Central interface under the 'Protect Devices' section. On the left sidebar, 'Protect Devices' is selected. In the main content area, under 'How do I use the installers for endpoints and servers?', there's a 'Endpoint Protection' section. It includes links for 'Download Complete Windows Installer', 'Choose Components...', 'Download Complete macOS Installer', 'Choose Components...', and 'Send Installers to Users...'. A callout box highlights the 'Choose Components...' links. A larger callout box highlights the 'Component Installation Options' dialog window, which lists 'Sophos Intercept X Advanced with XDR' and 'Device Encryption' with a note about removing third-party security software. Buttons for 'Cancel' and 'Download Installer' are at the bottom.

For Endpoint Protection you can choose which components you want to install. This will only allow you to select the components you are licensed for.

In the example shown here you can choose whether to install Intercept X Advanced with XDR, Device Encryption, or both.

Agent Email Setup Link

The screenshot shows the Sophos Central 'People' management interface. On the left sidebar, under 'People', the 'Email Setup Link' button is highlighted with a red box. The main area displays a list of users with checkboxes next to their names. A larger red box highlights the 'Email Setup Link' dialog box, which contains sections for 'DEPLOYMENT EMAILS' and 'OTHER EMAILS'. It also includes a green callout box with the text 'Optionally include a setup link to the self-service portal' pointing to the 'Save' button. The 'Save' button is also highlighted with a red box.

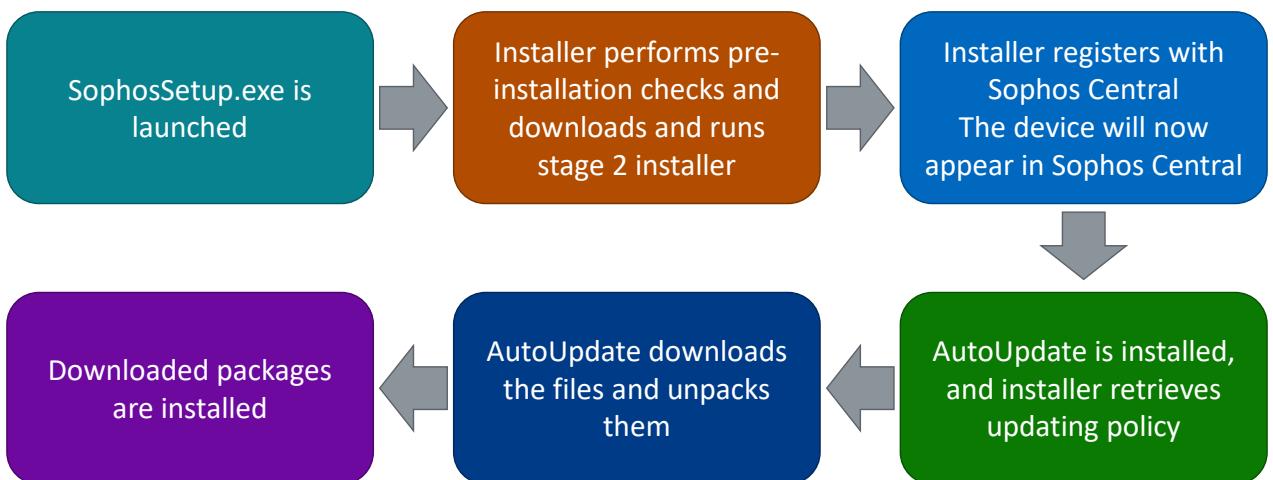
If your users have local administrator rights, they can install protection on their own devices using a link emailed to them.

To send an installation link, navigate to **People** in the left-hand menu, select the users you want to send the link to, then click **Email Setup Link**.

You can choose which setup links to send to a user. You can select to send an installation link for deploying the Sophos agent, and a setup link for the self service portal. The self service portal allows users to manage their devices, view their quarantined emails, read emails using an emergency inbox, and retrieve recovery passwords for device encryption.

When emailing an installation link to users you cannot select individual components, all licensed components will be included.

Windows Installation Process



SOPHOS

Manual installation on Windows is very simple, but let's consider what steps the installer is taking in the background.

1. Installation starts when SophosSetup.exe is launched
2. The installer performs per-installation checks and downloads and runs a second stage installer
3. The second stage installer takes over the installation process and registers with Sophos Central
4. AutoUpdate is installed and the installer retrieves the updating policy, which includes the details required to download
5. AutoUpdate downloads the files and unpacks them
6. The downloaded packages are installed

Simulation: Installation on Windows



In this simulation you will install Sophos Central Endpoint on Windows.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/WindowsInstall/1/start.html>

SOPHOS

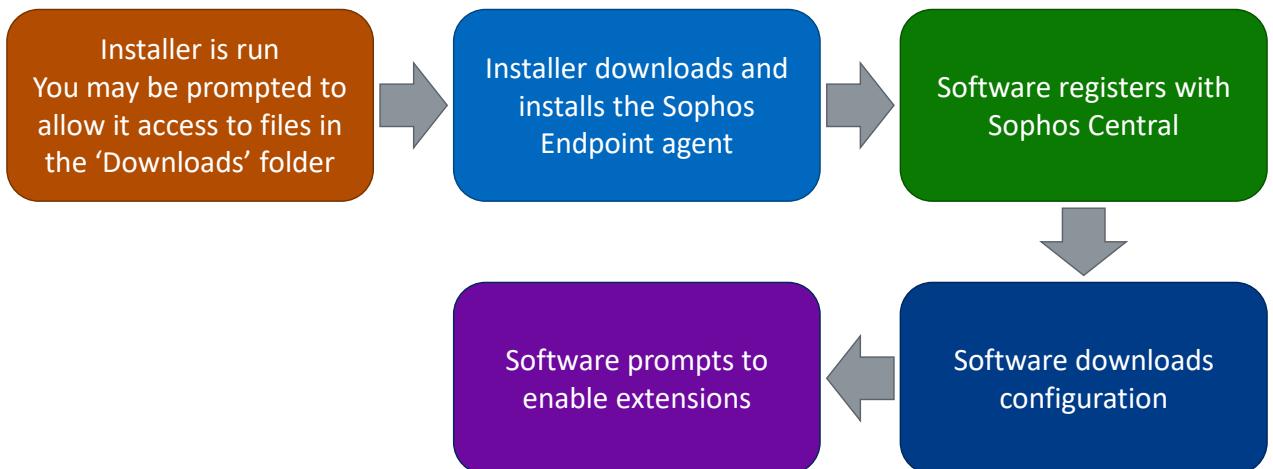
Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/WindowsInstall/1/start.html>

MacOS Installation Process

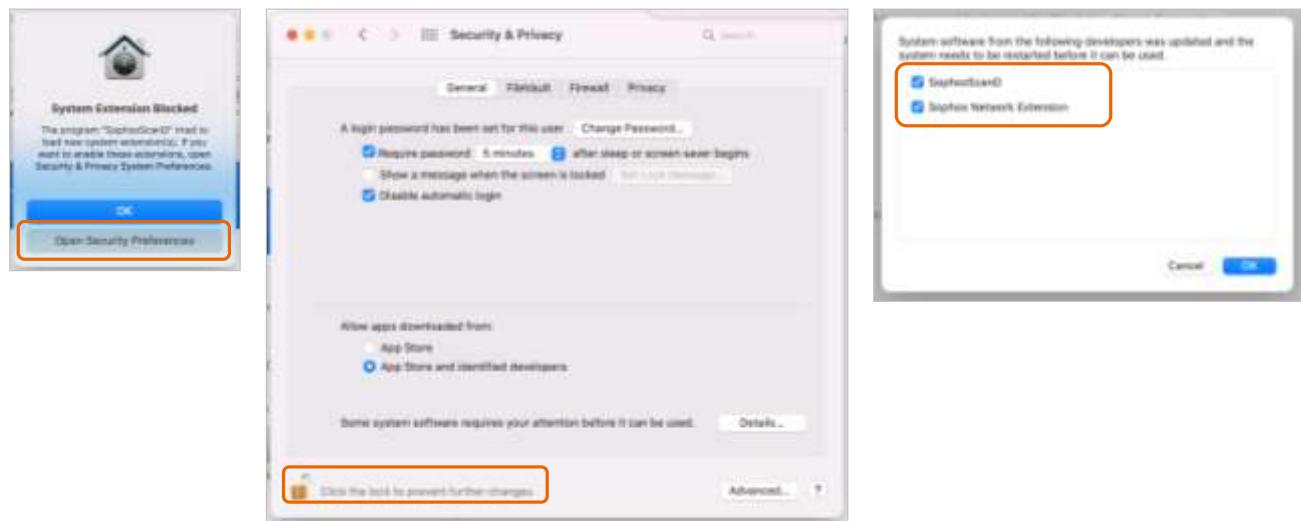


SOPHOS

The macOS installer works in a very similar way to Windows, but does things in a different order.

- You start by running the installer. Here you may be prompted to allow the installer access to the files in 'Downloads'. This is required to proceed with the installation
- The installer downloads and installs the Sophos Endpoint agent
- The Endpoint agent registers with Sophos Central so it can be managed
- The Endpoint agent downloads the configuration
- At the end of the installation the software will prompt for you to enable the extensions required for Sophos to provide protection. This is done in 'System Preferences'

MacOS Installation Process



SOPHOS

When prompted to enable extensions, click open **Security Preferences**.

You will need to click on the padlock in the bottom-left and authenticate to make the necessary changes.

Click **Details...**

Select both of the extensions and click **OK**.

Simulation: Installation on MacOS



In this simulation you will install the Sophos Central Endpoint agent on macOS.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/MacInstall/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/MacInstall/1/start.html>

Linux Installation Process

```
labuser@SophosLab-712250:~$ sudo su -
root@SophosLab-712250:~# bash /home/labuser/SophosSetup.sh
This software is governed by the terms and conditions of a licence agreement
with Sophos Limited
Installation process for Sophos Linux Protection started
Attempting to connect to Sophos Central
Successfully verified connection to Sophos Central
Downloading base installer (this may take some time)
Finished downloading base installer
Running base installer
Product will be installed to: /opt/sophos-spl
Installation complete, performing post install steps
Registering with Sophos Central
Now managed by Sophos Central
root@SophosLab-712250:~#
```

SOPHOS

The installation on Linux is similar to macOS, in that the software is installed before it registers with Sophos Central.

You will need to run the installer as the root user. When the installation starts, it will connect to Sophos Central and download the base installer.

Once downloaded the base installer is run to install Server Protection. When it has finished installing it will register with Sophos Central and download the configuration.

Video Demo: Install Sophos Server Protection for Linux



In this demo we will install Sophos Server Protection for Linux.

LAUNCH DEMONSTRATION

CONTINUE

<https://training.sophos.com/ce/demo/LinuxInstall/1/play.html>

SOPHOS

Please watch this video demonstration.

Click **Launch Demonstration** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/demo/LinuxInstall/1/play.html>



Bulk Installation to Existing Devices

Windows

- Active Directory Group Policy
- Microsoft Endpoint Configuration Manager
- Microsoft Intune
- Others...

Mac OSX

- JAMF Pro
- Others...

Linux

- Puppet
- Others...

- Use installer from Central Admin Dashboard
- Same installer can be used for all Windows (endpoint/server)
- Use third party tools to run installer on target computers with admin rights

SOPHOS

If you need to deploy the Sophos Endpoint agent to multiple devices, you can create a script that will automatically deploy and install it.

You can either use Active Directory scripts in your Group Policy, or alternatively you can choose to use an RMM tool. For example, Microsoft Endpoint Configuration Manager to distribute and install the Sophos Endpoint agent.

It is important to note that bulk deployments should **NOT** be created using an installer that has been sent using the email setup link. If this installer is used, all devices will be associated with the user the email setup link was sent to.

[Additional Information]

The steps required to force devices to re-register with Sophos Central can be found in knowledge base article **KB-000035040**. <https://support.sophos.com/support/s/article/KB-000035049>

Endpoint protection deployment methods: **KB-000034831**.

<https://support.sophos.com/support/article/KB-000034831>



Including Sophos Central in a ‘Gold’ Image

Device identity is set during install

Multiple images of the same device will try to use the same identity

To resolve this...

Install using **--goldimage** to detect name change and register a new identity

WINDOWS

Install then remove the identity causing it to register on next boot

WINDOWS

LINUX

macOS

SOPHOS

For organizations using virtual machines, it is common to create a gold image and run multiple instances of that image.

During the installation of the Sophos agent the device identity is set, this is used by Sophos Central to identify individual devices. If you run multiple images using the same identity, all devices will report to Sophos Central as the same device. To prevent this issue, new images created from the gold image must register for a new identity. There are a couple of ways this can be done.

On Windows you can install with the **--goldimage** option. When the device name changes when a new instance is created from the image, the Sophos Endpoint agent will register for a new identity.

On Windows and Linux you can remove the identity, which causes the Sophos Endpoint agent to register for a new identity when it next starts.

[Additional Information]

Removing identity from Windows to create a gold image **KB-000035040**:

<https://support.sophos.com/support/s/article/KB-000035040>

Creating a Linux gold image: <https://docs.sophos.com/central/customer/help/en-us/PeopleAndDevices/ProtectDevices/ServerProtection/SophosProtectionLinux/LinuxGoldImage/index.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

For which products can you choose the components to install when downloading the installer from Sophos Central?

Endpoint Protection for
Windows

Endpoint Protection for
macOS

Endpoint Protection for
Linux

Server Protection for
Windows

Server Protection for Linux

SOPHOS



Question 2 of 3

True or False: When you email a setup link to a user they must have administrator rights to be able to install.

True

False

SOPHOS



Question 3 of 3

Which of the following happens first during a Windows installation after the installer is run?

The device is registered with Sophos Central

The AutoUpdate policies are retrieved

The stage 2 installer is downloaded

The software is downloaded

SOPHOS

Chapter Review

Sophos can be installed on devices by manually **downloading and running the installer**, this requires **administrator** rights. Endpoint Protection allows you to **select** which of your licensed components you want to install.

You can send a **setup link** via **email** to the **device owner** to **install** if they have **administrator rights**. You can **include links for deploying** the software and **setting up access** to the **self-service portal**.

The Sophos Endpoint agent can be **deployed to multiple devices** using a **script**, third-party **RMM tools**, or including the agent in a **gold image**.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos can be installed on devices by manually downloading and running the installer, this requires administrator rights. Endpoint Protection allows you to select which of your licensed components you want to install.

You can send a setup link via email to the device owner to install if they have administrator rights. You can include links for deploying the software and setting up access to the self-service portal.

The Sophos Endpoint agent can be deployed to multiple devices using a script, third-party RMM tools, or including the agent in a gold image.



Getting Started with Sophos Central Updating

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE2005: Getting Started with Sophos Central Updating

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Updating

In this chapter you will learn how Sophos Central updates and maintains the Sophos Endpoint Agent on managed devices, and how Sophos minimizes the bandwidth required for updating.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to deploy the Sophos Endpoint Agent

DURATION **6 minutes**

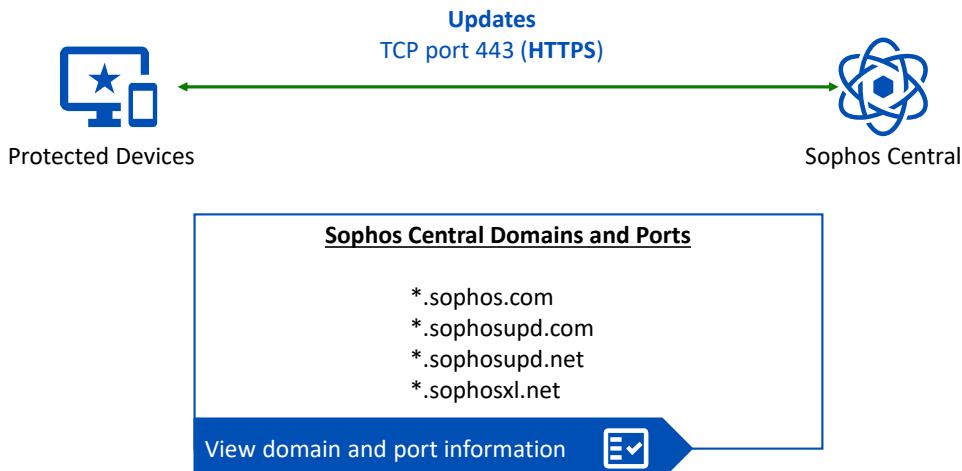
SOPHOS

In this chapter you will learn how Sophos Central updates and maintains the Sophos Endpoint Agent on managed devices, and how Sophos minimizes the bandwidth required for updating.



Additional information in
the notes

Sophos Central Updating Overview



SOPHOS

Once a device has been protected, all installed components are maintained by the Sophos AutoUpdate service. Sophos Central updating uses TCP port 443 to communicate updates between Sophos Central and protected devices.

If you need to allow updating through a firewall or proxy, you need to ensure that the domains shown are allowed.

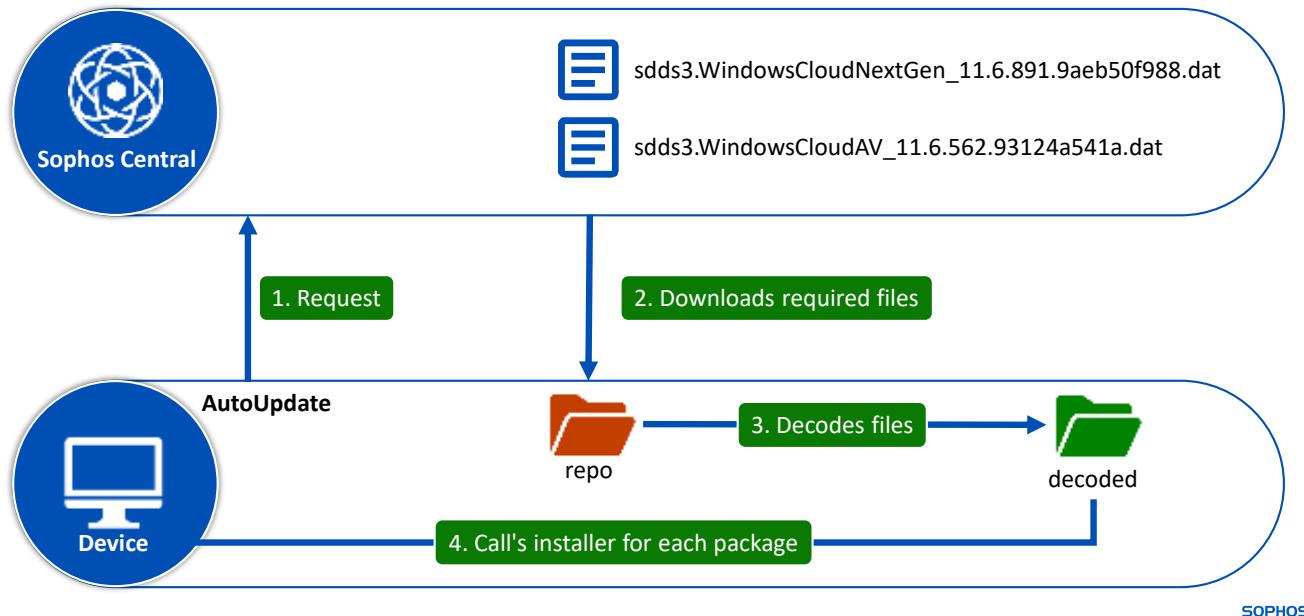
If your proxy or firewall doesn't support wildcards, you must identify the exact Sophos domains you need, and then enter them manually.

[Additional Information]

Full list of domains and ports that need to be allowed:

<https://docs.sophos.com/central/customer/help/en-us/PeopleAndDevices/ProtectDevices/DomainsPorts/index.html#sophos-central-admin-domains>

How Sophos Central Updates



Let's have a look at how updating works.

Sophos AutoUpdate requests a manifest of the files that are required for the latest version of the Sophos Endpoint Agent.

Once the required files have been identified, they are downloaded to the device. Sophos AutoUpdate uses the **repo** folder to store the downloaded files and decodes the files into a local cache folder named **decoded**.

Once decoded, Sophos AutoUpdate calls the installer for each package to perform any required updates.

If a component is added to a device in Sophos Central, for example Device Encryption, the devices subscription package is updated. When the device receives the new policy, Sophos AutoUpdate identifies the new component, downloads, and installs the component.

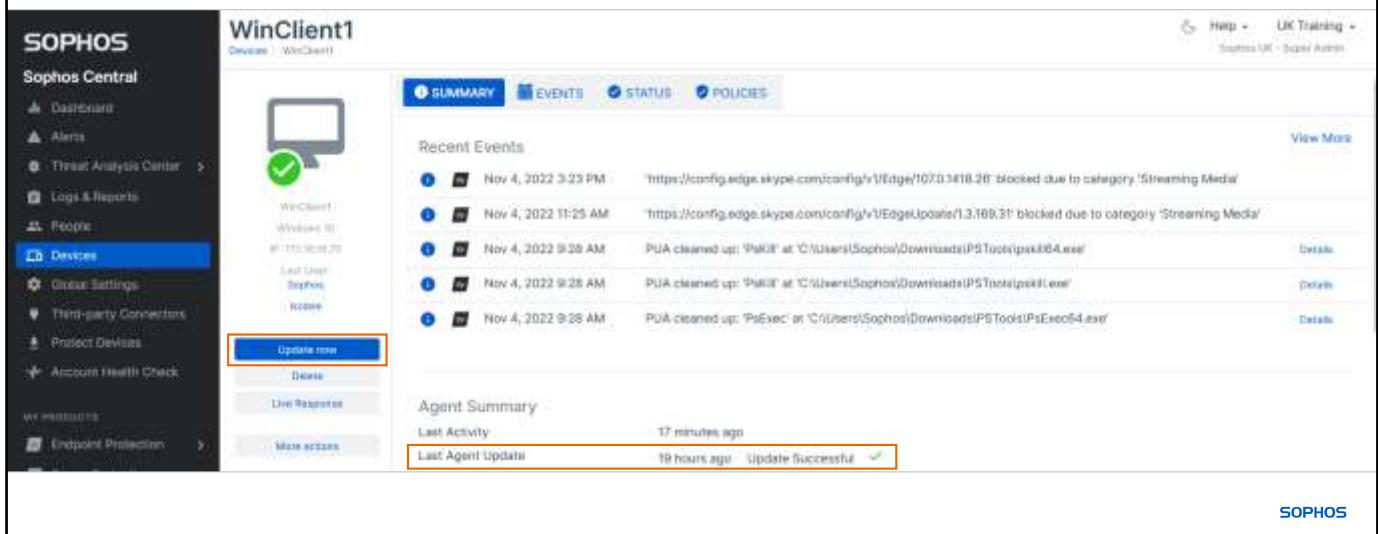
[Additional Information]

Files are downloaded to C:\ProgramData\AutoUpdate\data\repo

The local cache folder can be found here: C:\ProgramData\AutoUpdate\Cache\decoded

Updating Status

- View the updating status of a device in Sophos Central



The screenshot shows the Sophos Central interface for a device named 'WinClient1'. The left sidebar has a 'Devices' section with 'Update now' highlighted in red. The main area shows a summary tab with recent events, agent summary, and last activity information. The 'Last Agent Update' row is also highlighted in red.

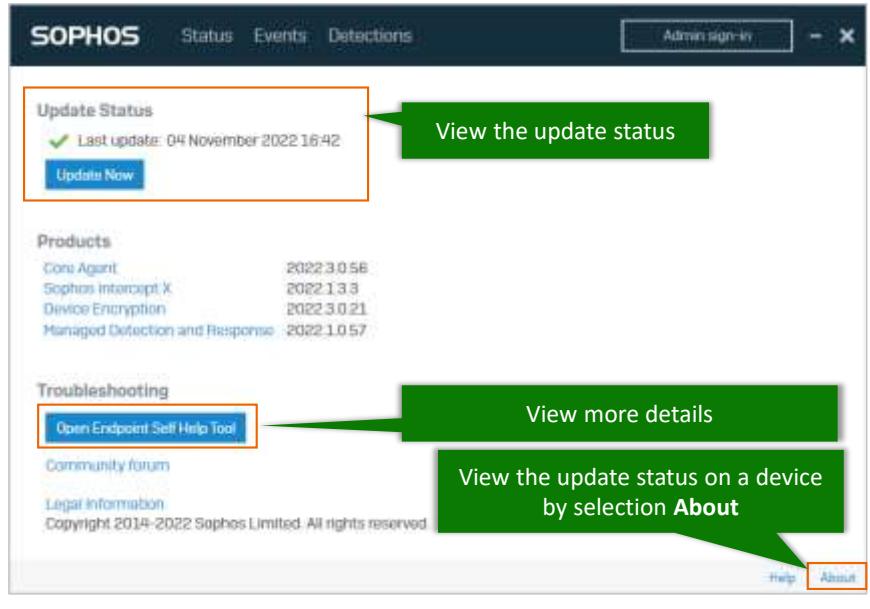
Date	Action	Details
Nov 4, 2022 3:33 PM	https://config.edge.skype.com/config/vUEdge/107.0.3418.28 blocked due to category 'Streaming Media'	
Nov 4, 2022 11:25 AM	https://config.edge.skype.com/config/vUEdgeUpdate/1.3.169.31 blocked due to category 'Streaming Media'	
Nov 4, 2022 9:28 AM	PUA cleaned up: 'PakKill' at 'C:\Users\Sophos\Downloads\PS9Tools\pakkill64.exe'	Details
Nov 4, 2022 9:28 AM	PUA cleaned up: 'PakKill' at 'C:\Users\Sophos\Downloads\PS9Tools\pakkill64.exe'	Details
Nov 4, 2022 9:28 AM	PUA cleaned up: 'PsExec' at 'C:\Users\Sophos\Downloads\PS9Tools\PsExec64.exe'	Details

SOPHOS

The updating status of a device is displayed in the device record. In the 'Agent Summary' section you can see the last activity on the device and the 'Last Agent Update' time and whether it was successful or not.

You can force an update from Sophos Central by clicking **Update now**.

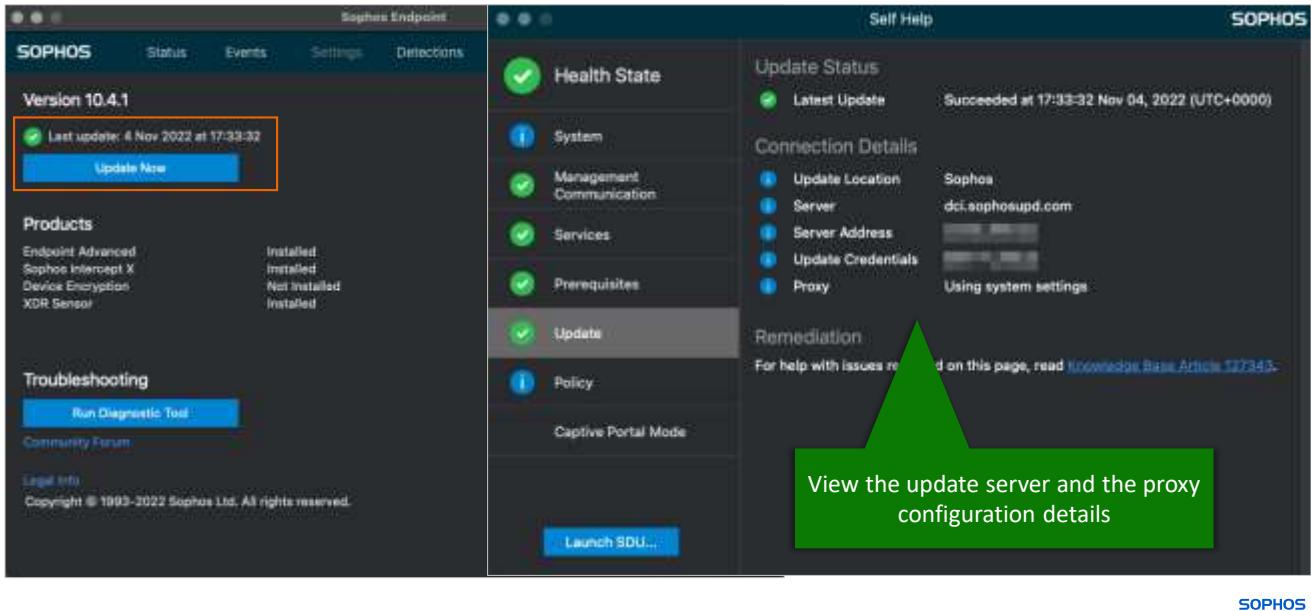
Updating on Windows



On a Windows device, The Sophos Endpoint Agent displays the ‘Update Status’ in the **About** menu. You can select to force an update by clicking **Update Now**.

Opening the Endpoint Self Help tool allows you to view further updating information. You can see where the device is updating from, in this example, the device is updating directly from Sophos. If a proxy server has been configured for updating, the proxy server details will be displayed here.

Updating on MacOS



On a macOS device, the Sophos Endpoint Agent displays the update status on the **About** page.

In the diagnostic tool, the **Update** tab details the latest update date and time, and the connection details. You can view the update location and server along with any proxy server details if they have been configured.

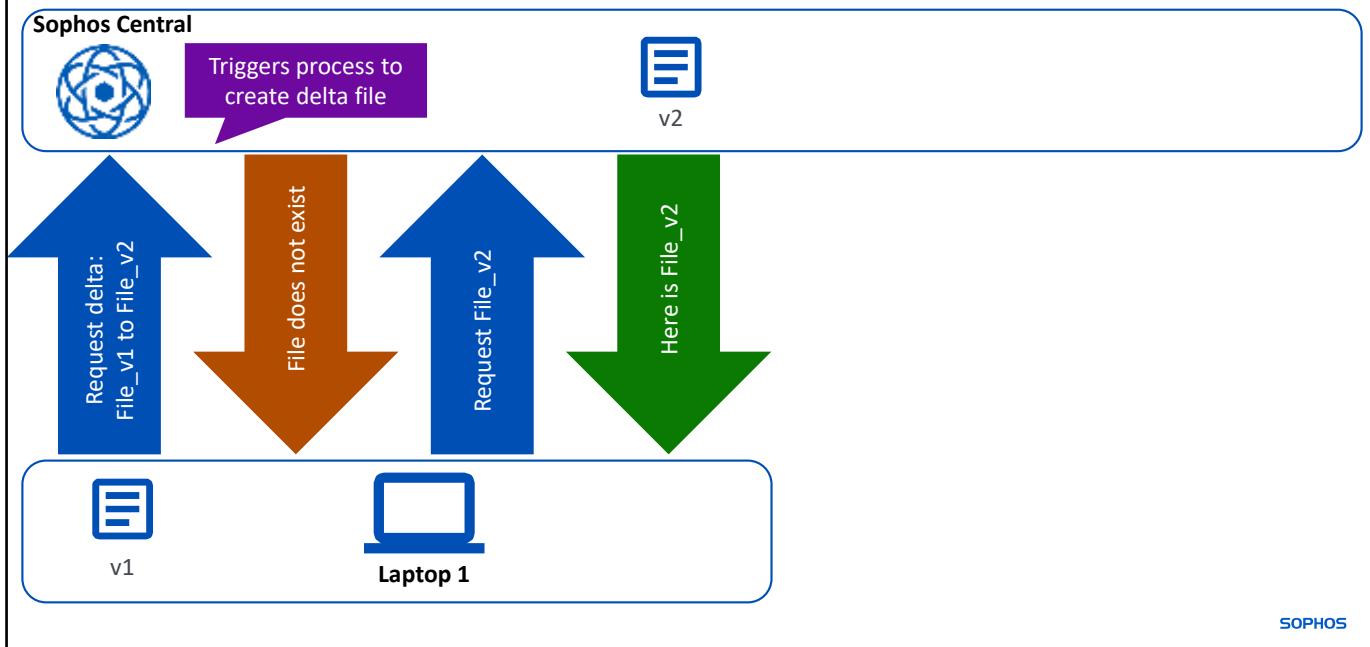
Updating on Linux

The screenshot shows the Sophos Central interface for a device named 'linuxserver1'. The left sidebar has 'Devices' selected under 'Sophos Central'. The main area shows 'Recent Events' with three entries: 'Nov 4, 2022 9:17 PM Server re-protected: linuxserver1', 'Aug 19, 2022 10:24 AM Update successful.', and 'Aug 19, 2022 10:22 AM New server registered: linuxserver1'. Below this is 'Agent Summary' showing 'Last Sophos Central Activity' at '13 minutes ago' and 'Last Agent Update' at '11 minutes ago' with status 'Update-Successful'. An 'Update Now' button is highlighted with a red box. The 'Assigned Products' section lists 'Core Agent', 'Server Protection', and 'XDR' all as 'Assigned'. At the bottom, the IP address is listed as '172.16.16.130'.

For Linux servers protected with Sophos Protection, you cannot force an update directly on the server.

You can click **Update Now** in the device details in Sophos Central which will force an update on the server.

How Sophos Minimizes Bandwidth Usage



Sophos uses a dynamic file delta technique to help reduce the amount of bandwidth that is required for devices to update. Let's look at how this happens.

We have a device, Laptop 1. It has version 1 of a file, but needs version 2 of the file.

Laptop 1 sends a request to Sophos for the delta between version 1 and version 2 of the file.

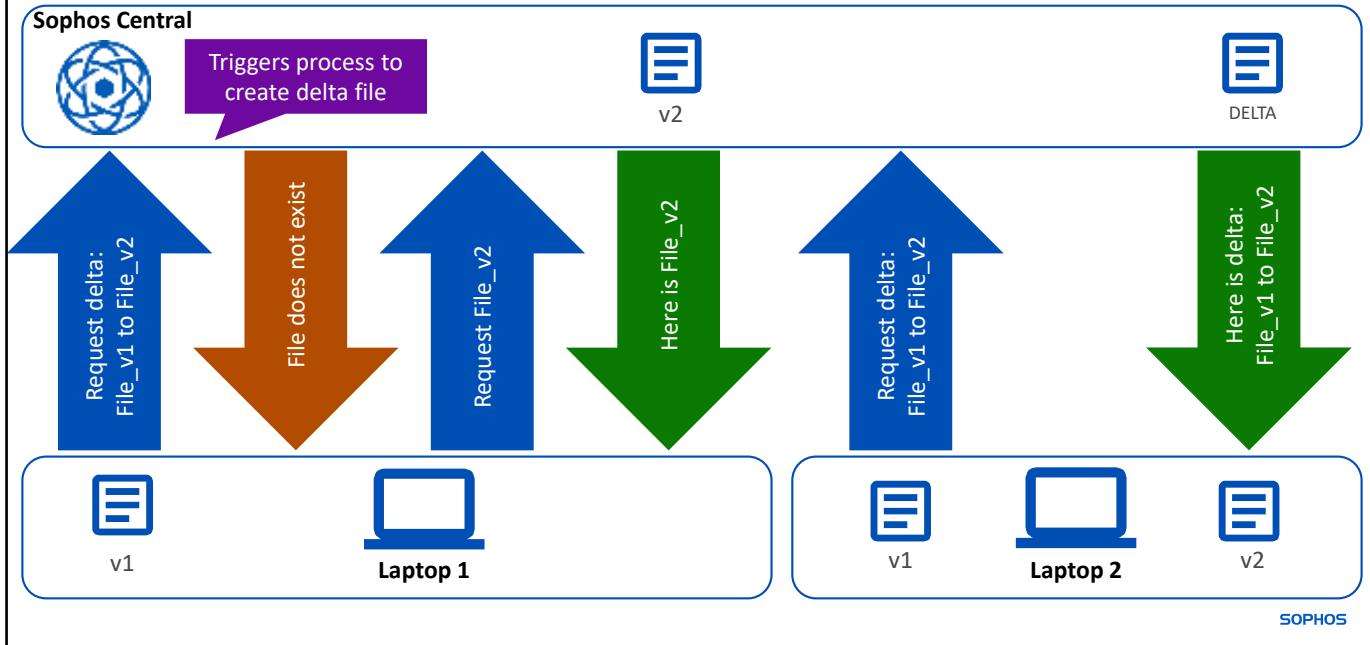
This is the first time the device has requested the delta file which currently does not exist.

Sophos responds to the device that the file does not exist, and triggers the process to create that delta file.

As the delta file does not exist, Laptop 1 requests the full version 2 of the file.

Version 2 of the file is sent to Laptop 1.

How Sophos Minimizes Bandwidth Usage



Laptop 2 needs to update from version 1 to version 2 for the same file.

Laptop 2 sends a request to Sophos for the delta between version 1 and version 2 of the file.

Sophos created the delta file following the request from Laptop 1 and sends it to Laptop 2.

Laptop 2 merges version 1 of the file and the delta file received to create version 2 of the file.

Please note that not all files are suitable to have a delta created for them. Additionally, this technique is only applicable to updates. It does not apply to the initial installation of the Sophos Endpoint Agent.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Which Sophos service is used to update devices?

Protection

Health

AutoUpdate

Live Query

SOPHOS



Question 2 of 2

Which TCP port is used for Sophos Central updating?
(enter a numeric value)

SOPHOS

Chapter Review

Once a device is protected, **all** the **installed components** are **maintained** and **updated** using the **AutoUpdate service**.

The **updating status** of a device can be viewed in the **device record in Sophos Central** and in the **Sophos Endpoint Agent** on Windows and macOS devices.

Sophos uses a **dynamic file delta technique** to **reduce the bandwidth** required for devices to update.

SOPHOS

Here are the three main things you learned in this chapter.

Once a device is protected, all the installed components are maintained and updated using the AutoUpdate service.

The updating status of a device can be viewed in the device record for Sophos Central and in the Sophos Endpoint Agent on Windows and macOS devices.

Sophos uses a dynamic file delta technique to reduce the bandwidth required for devices to update.



An Introduction to Update Caches and Message Relays

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE2025: An Introduction to Update Caches and Message Relays

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

An Introduction to Update Caches and Message Relays

In this chapter you will learn the function of an Update Cache and a Message Relay. You will also learn the requirements for devices to host an Update Cache and Message Relay.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access and navigate Sophos Central
- ✓ How to protect devices with the Sophos Endpoint Agent
- ✓ How the Sophos Endpoint Agent is updated

DURATION **7 minutes**

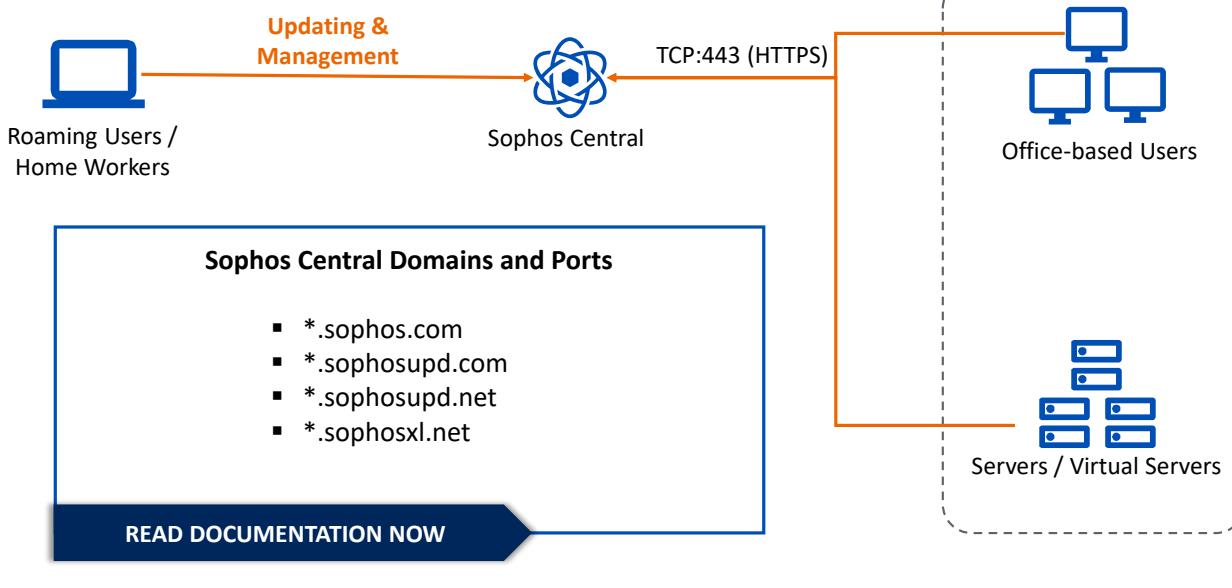
SOPHOS

In this chapter you will learn the function of an Update Cache and a Message Relay. You will also learn the requirements for devices to host an Update Cache and Message Relay.



Additional information in
the notes

Sophos Central Architecture



SOPHOS

For most organizations, protected devices will update from, and be managed directly by Sophos Central. In this configuration, devices use TCP port 443 (HTTPS) for updating and management.

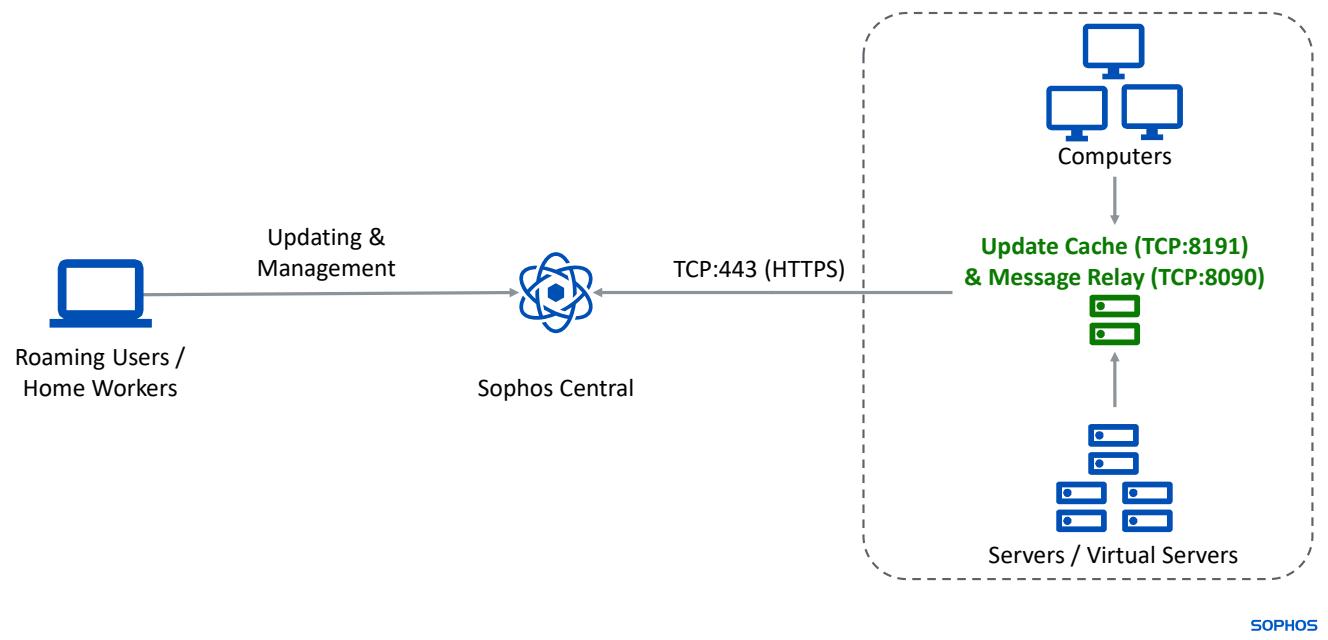
Sophos uses the domains shown here for updating and management. We recommend using DNS names for creating exceptions, as IP addresses may change.

[Additional Information]

Further information can be found in the help documentation here:

<https://docs.sophos.com/central/customer/help/en-us/PeopleAndDevices/ProtectDevices/DomainsPorts/index.html#sophos-central-admin-domains>

Update Caches and Message Relays



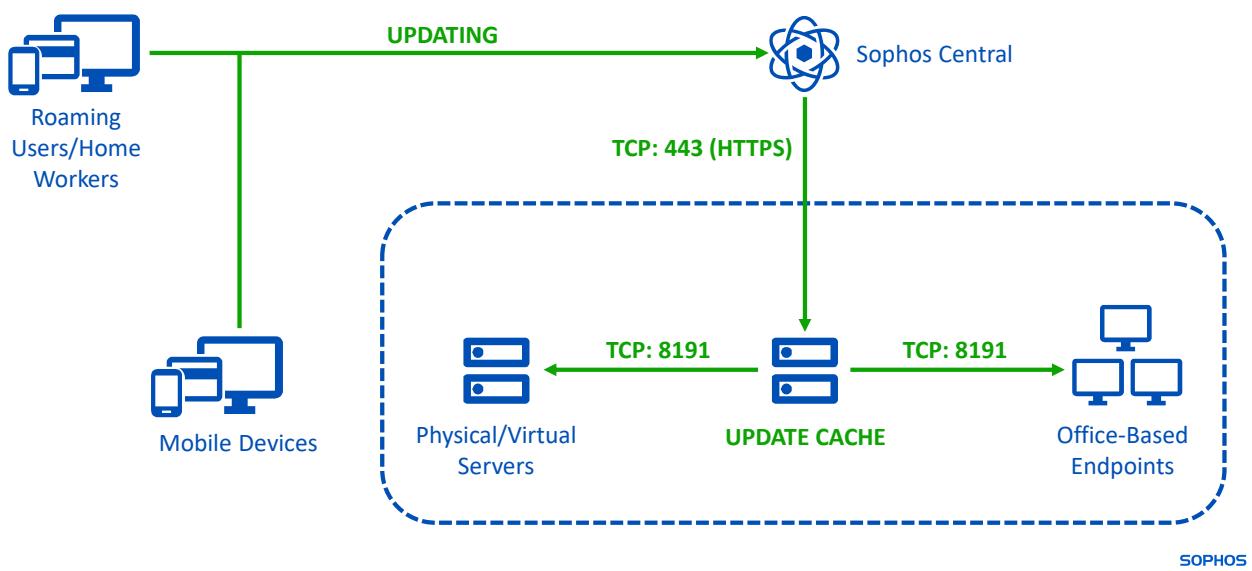
In some scenarios, either the default deployment will not work because of the way the network is designed, or an organization's experience can be improved by deploying Update Caches and Message Relays.

A Sophos Update Cache enables devices to receive updates from a cache on your network. This saves bandwidth, as updates are downloaded once by the Update Cache and devices then get their required updates from the Update Cache.

You can also enable devices to communicate with Sophos Central through a Message Relay on your network. This is especially useful if an organization has devices that are unable to connect to the Internet directly.

In this example, a server is being used as an Update Cache and Message Relay. Whilst the server still connects directly to Sophos Central, other devices connect to the server for update and management communication. Roaming users and home users will continue to update from, and be managed directly by Sophos.

How Does an Update Cache Work?



The Update Cache software is a modified version of the Apache webserver. It creates a local copy of the installation files and stores them in a cache on your network. Protected devices update from the cache location instead of directly from Sophos.

Update Caches use TCP port 8191 to communicate updates with devices, and TCP port 443 is used to communicate with Sophos Central.



Additional information in
the notes

Update Cache Requirements

Requirements

- **Server:** Windows 2008 R2 to Windows 2022
- **Endpoint:** Windows 10 x64 and Windows 11 x64
- At least **8 GB free disk space**
- TCP port **8191** must be open
- **DNS** must be working

Sizing

Up to 2,000 Devices

- 2 CPUs
- 4 GB RAM

Up to 10,000 Devices

- 4 CPUs
- 8 GB RAM

There is a limit of **500** Update Caches per Sophos Central account

SOPHOS

For a device to become an Update Cache, it must meet the following requirements.

A Windows server running 2008 R2 or later, or a Windows endpoint running Windows 10 or later. The device must have at least 8 GB of free disk space, and TCP port 8191 must be open for inbound and outbound traffic. When an Update Cache is deployed, TCP port 8191 is allowed on the Windows firewall. Additionally, DNS must be working to resolve the Update Cache IP address from the hostname.

Any device that you deploy an Update Cache on must be protected by Sophos Central **BEFORE** the Update Cache can be deployed. If the device is performing other roles, additional RAM and CPUs may need to be added.

We recommend the following specifications for an Update Cache server:

- 2 CPUs and 4 GB of RAM to serve up to 2,000 endpoints
- 4 CPUs and 8 GB of RAM to serve up to 10,000 endpoints

There is a limit of 500 Update Caches per Sophos Central account.

[Additional Information]

Additional server roles with Update Caches **KB-000035498**.

<https://support.sophos.com/support/s/article/KB-000035498>

We also recommended viewing the FAQ available in **KB-000035498**.

<https://support.sophos.com/support/s/article/KB-000035498>

Update Cache Considerations

Does not replace or override Sophos Central as an available update location

Does not work in the same way as an air gap

Devices still require access to Sophos Central

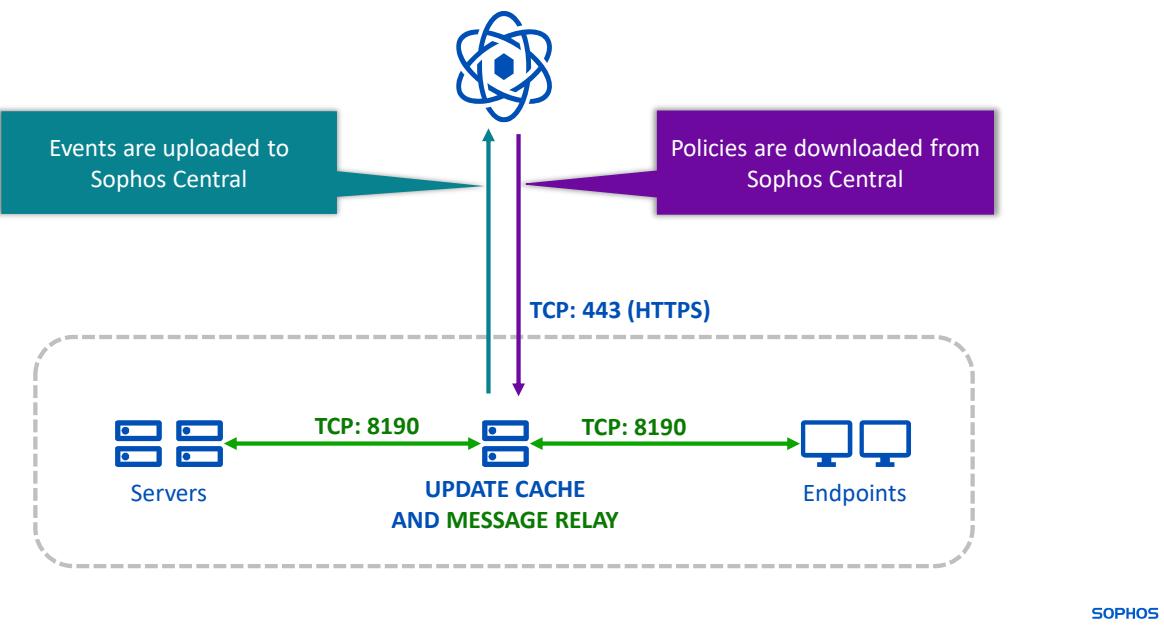
Misconfiguration of an Update Cache can cause unintended consequences

SOPHOS

It is important to understand that an Update Cache does not replace or override Sophos Central as an available update location, and does not work in the same way as an air gap. Your protected devices still require access to Sophos Central.

We strongly recommend that you take the time to understand what an Update Cache will do if configured on your network. The misconfiguration of an Update Cache can cause unintended consequences.

What is a Message Relay?



Should devices on a network not have direct Internet access you can make use of a Message Relay.

A Message Relay enables devices to communicate all policy and reporting data via a message relay server. All management traffic is routed through the message relay. We define management traffic as any communication traffic that is sent and received by the Management Communication System (MCS) on a protected device.

Protected devices use MCS to download new policies from Sophos Central, and to upload events, such as malware detections or health status changes to Sophos Central.

Message Relay Requirements

Requirements

- Windows 2008 R2 to Windows 2022
- At least **8 GB free disk space**
- TCP port **8190** must be open
- **DNS** must be working
- Device must be configured as an Update Cache

SOPHOS

For a device to be used as a Message Relay it must be a Windows Server running 2008 R2 or later. It must have at least 8 GB of free disk space and TCP port 8190 must be open. Additionally, the device must be configured as an Update Cache.

Message Relay Considerations

A protected device can be configured as both an Update Cache and a Message Relay

You cannot use a device as **ONLY** a Message Relay server

MCS traffic should not be decrypted or scanned, exclusions need to be created on any firewalls in use

Misconfiguration of a Message Relay can cause unintended consequences

SOPHOS

A protected device can be configured as an Update Cache and as a Message Relay. However, you cannot use a device as only a Message Relay server.

We strongly recommend that you take the time to understand what a Message Relay will do in your network if configured. The misconfiguration of a Message Relay can cause unintended consequences.

It is important that MCS traffic is not subject to decryption and scanning, exclusions may need to be created on any firewalls in use.

Simulation: Deploy an Update Cache and a Message Relay



In this simulation you will deploy an Update Cache and a Message Relay

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/DeployCacheRelay/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/DeployCacheRelay/1/start.html>

Knowledge Check

Take a moment to check your knowledge!



Question 1 of 2

True or False: If an Update Cache is used, devices do not require direct access to Sophos Central.

True

False

SOPHOS



Question 2 of 2

What is the TCP port an Update Cache uses?
Enter a numerical value

SOPHOS

Chapter Review

The **Update Cache** software **creates a local copy of the installation files** on a network for devices to **update from**. Devices still require access to Sophos Central.

A Message Relay **enables devices to communicate all policy and reporting data via a dedicated server** which is useful for devices that cannot connect directly to Sophos Central.

For a device to be used as a **Message Relay** it **must** be an **Update Cache**.

SOPHOS

Here are the three main things you learned in this chapter.

The Update Cache software creates a local copy of the installation files on a network for devices to update from. Devices still require access to Sophos Central.

A Message Relay enables devices to communicate all policy and reporting data via a dedicated server which is useful for devices that cannot connect directly to Sophos Central.

For a device to be used as a Message Relay it must be an Update Cache.



Getting Started with Sophos Central Update Cache and Message Relay Deployment

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE2030: Getting Started with Sophos Central Update Cache and Message Relay Deployment

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Update Cache and Message Relay Deployment

In this chapter you will learn how to deploy an Update Cache and Message Relay as well as the firewall rules and client configuration required.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How Sophos Central updates
- ✓ What an Update Cache and Message Relay are
- ✓ System requirements for Update Cache and Message Relay deployment

DURATION **6 minutes**

SOPHOS

In this chapter you will learn how to deploy an Update Cache and Message Relay as well as the firewall rules and client configuration required.

Manage Update Caches and Message Relays

The screenshot shows the Sophos Central interface under 'Global Settings > Manage Update Caches and Message Relays'. On the left, there's a sidebar with various navigation links. The main area displays a table of devices with columns for 'DESCRIPTION', 'LAST ACTIVATED', 'USING THIS CACHE', 'LAST CACHE UPDATE', and 'MESSAGE RELAY'. A dropdown menu is open over the first row, showing filter options: 'Cache Capable Servers' (selected), 'Cache Capable Computers', 'Devices with Update Cache', and 'Servers with Message Relay'. A blue button 'Set Up Cache/Relay' is visible in the top right.

DESCRIPTION	LAST ACTIVATED	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY
Windows Server 2022 S...	8 months ago	No devices	8 months ago	Active
SRV1 172.16.2.20 Windows Server 2016 S...	8 months ago	Not installed	8 months ago	Not installed
SRV2 192.168.1.245 Windows Server 2022 S...	16 days ago	Not installed	16 days ago	Not installed
SRV3 192.168.1.166 Windows Server 2022 S...	4 days ago	Active	4 days ago	Active
WinServer1 172.16.16.10 Windows Server 2019 S...	7 minutes ago	Not installed	7 minutes ago	Not installed

Update Caches and Message Relays are deployed and managed in **Global Settings > Manage Update Caches and Message Relays**.

To deploy an Update Cache and a Message Relay, navigate to **Manage Update Caches and Message Relays**. The list of devices displayed is filtered automatically to show 'Cache Capable Servers'. This view can be changed by using the drop-down menu.

Deploy an Update Cache

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various navigation options under 'Sophos Central' and 'MY PRODUCTS'. The 'Global Settings' option is highlighted with a blue background. The main content area is titled 'Manage Update Caches and Message Relays' and shows a table of 'Cache Capable Servers'. A red box highlights the 'Set Up Cache/Relay' button in the top right corner of the table header. The table columns are: DESCRIPTION, LAST ACTIVE, CACHE STATUS, USING THIS CACHE, LAST CACHE UPDATE, and MESSAGE RELAY. The data in the table includes:

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY
Windows Server 2022 S...	a month ago	Active	No devices	a month ago	Active
SRV 172.16.2.20 Windows Server 2016 S...	16 days ago	Not installed			Not installed
SRV2 192.168.1.245 Windows Server 2022 S...	4 days ago	Active	2 Devices	4 days ago	Active
WinServer1 172.16.16.10 Windows Server 2019 S...	7 minutes ago	Not installed			Not installed
5 Devices					

To deploy an Update Cache and Message Relay, select a cache capable device from the list and click **Set Up Cache/Relay**.

Deploy an Update Cache

The screenshot shows the Sophos Central web interface. On the left, there's a sidebar with various navigation links like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is currently selected). The main area is titled "Manage Update Caches and Message Relays". A modal window titled "Set Up Update Cache and Message Relay" is open. It contains instructions: "Before you start, please ensure that:" followed by two bullet points: "The server has at least 8 GB free disk space available." and "Ports 890 and 891 are available and accessible to devices that will use the cache and relay.". Below this, it says "A server must be set up as an Update Cache if you want it to be a Message Relay." There are two checkboxes: "Update Cache" (which is checked) and "Message Relay". At the bottom of the modal, there are "Cancel" and "Get Started" buttons. In the background, there's a list of devices: SRV1 (Windows 10 Pro), SRV2 (Windows 10 Pro), SRV3 (Windows Server 2019 Standard), and WinServer1 (Windows Server 2019 Standard). Each device entry includes a "Last Cache Update" timestamp (7 minutes ago, 8 days ago, etc.) and a "Message Relay" status (Active or Not Installed).

Select what you want to deploy. In this example, we will deploy only an Update Cache.

Deploy an Update Cache

The screenshot shows the Sophos Central web interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is currently selected). The main area is titled "Manage Update Caches and Message Relays". A modal window titled "Set Up Update Cache and Message Relay" is open. It contains instructions to ensure the server has at least 8 GB free disk space and ports 8190 and 8191 are available. It also states that a server must be set up as an Update Cache if it wants to be a Message Relay. There are two checkboxes: "Update Cache" (checked) and "Message Relay" (unchecked). Below these is a note about default assignments and a link to KB122577. At the bottom right of the modal are "Cancel" and "Set up" buttons, with "Set up" being highlighted with a red border.

Click **Set up**.

Installing, Configuring and Downloading

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected and highlighted in blue), Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, and Mobile. The main content area is titled "Manage Update Caches and Message Relays" under "Global Settings / Manage Update Caches and Message Relays". It contains a sub-header: "Configure devices to be used as update caches and message relays. [More info...](#)". A search bar and a dropdown menu for "Cache Capable Servers" are at the top. A prominent blue button labeled "Set Up Cache/Relay" is on the right. The main table lists five cache servers:

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY
DC 192.168.1.94 Windows Server 2022 S...	5 days ago	Not installed			Not installed
SRV 172.16.2.20 Windows Server 2016 S...	a month ago	Active	No devices	a month ago	Active
SRV2 192.168.1.245 Windows Server 2022 S...	18 days ago	Not installed			Not installed
SRV3 192.168.1.166 Windows Server 2022 S...	4 days ago	Active	2 Devices	4 days ago	Active
WinServer1 5 Devices	9 minutes ago	Installing	Triggered set up Update Cache X		

The device receives a new AutoUpdate policy and performs an update to download and install the Update Cache. This is indicated by the 'installing' cache status.

The next step is to download the Update Cache policy and configure the device.

Once configured, the Update Cache will download the software to the repo folder; this may take some time to complete.

Deploying a Message Relay

SOPHOS

Sophos Central

- Dashboard
- Alerts
- Threat Analysis Center >
- Logs & Reports
- People
- Devices
- Global Settings**
- Third-party Connectors
- Protect Devices
- Account Health Check

MY PRODUCTS

- Endpoint Protection >
- Server Protection >
- Mobile >

Manage Update Caches and Message Relays

Global Settings / Manage Update Caches and Message Relays

Configure devices to be used as update caches and message relays. [More info...](#)

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY
Windows Server 2022 S...	a month ago	Active	No devices	a month ago	Active
SRV 172.16.2.20 Windows Server 2016 S...	16 days ago	Not installed			Not installed
SRV2 192.168.1.245 Windows Server 2022 S...	4 days ago	Active	2 Devices	4 days ago	Active
WinServer1 172.16.16.10 Windows Server 2019 S...	8 minutes ago	Active	3 Devices	9 minutes ago	Not installed
5 Devices					

You can deploy a Message Relay to a device that has already been setup as an Update Cache by selecting the device and then clicking **Set Up Relay**.



Firewall Rules

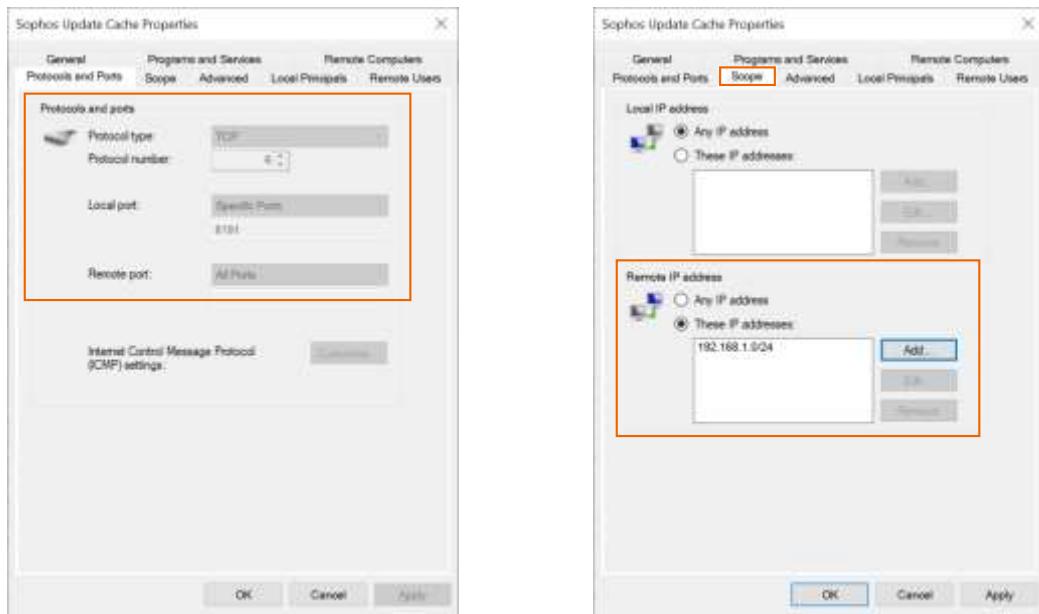
The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left navigation pane includes 'Inbound Rules' (selected), 'Outbound Rules', 'Connection Security Rules', and 'Monitoring'. The main table lists various firewall rules, with two specific entries highlighted: 'Sophos Message Relay' and 'Sophos Update Cache', both belonging to the 'Sophos' group and set to 'Allow' with 'All' profiles. The Actions pane on the right provides options for managing rules, including creating new ones and deleting existing ones.

Name	Group	Profile	Enabled	Action	Override
Remote Volume Management - Virtual Di...	Remote Volume Management	All	No	Allow	No
Remote Volume Management (RPC-EPMAP)	Remote Volume Management	All	No	Allow	No
Routing and Remote Access (GPO-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No
Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No
Secure Socket Tunneling Protocol (SSTP-In)	Secure Socket Tunneling Pro...	All	No	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Private...	No	Allow	No
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow	No
Software Load Balancer Multiplexer (TCP-In)	Software Load Balancer	All	No	Allow	No
Sophos Message Relay	Sophos	All	Yes	Allow	No
Sophos Update Cache	Sophos	All	Yes	Allow	No
Start	Start	Domain	Yes	Allow	No
Start	Start	Domain	Yes	Allow	No
TPM Virtual Smart Card Management (DC...	TPM Virtual Smart Card Man...	Private...	No	Allow	No
TPM Virtual Smart Card Management (DC...	TPM Virtual Smart Card Man...	Domain	No	Allow	No
TPM Virtual Smart Card Management (TCP...	TPM Virtual Smart Card Man...	Private...	No	Allow	No
TPM Virtual Smart Card Management (TCP...	TPM Virtual Smart Card Man...	Domain	No	Allow	No

As part of an Update Cache and Message Relay deployment, inbound firewall rules are added to the Windows firewall to allow TCP traffic to port 8191 for an Update cache and port 8190 for a Message Relay.

SOPHOS

Firewall Rules



SOPHOS

Details of the firewall rules can be viewed. The example shows the protocol and ports configured for the Update Cache rule. If required the rules can be modified to control access to the Update Cache and Message Relay.

This is achieved on the **Scope** tab of the rule properties by replacing the default of 'Any IP address' with the allowed IP addresses.

Installed Products

The screenshot shows the Sophos Central dashboard. On the left, there's a sidebar with 'Update Status' (last update: 14 July 2022 16:43), 'Products' (Message Relay 1.5.0.44, Server Anti-Virus 10.8.114, Server Core Agent 2.20.13, Server Intercept X 2021.3.1.11, Update Cache 1.8.0.422), and 'Troubleshooting' (Open Endpoint). A green callout box points to the 'Products' section with the text: 'View Cache and Message Relay products on the cache capable device using the Sophos Endpoint Agent'. On the right, the main area is titled 'Manage Update Caches and Message Relays' with a sub-section 'Cache Settings'. It lists several devices: DC (IP 192.168.1.94, Cache Status: Not Installed), SRV1 (IP 192.168.1.20, Cache Status: Active), SRV2 (IP 192.168.1.34, Cache Status: Not Installed), and SRV3 (IP 192.168.1.200, Cache Status: Active). A green callout box points to the 'Cache Status' column with the text: 'View Cache and Message Relay status in Sophos Central'. At the bottom right of the main area, there are 'Help' and 'About' links.

You can view the successful deployment of an Update Cache and Message Relay in Sophos Central by navigating to **Global Settings > Manage Update Caches and Message Relays**. The ‘Cache Status’ and ‘Message Relay Status’ will show as ‘Active’. You can also confirm the deployment on the cache capable device by opening the Sophos Endpoint Agent.

Click **About** in the bottom right-hand corner. A list of installed products is displayed. Update Cache and Message Relay should be listed.

Managing Devices

The screenshot shows the Sophos Central interface with the 'Global Settings' section selected in the sidebar. The main content area is titled 'Manage Update Caches and Message Relays'. It displays a table of 'Cache Capable Servers' with columns: DESCRIPTION, LAST ACTIVE, CACHE STATUS, USING THIS CACHE, LAST CACHE UPDATE, MESSAGE RELAY STATUS, and USING THIS RELAY. The table lists four servers: DC (192.168.1.84), SRV (172.16.2.20), SRV2 (192.168.1.245), and SRV3 (192.168.1.186). The 'USING THIS CACHE' column for SRV3 is highlighted with a red border. The 'Using This Cache' link for SRV3 is also highlighted with a red border.

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY STATUS	USING THIS RELAY
DC 192.168.1.84 Windows Server 2022 S...	5 days ago	Not installed			Not installed	
SRV 172.16.2.20 Windows Server 2016 S...	a month ago	Active	No devices	a month ago	Active	1 Device
SRV2 192.168.1.245 Windows Server 2022 S...	16 days ago	Not installed			Not installed	
SRV3 192.168.1.186 Windows Server 2022 S...	4 days ago	Active	3 Devices	4 days ago	Active	2 Devices
WinServer1 172.16.16.10 Windows Server 2019 S...	23 minutes ago	Active		15 minutes ago	Active	0 Devices

Protected devices will automatically use the closest Update Cache and Message Relay, however, you can manage which devices use the Update Cache and Message Relay manually if required.

This example shows that three devices are currently using the Update Cache. The number of devices in the 'using this cache' column is a clickable link.

Clicking on the link allows you to see which devices are using the Update Cache. You should view this a few hours following deployment to ensure that no devices are updating from an Update Cache that should not be.

Managing Devices

The screenshot shows the Sophos Central interface with the 'Global Settings' section selected in the sidebar. The main content area is titled 'Manage Update Cache and Message Relay' and displays a table of devices using 'WinServer1' as an update cache. The table includes columns for Name, Last Time Updated from Cache, Assignment Type, IP Address, Message Relay Status, and Device Type. One row is highlighted with an orange border, and a button labeled 'Manual assignment' is visible at the bottom right of the table.

Name	Last Time Updated from Cache	Assignment Type	IP Address	Message Relay Status	Device Type
WinClient4	In 10 minutes	Automatic	192.168.1.94	Not installed	4 Devices
WinClient2	In 10 minutes	Automatic	192.168.1.245	Not installed	2 Devices
WinClient3	In 18 minutes	Automatic	192.168.1.10	Not assigned	6 Devices

Here we can see information about the devices that are automatically using the Update Cache.

To manually manage devices that are using the Update Cache, click **Manual assignment**.

As Message Relays must be deployed with an Update Cache, assignments made for any Message Relay will also apply to the Update Cache.

Managing Devices

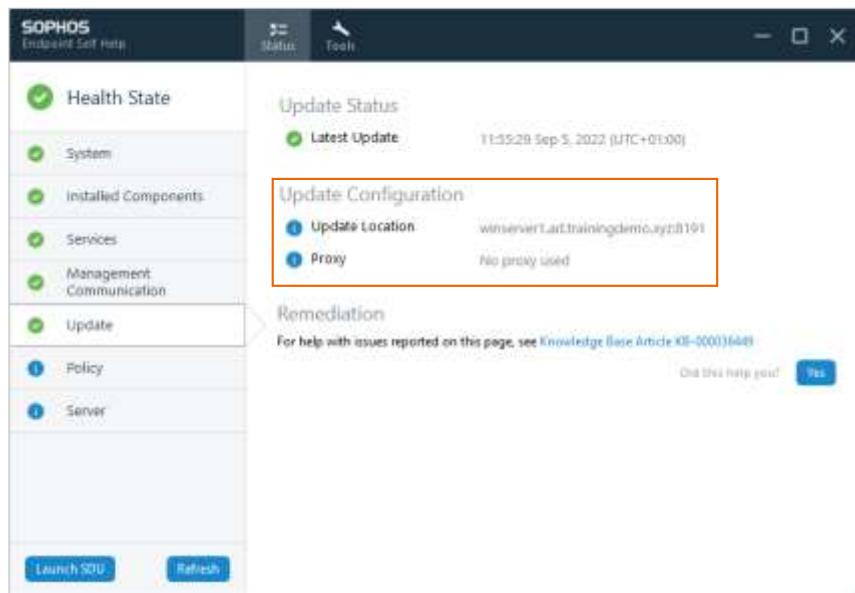
The screenshot shows the Sophos Central interface with the 'Global Settings' section selected in the left sidebar. A modal window titled 'Assign Devices Manually' is open, displaying two lists: 'AVAILABLE COMPUTERS' on the left and 'ASSIGNED COMPUTERS' on the right. In the 'AVAILABLE COMPUTERS' list, several devices are listed, including 'MN-6025A142964', 'SRV1', 'SRV2', 'SRV3', 'Training-Primary', 'Training-W10' (which has a checked checkbox), 'WinClient2', 'WinClient3', and 'WinClient4'. In the 'ASSIGNED COMPUTERS' list, 'WinClient1' and 'WinClient5' are listed. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

To assign devices manually, move them from the 'Available Computers' list in the left column to the 'Assigned Computers' list in the right column.

This function is most useful for overriding outlying devices that may be numerically close to an inappropriate Update Cache.

Please note that it is not possible to select computer groups for Update Cache and Message Relay assignment.

Managing Devices



SOPHOS

On a protected device, you can use the Endpoint Self Help Tool to check the updating and communication status.

On the **Update** tab, the ‘Update Configuration’ section displays the update location. If the device is using an Update Cache, the Update Cache server address is shown.

If the device is using Sophos to update, it will display Sophos in the update location.

Managing Devices

The screenshot shows the Sophos Endpoint Self Help application window. The left sidebar has a tree view with nodes: Health State (green checkmark), System (selected, grey background), Installed Components, Services, Management Communication, Update, Policy, and Server. Below the sidebar are two buttons: Launch SCD and Refresh. The main content area is titled 'Management Communication'. It shows a green status icon with 'Last Communication' and 'Succeeded at 11:53:47 Sep 5, 2022 (UTC+01:00)'. A section titled 'Connection Details' is highlighted with an orange border and contains three items: 'Server' (https://mcsl2-cloudstation-eu-west-1.gwthydra.sophos.com/sophos/management/api), 'Message Relay Address' (172.16.16.10), and 'Message Relay' (wmserver1.ad.trainingdemo.local). Below this is a 'Remediation' section with a link to 'Knowledge Base Article KB-000036450' and a 'Did this help you?' button with 'Yes' selected.

SOPHOS

On the **Management Communication** tab you can view whether a device is using a Message Relay.

The server address of the Message Relay server is displayed.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 4

True or False: Devices can be configured to use a different Message Relay from their Update Cache.

True

False

SOPHOS



Question 2 of 4

What is the best method for overriding outlying devices that may be numerically closest to an inappropriate Update Cache?

Assign devices manually

Change the firewall rules to
block the device

Change the IP address of the
device

Change the Update
Management Policy

SOPHOS



Question 3 of 4

What method can be used to change the devices that are able to connect to an Update Cache?

Assign devices manually

Modify the 'Scope' setting of
the firewall rule

Remove the devices from
those listed for the Cache

Change the Update
Management Policy

SOPHOS



Question 4 of 4

Which is the first step when deploying an Update Cache?

Download the installation package

Download the warehouse package from Sophos

Identify a cache capable server or computer

Change the Update Management Policy

SOPHOS

Chapter Review

Update Caches and Message Relays are **managed in Global Settings**. The **first stage** is to select a server or endpoint that is a '**Cache Capable Server**'.

Firewall rules are added to allow **TCP traffic** to port **8191** for an Update cache and port **8190** for a Message Relay. The **scope** for these rules can be **modified if required**.

Devices assign themselves automatically to use the Cache and Message Relay. This can be amended manually per device if required.

SOPHOS

Here are the three main things you learned in this chapter.

Update Caches and Message Relays are managed in Global Settings. The first stage is to select a server or endpoint that meets the requirements for being an Update Cache, referred to as a '**Cache Capable Server**'.

As part of the installation, firewall rules are added to allow TCP traffic to port 8191 for an Update cache and port 8190 for a Message Relay. The scope for these rules can be modified if required.

Devices assign themselves automatically to use an Update Cache and Message Relay. This can be amended manually per device if required.



Getting Started with Sophos Central Virtual Protection

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE2505: Getting Started with Sophos Central Virtual Protection

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Virtual Protection

In this chapter you will learn how Sophos Central can protect virtual machines running on-premise and in the Cloud.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Sophos Central Server Protection
- ✓ On-premise and/or cloud-based server virtualization

DURATION **8 minutes**

SOPHOS

In this chapter you will learn how Sophos Central can protect virtual machines running on-premise and in the Cloud.

Virtual Servers

On-Premise

- VMware vSphere/ESX
- VMware Workstation
- Microsoft Hyper-V Server
- Citrix XenServer

Cloud

- Amazon Web Services
- Microsoft Azure
- Google Cloud

SOPHOS

Sophos Central provides anti-malware and anti-ransomware protection to virtual servers in the same way it does for physical servers.

The servers may be hosted on-premise, using platforms such as VMware and Hyper-V, or hosted in the Cloud using Microsoft Azure, or Amazon Web Services (AWS).



Additional information in
the notes

On-Premise Virtual Machines



Server Workload Protection

Enhanced protection features including Server Lockdown, MTD, CryptoGuard

Example use: Endpoints with high-value data and exposure to multiple attack vectors

Recommended



Sophos for Virtual Environments

Ultra-thin guest agent with centralized threat protection

Anti-malware including Live Protection lookups, with automated threat clean-up

Lower resource overheads; enables higher VM density
Relief from scan storms and update storms

Example use: Endpoints with restricted access to lower value data and exposure to fewer attack vectors

SOPHOS

Sophos offers two approaches to protecting on-premise virtual machines.

The first option is to deploy the full Sophos Endpoint Agent on each virtual machine. This is the only option available for servers hosted on AWS and Azure.

The alternative, for servers hosted on VMware or Hyper-V, is to install the ultra-thin guest agent provided by Sophos for Virtual Environments (SVE) and deploy Sophos Security Virtual Machines (SVMs) to provide centralized threat protection.

Our recommendation is to protect all virtual servers with the full Sophos Endpoint Agent as the protection provided by the guest agent is limited in comparison.

[Additional Information]

Sophos for Virtual Environments is not supported after 20 July 2023.

Cloud-based Virtual Machines

STORING DATA

Storing files that were traditionally stored on physical servers



RUNNING WEB APPLICATIONS

Running web applications
Running websites
Providing web-based services



SOFTWARE DEVELOPMENT

Writing and testing code
Building software products



SOPHOS

A significant number of organisations now use virtual machines hosted in the public cloud. There are a few reasons for this, a few could be:

- As a replacement of physical servers. Instead of maintaining on-premise servers, organizations now store their data in the cloud
- For running web applications. This could be running a website or providing web-based services
- For Software development. Increasingly software engineers are developing software using public cloud servers as these are quicker and easier to build and remove

Security Challenges

Cloud Challenges

Dynamic environments

Infrastructure Evolution

Software Evolution

Security Challenges

Limited visibility

Manual compliance

Complex attacks

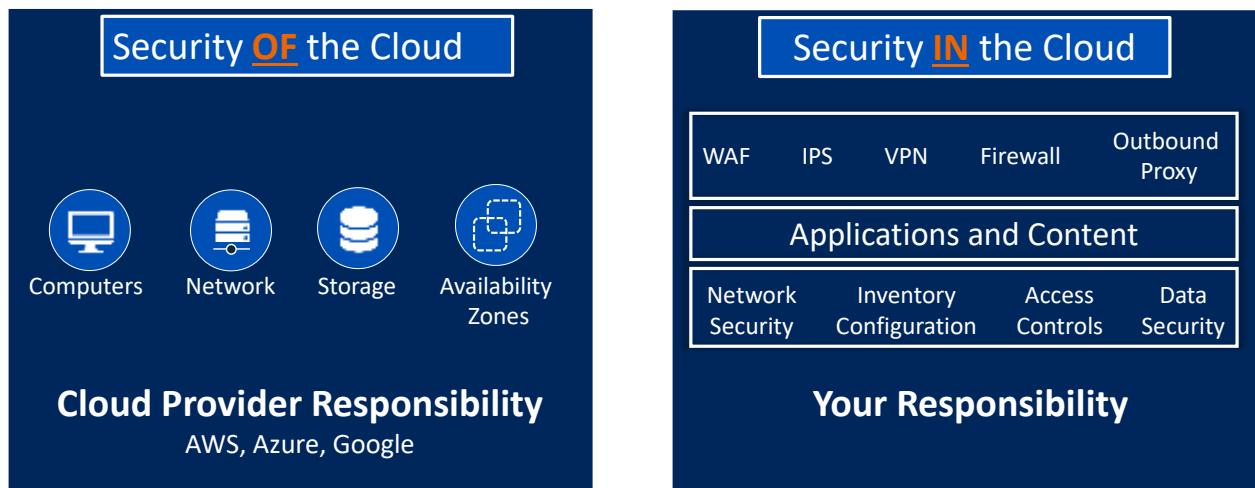
SOPHOS

There are several challenges that come with ensuring your cloud resources are secure.

The public cloud platform allows for dynamic environments, with multiple virtual machines starting and terminating regularly. This infrastructure can be hard to secure as you want to provide flexibility and functionality that does not expose your resources.

Because of the changing environment, you have limited visibility of what is happening and therefore have to manually ensure each virtual machine meets your compliance needs. This can take up a lot of time and whilst you are busy ensuring your network is secure, an attacker could be using complex attacks to compromise your resources.

Security Responsibility



SOPHOS

Securing your cloud environment is not all your responsibility. Typically, a cloud provider will take full responsibility for physical assets. For example, the security of data centres, storage, and network availability. However, they can only account for those things within their control.

The responsibility of providing a secure platform is shared when the platform is used within your environment. Most cloud providers provide tools to aid with security, however, the responsibility is with the user to ensure that the tools are implemented and that best practice recommendations are followed. For example, a cloud platform that allows public access is a valid environment, but for most organizations this will not provide a secure environment for their data and users.

Cloud providers are not all knowing, they rely on users to let them know what assets need protecting, to what standard of protection, and who should have access. Most providers supply recommendations for extended services via third party tools that enhance security.

Challenges for Cloud Server Protection

It is easy for users or services with appropriate permissions to deploy a virtual machine
For example:

- Developers working in the cloud deploying test virtual machines
- Autoscaling using temporary clones of a primary virtual machine

All virtual machines need to be protected

It is difficult for the security team to know how many virtual machines are deployed without the required protection

SOPHOS

In the cloud it is very easy for users or services with appropriate permissions to deploy a virtual machine. For example, developers working in the cloud may be deploying multiple test virtual machines. Alternatively, if autoscaling is being utilized, several temporary clones of a primary virtual machine could be deployed and suspended on demand.

In all cases any provisioned virtual machines need to be protected as you would a physical device. It can be difficult for a security team to know how many virtual machines are provisioned without the required protection.

Sophos Central Cloud Server Protection



Manage policies and visibility of workloads across different environments



Central management responds to autoscaling and transient VMs



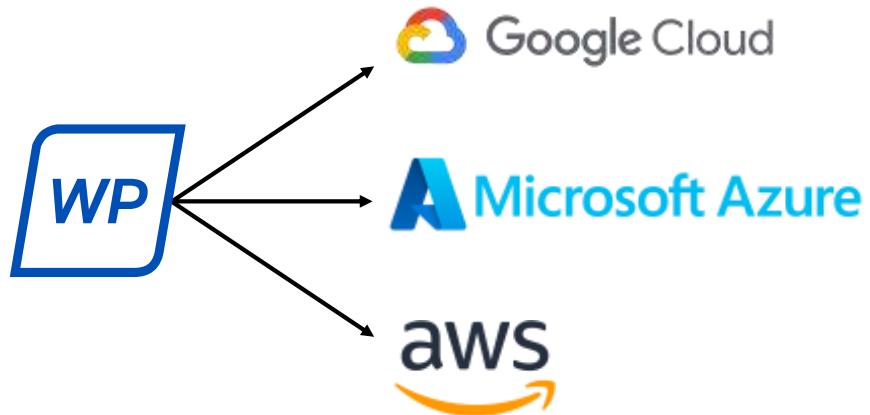
VMs Policies are automatically applied to auto-scaling instances

SOPHOS

Sophos Central allows you to secure virtual hosted Windows and Linux devices. Sophos Central policies can be applied to all devices regardless if they are virtual or physical, making deployment, configuration, and management quick and easy.

Sophos Central management responds to autoscaling and transient virtual machines by using policies that automatically apply to auto-scaling instances.

Cloud Deployment



Sophos provides scripted deployments independent of platform

SOPHOS

Virtual servers can be protected manually in the same way you protect a physical server. Sophos supports scripted and automatic installations with scripted deployment independent of the underlying platform.

If the script provided can run on the VM, Sophos can install the protection agent.

Cloud Deployment

Central Connectors allow you to connect your Sophos Central account to your AWS and/or Azure accounts. This provides integrated features such as dynamic licensing.

Integration with APIs helps with the challenge of workload protection by ensuring that all virtual machines have the Sophos Endpoint Agent installed.

SOPHOS

Additional functionality is provided when deploying the Sophos Security Agent onto AWS or Azure. Central Connectors allow you to connect your Sophos Central account to your AWS and/or Azure accounts which provide integrated features such as dynamic licensing where new machines receive a license from a pool of licenses, and terminated machines automatically have their license re-added to the pool of licenses.

Server protection allows integration with APIs to create new workloads. This helps with a key challenge in the cloud which is usually referred to as workload protection. At a high level this would be deploying the Sophos Endpoint Agent to protect virtual machines running in the cloud.

Sophos Cloud Protection Products



- Sophos Intercept X Advanced for Server with XDR
- Sophos Cloud Optix
- Sophos Firewall



- Sophos Intercept X Advanced for Server with XDR
- Sophos Cloud Optix
- Sophos Firewall



- Sophos Intercept X Advanced for Server with XDR
- Sophos Cloud Optix



- Sophos Intercept X Advanced for Server with XDR

SOPHOS

Sophos Intercept X Advanced for Server with XDR is part of multiple Sophos products available for Public Cloud. The protection provided can be complimented by Sophos Cloud Optix and Sophos Firewall.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

True or False: A different version of the installer must be used for servers hosted in the Cloud.

True

False

SOPHOS



Question 2 of 2

Which 2 of these Cloud platforms support integrated features such as dynamic licensing ?

Google Cloud

AWS

Oracle Cloud

Azure

SOPHOS

Chapter Review

Sophos Intercept X Advanced for Server provides anti-malware and anti-ransomware protection for virtual servers in the same way as it does for physical servers.

Sophos supports scripted and automatic installation with scripted deployment independent of the underlying platform.

Integration with APIs helps with the challenge of workload protection, ensuring that all virtual machines have the Sophos Endpoint Agent if needed.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos Intercept X Advanced for Server provides anti-malware and anti-ransomware protection for virtual servers in the same way as it does for physical servers.

Sophos supports scripted and automatic installation with scripted deployment independent of the underlying platform.

Integration with APIs helps with the challenge of workload protection, ensuring that all virtual machines have the Sophos Endpoint Agent if needed.



Protecting On-Premise Virtual Machines with Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE2520: Protecting On-Premise Virtual Machines with Central

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Protecting On-Premise Virtual Machines with Central

In this chapter you will learn how on-premise virtual machines can be protected using Sophos for Virtual Environments (SVE).

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to deploy the Sophos Endpoint Agent to devices
- ✓ Working with VMware and/or Hyper-V virtualization platforms

DURATION

17 minutes

SOPHOS

In this chapter you will learn how on-premise virtual machines can be protected using Sophos for Virtual Environments (SVE).

Two Approaches to Protecting Virtual Machines

Full Agent



Each guest VM has its own active anti-malware engine; meaning processing, RAM and disk storage is required on each GVM

Simultaneous scheduled or on-demand scans across multiple VMs can lead to a "scan storm"

Update storms can result in over-use of resources due to simultaneous updates

A master image may require substantial updates to become current

V's



Sophos for Virtual Environments



Inspection is off-loaded to a central Security VM. Each guest VM does not have its own engine

Scheduled scans across multiple VMs are staggered automatically

Updates to definitions take place on the Security VM only; guest agents do not require definition updates

The off-box approach means that the guest agent does not require frequent updates

SOPHOS

Sophos offers two approaches to protecting virtual machines.

The first option is to deploy the full Sophos Endpoint Agent on each guest virtual machine. This is the only option available for servers hosted by Amazon Web Services (AWS) and Microsoft Azure.

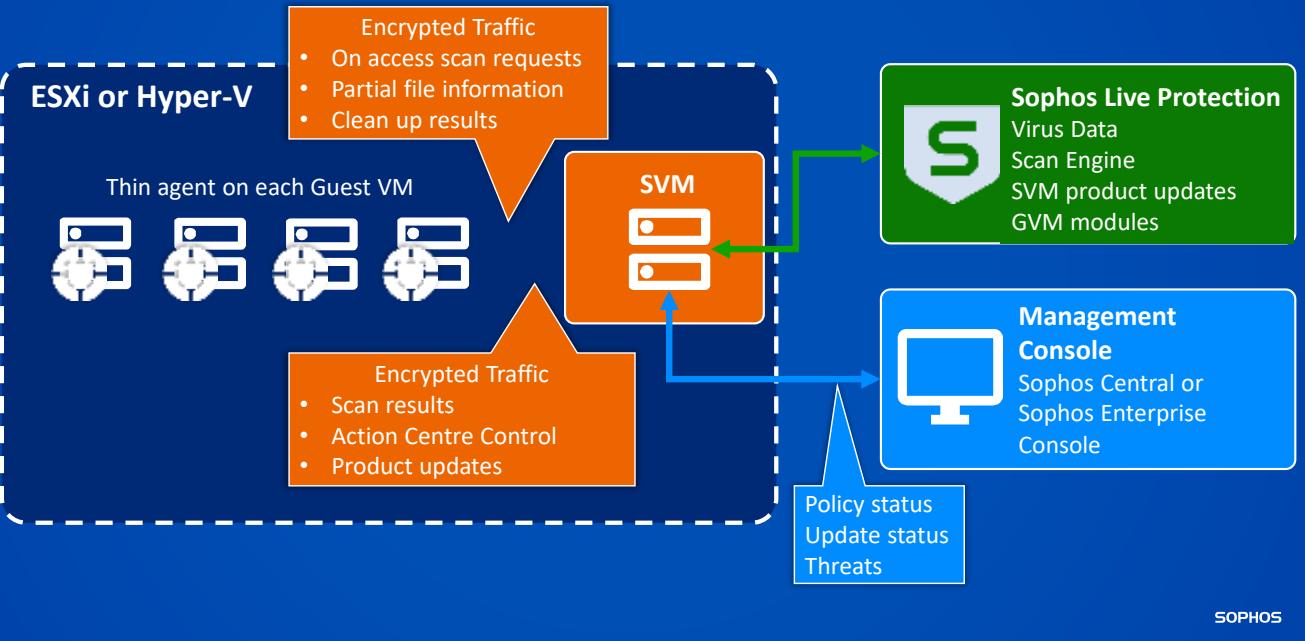
The alternative, for servers hosted using VMware or Hyper-V is to install the ultra-thin guest agent provided by Sophos for Virtual Environments and deploy Sophos Security Virtual Machines to provide centralized threat protection.

Our recommendation is to protect all virtual servers with the full Sophos Endpoint Agent as the protection provided by the guest agent is limited in comparison. However, for dynamic environments with large numbers of virtual servers, installing the Guest VM Agent on a template VM can reduce management time.

[Additional Information]

Sophos for Virtual Environments is not supported after 20 July 2023.

SVE Architecture

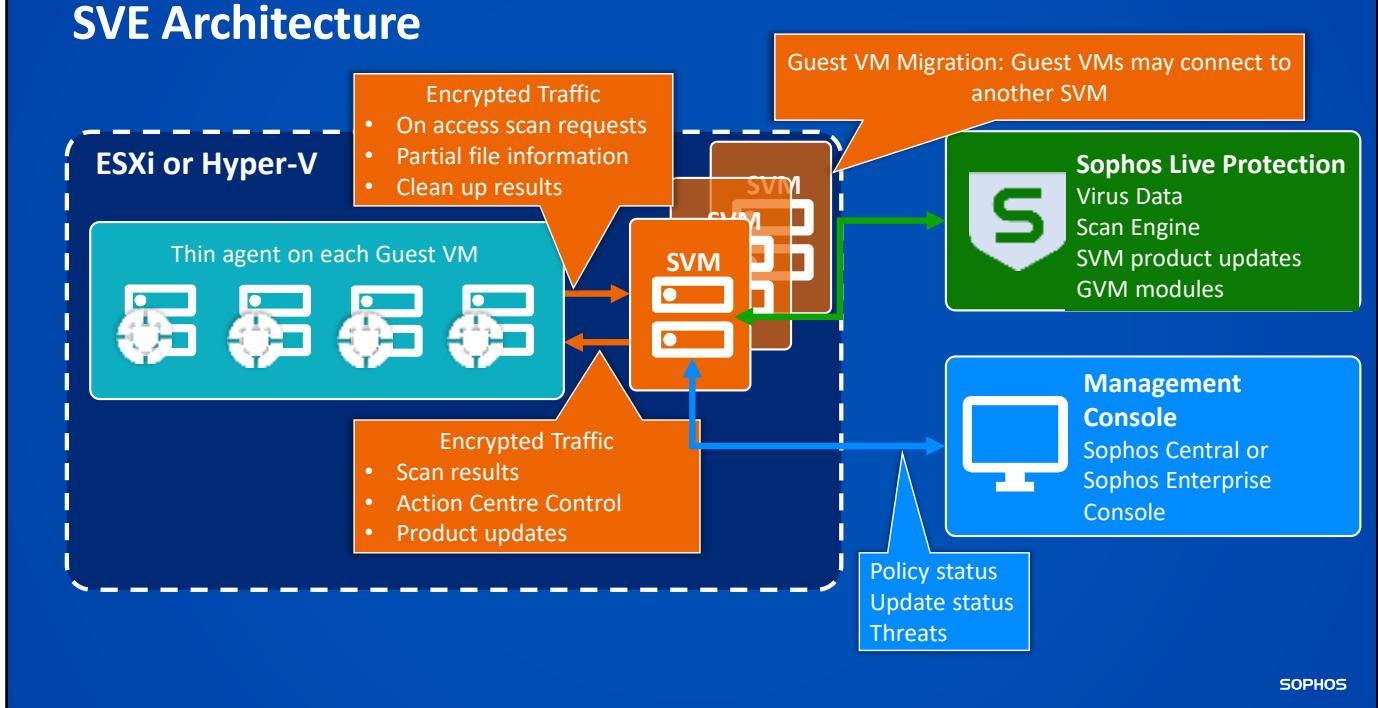


The SVM is a Sophos Security VM that will perform scanning, acting as a centralized resource for each of the Guest VMs. It is installed using a setup program on an existing VMware or Hyper-V server.

Please note that for VMware virtual environments the ESXi servers must be managed by vCenter.

Traffic between Guest VMs and the SVM is encrypted using AES 128.

SVE Architecture



If multiple SVMs are installed the Guest VMs can migrate between SVMs.



Required Firewall Ports

Security VM (SVM)

- Inbound
 - TCP 48651, 48652
 - Windows File and Printer sharing (ports 445 and 139)
 - TCP 80, 443 (HTTP, HTTPS)
- Outbound
 - TCP 80, 443 (HTTP, HTTPS)

Guest VM (GVM)

- Outbound
 - TCP 48651, 48652
 - Windows File and Printer sharing (ports 445 and 139)

SOPHOS

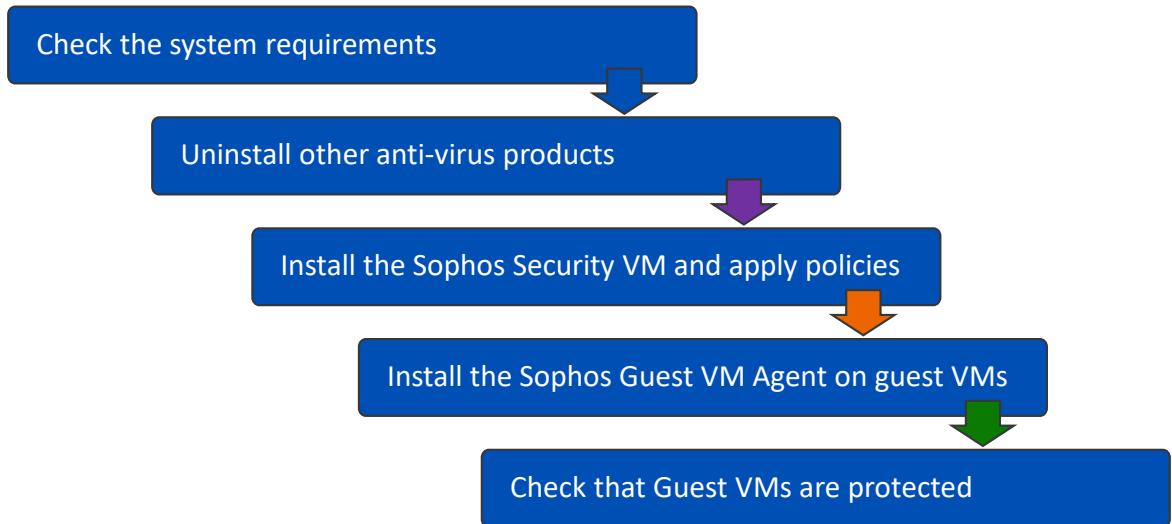
The Security VM and Guest VMs need to share a network connection.

The network traffic between Security VM and Guest VMs must not be blocked by firewalls. If the Security VM and Guest VM are separated by a firewall, several ports must be allowed to support communication.

[Additional Information]

The required firewall ports are shown on this slide and further information can be found in the knowledgebase article **KB-000036689**. <https://support.sophos.com/support/s/article/KB-000036689>

Deployment Steps



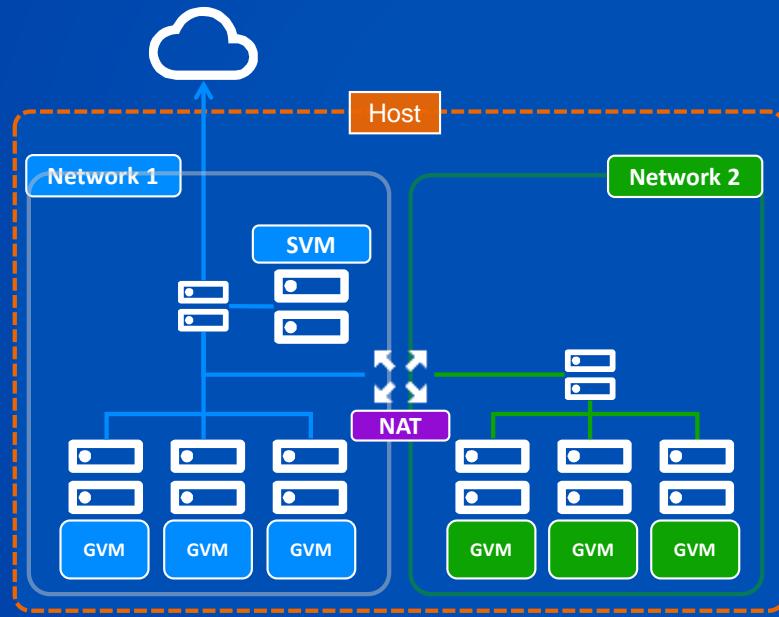
SOPHOS

The key steps required to deploy Sophos for Virtual Environments are:

1. Check the system requirements
2. Uninstall other anti-virus products
3. Install the Sophos Security VM and apply policies
4. Install the Guest VM agent on any guest virtual machines
5. Check that the guest VMs are protected



Deployment Scenario



You hope to deploy a single instance of the Sophos Security VM

1. Can Sophos Security VMs located on Network 1 be accessed by all Guest VMs in this scenario?
2. How many IP addresses will a Sophos Security VM require?
3. Should the primary IP address for a Sophos Security VM be the address for Network 1 or the address for Network 2?

SVE Start Up Guide

SOPHOS

Let's consider a network scenario, which is shown here. You want to deploy Security VMs on Network 1 and use these to manage Guest VMs on both networks. VMs on Network 2 have NATed connectivity to Network 1.

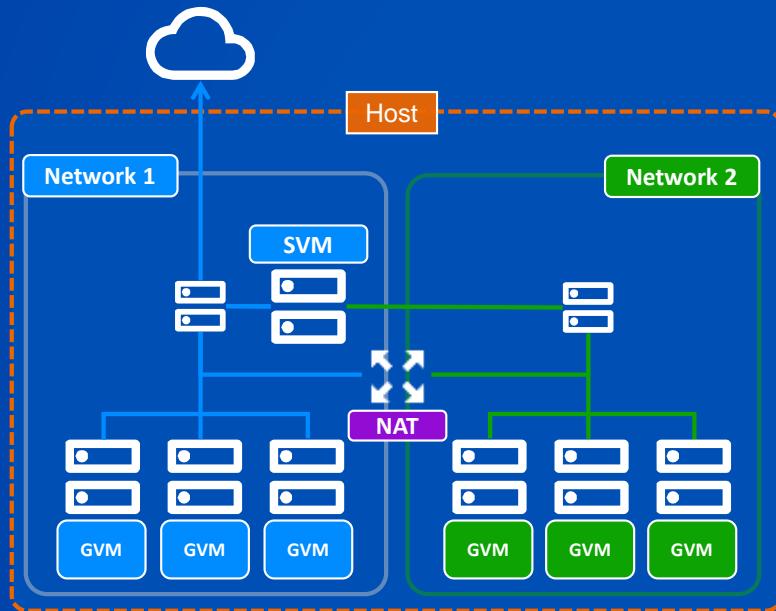
Use the Network requirements section of the **Sophos for Virtual Environments – Startup Guide** to answer the questions below:

- Can Sophos Security VMs located on Network 1 be accessed by all Guest VMs in this scenario?
- How many IP addresses will a Sophos Security VM require for this scenario?
- Should the primary IP address for a Sophos Security VM be the address for Network 1 or the address for Network 2?

[Additional Information]

The startup guide is available here: https://docs.sophos.com/esg/Sophos-Virtual-Environments/1-3/central-startup/en-us/sve_central_sg.html

Deployment Scenario



Answers

1. Can Sophos Security VMs located on Network 1 be accessed by all Guest VMs this scenario?
Yes
2. How many IP addresses will a Sophos Security VM require?
Two, one for each network
3. Should the primary IP address for a Sophos Security VM be the address for Network 1 or the address for Network 2?
Network 1, as that has access to Sophos Central

SOPHOS

Question one. Yes, you can install Security VMs on Network 1, however the SVM must have an IP address on the NATed network.

Question two. A Sophos Security VM will require 2 IP addresses in this scenario, one for each of the networks.

Question three. The primary IP address should be on Network 1 as this will be used to access Sophos Central.

Security VM Installer

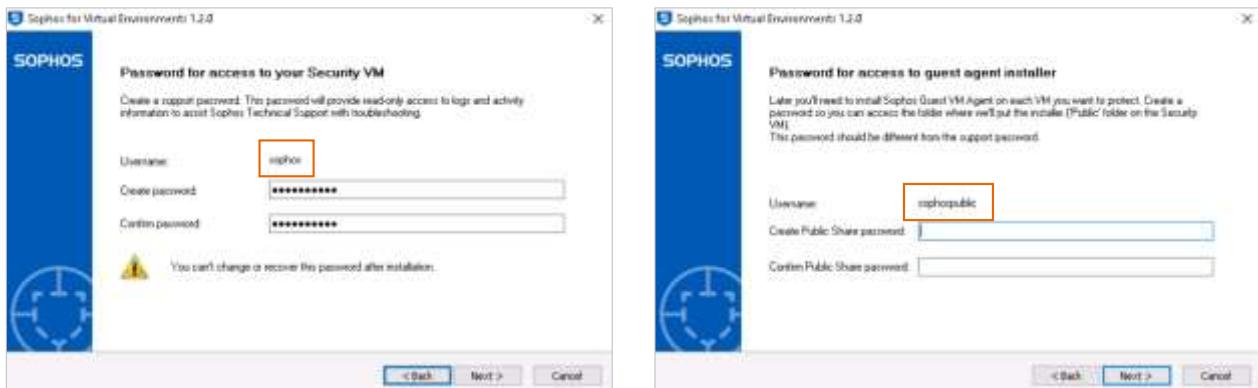
The screenshot shows the Sophos Central web interface. On the left, there's a sidebar with 'Overview' and 'Protect Devices' selected. Below that is a 'VMWARE' section with various protection options like Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, and Email Gateway. The main content area has sections for 'Cloud Optin', 'Server Protection', and 'Sophos for Virtual Environments'. A green callout box points to the 'Sophos for Virtual Environments' section, stating 'The installer is not linked to the Central account'. In this section, there are two download links: 'Download Security VM Installer for Hyper-V' and 'Download Security VM Installer for ESXi', with the Hyper-V link highlighted by a red box.

SOPHOS

The installer for the Security VM can be downloaded from your Sophos Central account.

Unlike the other installers, the security VM installer is not linked to the Central account. The installer prompts for entry of the Central administrator email and password to determine the account.

Security VM Installer



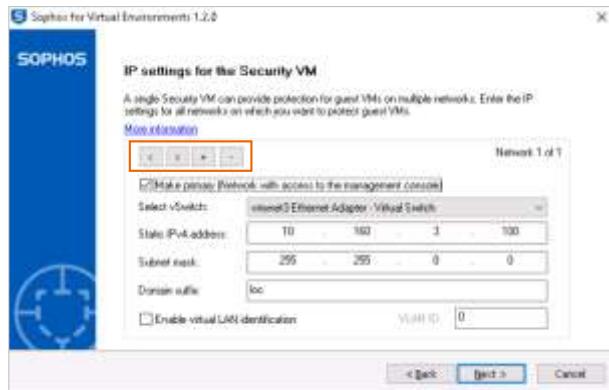
SOPHOS

The installer prompts for two account passwords which are used to access the Security VM.

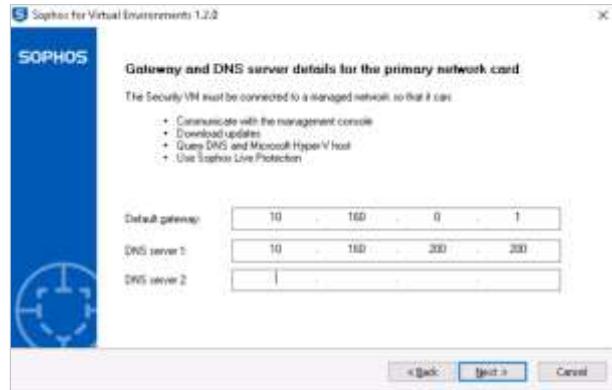
The first is for the sophos user, which is used for administrative access to the Security VM. Logging in with this account allows access to the logs share and allows console access to the Security VM.

The second account is sophos public, which has access to the public share containing the Guest VM installer.

Security VM Installer



- IPv4 settings for up to 5 network interfaces
- The primary network is used for access to Sophos Central



- Gateway and DNS settings for the primary network interface

SOPHOS

Security VMs can be configured with up to 5 IP addresses. Each IP address must be on a different subnet and be associated with a vSwitch (for Hyper-V) or Virtual LAN (for ESXi). A static IPv4 address is required. A domain suffix must also be provided, for example com, co.uk, or net. This will assist in routing to the Security VM using DNS or NETBIOS.

Enabling Virtual LAN Identification allows you to use the features of Hyper-V VLAN IDs. This allows machines sharing one network connection to use different virtual networks over the same connection. The controls at the top of the page allow you to navigate backward and forward, and to add and/or remove network connections as required.

Select **Make Primary** for the network that should have access to Sophos Central. You can only have one primary network. If you have guest VMs inside a NATed network, you can protect them with a Security VM inside or outside of that network.

During installation you must configure the Security VM with the following:

- a primary IP address outside of the NAT, which must be able to communicate with Sophos Central
- A secondary IP address that is within the NAT

In the Gateway and DNS server details for the primary network card, enter details that will enable the Security VM to communicate with the Management Console and to download updates.

Guest VM Installation

Once the Security Virtual Machine has been successfully deployed; the installer can be located in:
\\<SVM IP ADDRESS>\public\

Replace <SVM IP ADDRESS> with the IP address of the primary network card specified in the Security Virtual Machine installation process.

This share will need authentication using either the 'sophos' or 'sophospublic' accounts set up during the installation of the SVM.

SOPHOS

Once the Security Virtual Machine has been successfully deployed, the installer is saved in the public share on the SVM.

Replace the IP address of the primary network card specified in the Security Virtual Machine installation process. If you are using the Guest VM Migration functionality, then this address can be the facing address of any of the migration-enabled Security VMs you specified during installation.

This share will need authentication using either the sophos or sophospublic accounts set up during the installation of the SVM.

Guest VM Migration

SOPHOS

How Does a GVM Select an SVM?

GVMs evaluate available Security VMs

- Can it connect to the security VM IP address?
- Is the SVM healthy and able to provide scanning services?
- Can the SVM provide reasonable performance

Reasons for loss of connectivity

- The SVM is shutdown or rebooted
- A network failure
- The GVM is migrated to a different host and the network connection is prevented by a firewall

SOPHOS

Each guest virtual machine will evaluate the list of available security virtual machines to determine the following:

- If it can connect to the Security VM IP address
- If the Security VM is healthy and can provide scanning services
- If the Security VM can provide reasonable performance. Security VMs that are likely to degrade scanning performance due to having increased latency are de-prioritised

Based on these criteria the guest VM will then choose a good security VM to connect to. The guest VM will periodically evaluate security VM's to determine if anything has changed. If the state of a Security VM currently providing protection has changed, the guest VM will migrate to a better Security VM.

Guest VM Migration

Forced Migration/Fail Over

- Guest VM loses connection to its current SVM
- Fails over to the next available SVM

Elective Migration

- Adding new SVMs
- Powering on SVMs
- Restarting SVMs
- Security VM health
- Latency

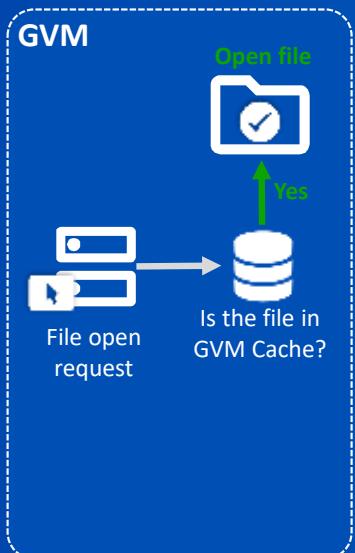
SOPHOS

Guest VM migration can occur under several circumstances.

Forced Migration or Fail Over. If a guest VM loses its connection to the Security VM it is currently connected to, then it will fail over to the next available Security VM, in order to maintain protection

Elective Migration. When an SVM is added, powered on or restarted, this triggers GVMs to redistribute to use the newly available SVM. If certain key processes on a Security VM are not available due to a failure on the Security VM, then it will report to the guest VMs as unhealthy, and the connected guest VMs will migrate away to a different healthy Security VM for protection. If the latency of the GVM's connection to its current SVM becomes significantly degraded, the GVM will move to an SVM with which it can form a better latency connection.

Caching for Efficient Performance

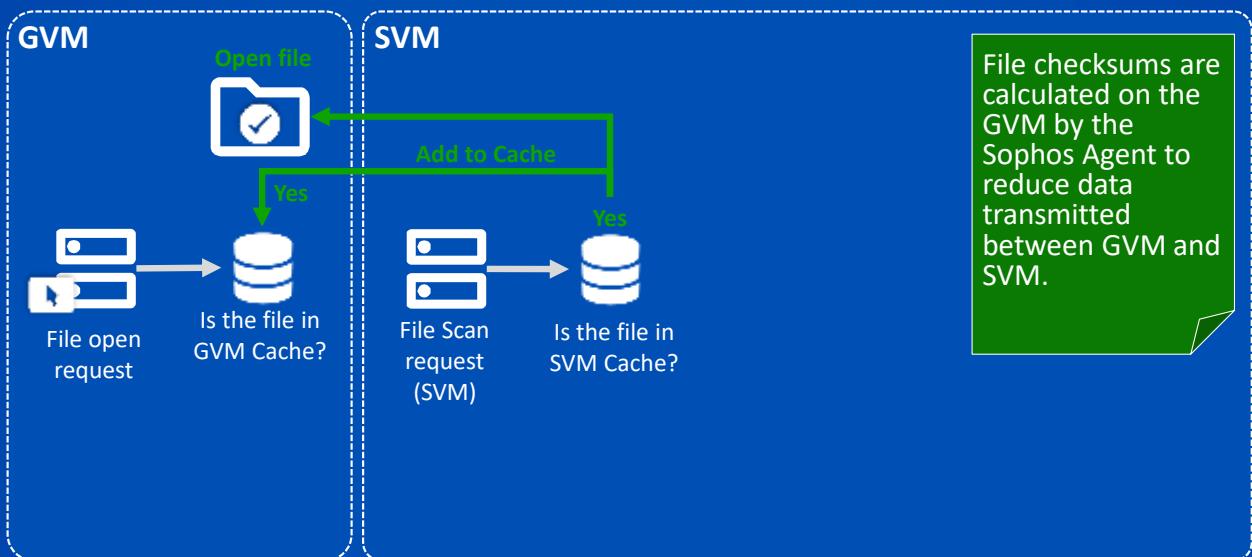


SOPHOS

SVE uses multiple layers of caching to optimise performance. Let's look at how this works.

The first level of caching is completed on the GVM. When a file open request is processed, the agent checks the local cache. If it can find a match it will allow the file to be opened. In this case the SVM does not have to take part in the process.

Caching for Efficient Performance



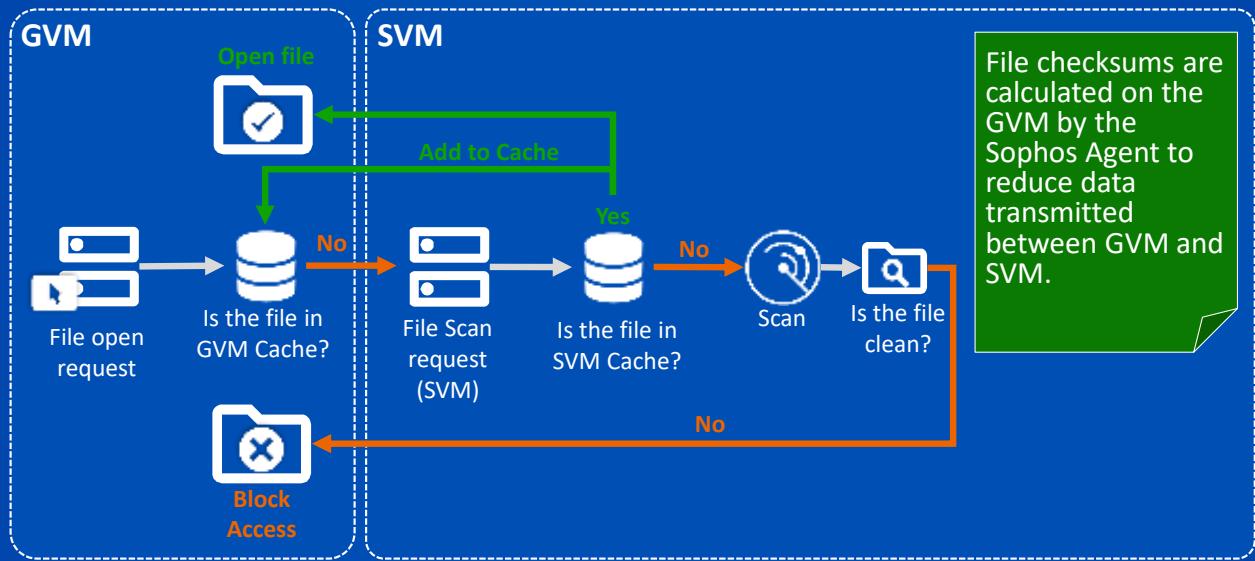
SOPHOS

The second layer of caching is completed on the SVM. This contains data on all of the files it has scanned for all of the GVMs it serves which provides efficiency.

If the GVM does not have the file in its local cache, the GVM calculates an MDS checksum of the file and sends this checksum to the SVM.

If the SVM finds the file in its cache, the checksum is added to the local GVM cache and the file is allowed.

Caching for Efficient Performance



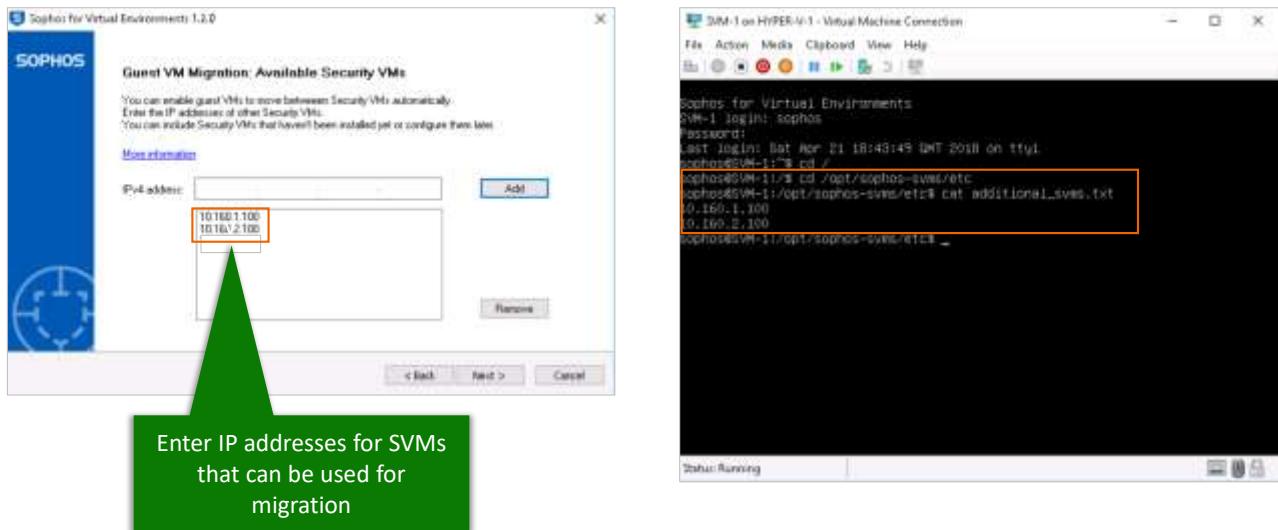
If no record of the file is in the SVM cache, it will identify the file type from the header, then flag certain blocks within the file that are required for scanning. The SVM then requests those blocks from the GVM to scan.

Once the engine on the SVM has scanned the file, it puts the results in the SVMs scan cache and sends the response back to the GVM, allowing or blocking access as appropriate.

If the file is clean, the GVM adds an entry into its local cache.

Both SVM and GVM caches are purged when there are engine or data updates. The first GVM that hits a file for the first time after an data update takes the hit, (on that file). All other GVMs then take the benefit. The system is designed so the process will be spread across many machines making it less noticeable.

How To Select Available SVMs for GVM Migration



The installation prompts for the IP addresses of any security VMs that can be used for migration. IP addresses can be entered for SVMs that have not yet been deployed. Please note we do not limit the number of SVMs you deploy or include in an availability group.

If a new SVM is deployed that has not been added using the GUI, the additional SVMs text file should be modified on each SVM to include the additional IP address.

How To Select Available SVMs for GVM Migration

Connect to the SVM console and log on as the '**sophos**' user

Open the **additional_svms.txt** configuration file for editing: /opt/sophos-svms/etc/additional_svms.txt

Edit the file to **add or remove IP addresses of Security VMs that are available to protect migrating guest VMs**

- Put one IP address per line with no additional separating characters. For example:
 - 1.2.3.4
 - 5.6.7.8
- The IP addresses for the current Security VM do not need to be included

Save and close the file

Check the SVM log (/var/log/ssvm.log) to see if there were any errors in processing the additional Security VMs list
If there are no errors, the updated list is sent to all connected guest VMs so they can get protection from the new Security VMs

SOPHOS

To select available SVMs for GVM migration, follow these steps:

- Connect to the SVM console and log on as the **sophos** user
- Open the **additional_svms.txt** configuration file for editing
- Edit the file to add or remove IP addresses of Security VMs that are available to protect migrating guest VMs
 - One IP address per line with no additional separating characters
 - The IP addresses for the current Security VM do not need to be included
- **Save and close** the file
- Check the SVM log to see if there were any errors in processing the additional Security VMs list. If there are no errors, the updated list is sent to all connected guest VMs so they can get protection from the new Security VMs

[Additional Information]

Additional_svms.txt file location: /opt/sophos-svms/etc/additional_svms.txt

Location for the svm log: /var/log/ssvm.log

Best Practice

SOPHOS

Best Practice

DO	DON'T	TIPS
<ul style="list-style-type: none">▪ Power on SVMs manually following downtime▪ Power on SVM before GVMs, so that the GVMs are protected immediately▪ Verify that the SVM is receiving Sophos updates▪ Exclude the SVM from backups	<ul style="list-style-type: none">▪ Suspend the SVM. GVMs will lose protection unless migration is configured▪ Power on GVMs before the SVM is available	<ul style="list-style-type: none">▪ If the SVM needs to be recovered<ul style="list-style-type: none">▪ Redeploy the SVM using the same IP address▪ GVMs will reconnect when it is available

SOPHOS

Sophos recommends the following best practice for Security VM maintenance:

- Power on a SVM manually whenever the host is taken out of maintenance or standby mode. Do this before you power on any GVMs, to ensure they are protected immediately
- Do not suspend the SVM. If you do, communications with the management software will not be able to resume later
- Verify that the SVM is receiving security updates from Sophos. You can do this by checking its update status in Sophos Central
- An SVM should be excluded from regular backup tasks which can degrade the performance
- If an SVM needs to be recovered due to infrastructure failures, re-deploy the SVM. GVMs will connect to the re-deployed SVM provided the same IP address is used



Additional information in
the notes

Threat Protection Policy

- Available policy settings differ for Sophos for Virtual Environments
- Examples below are from Realtime Scanning settings

Realtime scanning*



Scan local, or scan local and remote*



Realtime scanning - Internet



Detect malicious behaviour (HIPS)



Live protection*



Automatic clean up



*Realtime scanning can be enabled/disabled

*Scan local and remote includes files in network shares

*Live protection can be enabled/disabled

SOPHOS

By default, Sophos Central applies a base Threat Protection policy to all your Security VMs. The settings in the policy are then used for the guest VMs.

These settings offer:

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

If required, additional policies can be created which can be used to customize settings.

[Additional Information]

There are some differences in the threat protection policy settings that apply for SVE:

http://docs.sophos.com/esg/virtual-environments/1-2/Central-Help/en-us/esg/Sophos-Virtual-Environments/concepts/Configuring_policy_central.html

Sizing Guidelines

The number of SVMs required depends on the infrastructure

Add SVMs to spread the load

No more than 500 GVMs per SVM

SOPHOS

The number of SVMs required will depend on the infrastructure it is being deployed on and will be based on the load on the SVMs.

You can then add additional SVMs to spread the load.

We don't have a limit on the number of GVMs associated with an SVM. However, we recommend having no more than 500 GVMs per SVM.



Sizing Guidelines

Checking SVM load

Login to the SVM and run
`nproc`

Example Output: 2

Run `cat /proc/loadavg`

Example output from a normal SVM
0.76 0.26 0.09 1/317 1730

Example output from an overloaded SVM
5.61 2.30 0.87 1/293 9498

SOPHOS

To check the load of an SVM to see if you need to deploy additional SVMs, start by logging in and running the nproc command. This will display the number of processing units available, which is the number of threads multiplied by the number of cores per socket multiplied by the number of sockets. For a single core CPU with hyperthreading you would expect to see 2.

You then need to run the command shown here, to see the load averages for the SVM. The first number is the most important because it shows the load over the last minute. The second and third numbers show the average load over the last 5 and 10 minutes, respectively. The first number should be less than the output of the command.

In the second example which shows the output from an overloaded SVM, the first number is greater than the output of the command showing that it is overloaded.

[Additional Information]

See knowledgebase article **KB-000037978** for more information.

<https://support.sophos.com/support/s/article/KB-000037978>

Here is an example output from a normal SVM:

0.76 0.26 0.09 1/317 1730

Here is an example output from an overloaded SVM

5.61 2.30 0.87 1/293 9498

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Which 2 of the following protection features are supported in GVMs protected by SVE?

Automated threat clean up

Malicious traffic detection

Exploit prevention

Live protection

SOPHOS



Question 2 of 2

You have an existing Sophos Central deployment and have configured your firewalls to allow the communication required by this. You now want to deploy SVE. Which 2 additional TCP ports should be allowed on any firewall located between SVMs and GVMs?

139

445

8192

8194

48651

48652

SOPHOS

Chapter Review

Sophos offers **two approaches to protecting virtual machines**: for AWS or Azure deploy the full server or endpoint agent on each guest virtual machine.

For VMware or Hyper-V an alternative is to install the **ultra-thin guest agent** for Virtual Environments (SVE) and deploy Sophos Security Virtual Machines (SVMs) to provide centralized protection.

Sophos recommends using the Sophos Endpoint Agent. However, for dynamic environments with large numbers of virtual servers, installing the Guest VM Agent on a template VM can reduce management time.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos offers two approaches to protecting virtual machines: for AWS or Azure deploy the full server or endpoint agent on each guest virtual machine.

For VMware or Hyper-V an alternative is to install the ultra-thin guest agent for Virtual Environments and deploy Sophos Security Virtual Machines to provide centralized protection.

Sophos recommends using the Sophos Endpoint Agent. However, for dynamic environments with large numbers of virtual servers, installing the Guest VM Agent on a template VM can reduce management time.



Getting Started with Sophos Central Device Management

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3005: Getting Started with Sophos Central Device Management

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Device Management

In this chapter you will learn how to view device details and create computer and server groups.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to deploy Sophos protection to devices

DURATION **9 minutes**

SOPHOS

In this chapter you will learn how to view device details and create computer and server groups.

Devices Summary

The screenshot shows the Sophos Central Dashboard with a sidebar on the left containing navigation links like Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, Account Health Check, Endpoint Protection, Server Protection, and Mobile. The main area features a large orange-bordered 'Devices and users: summary' card. This card includes a circular gauge showing '7 Active' devices, a bar chart for 'Endpoint Computer Activity Status' with the following data:

Status	Count
Active	7
Inactive 2+ Weeks	0
Inactive 2+ Months	0
Not Protected	0

Below this are sections for Cloud Security Posture Management (with a link to the product dashboard) and Unified Endpoint Management (with a link to the product dashboard). A 'Device Platforms' section is also visible at the bottom.

The 'Devices and users: Summary' widget on the Sophos Central Dashboard displays at-a-glance information about protected devices, users, and servers.

The widget displays device data based on activity status. The **See Report** link takes you directly to the computer report which provides further details on protected devices.

Devices

The screenshot shows the Sophos Central interface. On the left, a sidebar menu is open with several options: Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, and Devices. The 'Devices' option is highlighted with a blue box. The main content area is titled 'Computers' with the subtitle 'View and manage your computers'. At the top right, there are links for Help, Simon Smith (Sophos UK - Super Admin), and a sign-out button. Below the title, there are tabs for Computers, Mobile Devices, Servers, and Unmanaged devices. A toolbar includes Manage Endpoint Software, Turn on temporary protection, Retrieve Recovery Key, Reset health status, Delete, and Export to CSV. A search bar is also present. The main table lists seven computers: WinClient5, WinClient1, WinClient3, and WinClient2. Each row includes columns for Name, IP, OS, and protection status. All four clients are listed with 'Intercept X Advanced with XDR' checked. The table footer shows '1-7 of 7 computers / 0 selected' and navigation icons. The bottom right corner indicates the last update was on Aug 22, 2022, at 2:13 PM.

Name	IP	OS	protection
WinClient5	172.16.16.110	Windows 10 Pro	✓ Intercept X Advanced with XDR
WinClient1	172.16.16.70	Windows 10 Pro	✓ Intercept X Advanced with XDR
WinClient3	172.16.16.90	Windows 10 Pro	✓ Intercept X Advanced with XDR
WinClient2	172.16.16.80	Windows 10 Pro	✓ Intercept X Advanced with XDR

Navigating to **Devices** in the left hand menu displays a list of protected devices by the Sophos Central account.

This list can be filtered.

Manage Endpoint Software

The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, and Devices (which is selected). Under Devices, there are links for Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below this, MY PRODUCTS lists Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'Computers' with the sub-instruction 'View and manage your computers'. It features tabs for Computers, Servers, Mobile Devices, and Unmanaged devices. A prominent orange box highlights the 'Manage Endpoint Software' button, which is located in the top navigation bar above the device list. The device list table shows 8 items, with one row highlighted in blue. The table columns include Device Name, IP Address, OS Version, and Protection status. A green callout box points to the 'Managed Endpoint Software' text in the table header. The bottom right of the screen shows the last update time as 'Nov 9, 2022, 11:45 AM'.

Managed Endpoint Software				
	Device Name	IP Address	OS Version	Protection
<input type="checkbox"/>	macOS Monterey 12.6			<input checked="" type="checkbox"/> Intercept X Advanced with XDR
<input checked="" type="checkbox"/>	WinClient1	172.16.16.70	Windows 10 Pro	<input checked="" type="checkbox"/> Intercept X Advanced with XDR
<input type="checkbox"/>	Training-W10	192.168.1.250	Windows 10 Enterprise	<input checked="" type="checkbox"/> Intercept X Advanced with XDR
<input type="checkbox"/>	WinClient5	172.16.16.110	Windows 10 Pro	<input checked="" type="checkbox"/> Intercept X Advanced with XDR

You can manage your devices in Sophos Central in the devices page.

Selecting a device from the list will display additional options that are available for the device. To manage the software installed on a device, click **Manage Endpoint Software**.

Manage Endpoint Software

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices (which is selected), Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for Products (Endpoint Protection, Server Protection, Mobile) and Integrations (Filebeat, Logstash, Splunk). The main area is titled 'Computers' and shows a list of devices: WinClient5, WinClient6, WinClient7, WinClient8, WinClient9, WinClient10, WinClient11, and WinClient12. Each device has a status icon (green for online), IP address, and operating system (Windows 10 Pro). A search bar and a 'Protection' dropdown are also present. A modal window titled 'Manage Endpoint Software' is open over the list, prompting the user to 'Choose what to do on the device you selected.' It contains a dropdown menu for 'Protection' with four options: 'Do not change' (selected), 'Intercept X Advanced with XDR', 'XDR Sensor', and 'No protection (Remove any current protection)'. There are 'Cancel' and 'OK' buttons at the bottom of the modal.

From the protection drop-down menu you can select to change the protection of a single device or multiple devices.

The protection options include software that you can install on devices that are already protected with Sophos Central. You can choose to remove the protection of a managed device.

Manage Endpoint Software

The screenshot shows the Sophos Central interface. On the left, the navigation bar includes sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices (which is selected), Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under 'Our Products', there are links for Endpoint Protection, Server Protection, and Mobile. The main area is titled 'Computers' with the sub-section 'Manage Endpoint Software'. A modal window titled 'Manage Endpoint Software' is open, prompting the user to 'Choose what to do on the device you selected.' It has two dropdown menus: 'Protection' set to 'Do not change' and 'Encryption' also set to 'Do not change'. A dropdown menu for 'Encryption' is open, showing options: 'Do not change' (selected), 'Install', and 'Uninstall'. In the background, a list of computers is visible, including 'WinClient5' (Windows 10 Pro) which is selected. The top right corner shows help links ('Help', 'UK Training'), a user account ('Sophos UK - Super Admin'), and export options ('Export to CSV').

Encryption software is included in the full installer that can be downloaded from Sophos Central.

If you select to install only specific components, you may find that devices do not have encryption installed. You can select from the drop-down menu to either install or uninstall encryption.

Manage Endpoint Software

The screenshot shows the Sophos Central web interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, and Devices (which is currently selected). The main area is titled 'Computers' and shows a list of devices. A modal window titled 'Manage Endpoint Software' is open over the list. The modal has sections for 'Protection' (set to 'do not change') and 'Encryption' (set to 'Universal'). It includes a note: 'Note: We won't install software on devices that do not support it. This may be applicable depending on the selection you make.' Below this is a progress bar indicating '1 / 1 Devices Updated'. At the bottom of the modal are 'Cancel' and 'Save' buttons. The background list of devices shows names like 'niberraccor', 'Sophos', 'Training', and 'TrainingDemo', along with their last active times.

Once you select to change the endpoint protection you will see a progress bar.

Please note that you cannot install software on a device that does not support it.

Manage Endpoint Software

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Sophos Central' and several menu items: Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices (which is selected), Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'Computers' with the sub-instruction 'View and manage your computers'. At the top of this area are tabs for Computers (selected), Servers, Mobile Devices, and Unmanaged devices. Below these are buttons for Manage Endpoint Software, Turn on tamper protection, Retrieve Recovery Key, Reset health status, Delete, and Export to CSV. A search bar with a 'Search' placeholder is also present. The main table lists 8 computers, each with columns for Protection, Encryption, Last user, Last active, and Group. The first four rows show Intercept X Advanced with XDR protection, while the last four show Intercept X Advanced with XDR encryption. The 'Encryption' column contains a plus sign (+) for each row. The 'Group' column shows 'Office Workers' for the first two rows and 'Reading Office' for the last two. The table footer indicates '1 - 8 of 8 computers / 1 selected' and includes navigation icons for sorting and filtering.

Protection	Encryption	Last user	Last active	Group
✓ Intercept X Advanced with XDR	+	Sophos	Nov 7, 2022 5:11 PM	Office Workers
✓ Intercept X Advanced with XDR	+	Training	Nov 6, 2022 6:04 PM	Reading Office
✓ Intercept X Advanced with XDR	+	TrainingDemo	Nov 4, 2022 4:57 PM	
✓ Intercept X Advanced with XDR	+	anoble	Nov 4, 2022 4:55 PM	
✓ Intercept X Advanced with XDR	+			
✓ Intercept X Advanced with XDR	+			
✓ Intercept X Advanced with XDR	+			

In the encryption column of the device list, you can select to add the encryption software to a device or multiple devices if required.

Device Details

The screenshot shows the Sophos Central interface. On the left is a sidebar with 'SOPHOS' and 'Sophos Central' sections, and 'MY PRODUCTS' with categories like Endpoint Protection, Server Protection, Mobile, Encryption, and Wireless. The main area is titled 'WinClient1' under 'Devices'. It features a summary card with device status (green checkmark), operating system (Windows 10), IP address (172.16.18.70), last user (administrator), and isolation status (Isolate). Below the card are tabs: SUMMARY (highlighted with a red border), EVENTS, STATUS, and POLICIES. The 'SUMMARY' tab displays 'Recent Events' with five entries: 'Update succeeded' (Aug 22, 2022 11:09 AM), 'Controlled application blocked: Microsoft Powershell (System tool)' (Aug 22, 2022 11:07 AM), 'Update succeeded' (Aug 19, 2022 3:40 PM), 'Blocked URL' (Aug 19, 2022 2:51 PM), and another 'Blocked URL' (Aug 19, 2022 2:51 PM). To the right of the events is a 'View More' link. Below the events is an 'Agent Summary' section showing 'Last Activity' (42 minutes ago), 'Last Agent Update' (3 hours ago, Update Successful), and 'Assigned Products' (Core Agent and Sophos Intercept X, both assigned and licensed). A 'More actions' button is located at the bottom of the summary card.

Selecting a device from the list will display the device page. The device page is split into tabs; **SUMMARY, EVENTS, STATUS** and **POLICIES**.

The status of a device is denoted with a green, orange, or red icon. On the **SUMMARY** tab you can easily view the device name, operating system, IP address, and the last user that was logged onto the device.

This page also allows you to perform an update, **Delete** the device from the Sophos Central account, or start a **Live Response** session. Additional actions can be displayed by clicking **More actions**.

More actions include the option to change the device group, start a scan, **reset the health status** of the device. You can also select **Diagnose** to perform troubleshooting steps or **create a forensic snapshot**.

Computer Groups

The screenshot shows the Sophos Endpoint Protection - Computers page. The left sidebar has 'Endpoint Protection' selected under 'ANALYZE'. The main area has 'Computer Groups' selected under 'MANAGE PROTECTION'. The table lists five computers: WinClient5, WinClient1, WinClient3, WinClient2, and WinClient4, all protected by Intercept X Advanced with XDR.

Name	IP	OS	Protection	Encryption
WinClient5	172.16.16.110	Windows 10 Pro	✓ Intercept X Advanced with XDR	+
WinClient1	172.16.16.70	Windows 10 Pro	✓ Intercept X Advanced with XDR	+
WinClient3	172.16.16.90	Windows 10 Pro	✓ Intercept X Advanced with XDR	+
WinClient2	172.16.16.80	Windows 10 Pro	✓ Intercept X Advanced with XDR	+
WinClient4	172.16.16.100	Windows 10 Pro	✓ Intercept X Advanced with XDR	+

To make it easier to manage protected devices, you can create computer groups. With computers grouped, you can assign the same policy to multiple devices at the same time.

Computer groups are created by navigating to **Endpoint Protection > Computers**.

Select **Computer Groups**.

Computer Groups

The screenshot shows the Sophos Central interface for managing computer groups. The left sidebar has a dark theme with white text and icons. Under 'ANALYZE', 'Endpoint Protection' is selected. The main content area is titled 'Endpoint Protection - Computer Groups' and shows a list of computer groups. At the top, there are three tabs: 'Computers', 'Unmanaged computers', and 'Computer Groups', with 'Computer Groups' being the active tab. Below the tabs is a red-bordered button labeled 'Add Computer Group'. A search bar is located at the top right. The main list displays 13 computer groups, each with a checkbox, a name, and a device count. The names include 'Accounts UKI', 'Directors - AU', 'Engineering JPN', 'Human Resources - UKI', 'IT UK Windows 11', and 'Marketing'. The device counts range from 0 to 6. A message at the bottom indicates 13 of 13 top-level groups have been loaded. The top right corner shows the user 'Simon Smith' with a 'Super Admin' role and a timestamp: 'Last updated: Aug 22, 2022, 2:28 PM'.

Computers	Description
0	Accounts UKI
0	Directors - AU
0	Engineering JPN
0	Human Resources - UKI
6	IT UK Windows 11
0	Marketing

If you have synchronised the Sophos Central account with a directory, you may already have computer groups listed here. The number of devices assigned to a group is displayed and you can also search this list by entering the name of the group you are searching for into the search box.

You can manually create a computer group by selecting **Add Computer Group**.

Computer Groups

The screenshot shows the Sophos Central Device Management interface. The left sidebar has a dark theme with categories like Endpoint Protection, ANALYST, MANAGE PROTECTION, COMPUTERS, and HOME/BUSINESS. The 'Computers' section is selected and highlighted in blue. The main area is titled 'Endpoint Protection - Computer Groups'. It shows tabs for 'Computers', 'Unmanaged computers', and 'Computer Groups', with 'Computer Groups' being the active tab. A sub-header says 'Add Computer Group' with buttons for 'Create new top level group' and 'Create a group within an existing group'. The 'Create a group within an existing group' option is selected. Below this, there's a list of existing groups: 'Create new top level group', 'Eng', 'Human Resources - HQ', 'IT UK Windows (1)', and 'Marketing'. A progress bar at the bottom indicates '1/13 of 13 top level groups / 0 selected'. The top right corner shows user information: 'Help', 'Simon Smith', 'Support role', and 'Super Admin'.

You can either create a new top level group, or you can create a group within an existing group.

In this example, we will create a group within an existing group. Select the group you want to create the new group within and click **Next**.

Computer Groups

The screenshot shows the Sophos Central Device Management interface. On the left, there's a sidebar with various navigation options like Endpoint Protection, People, Computers, and Monitoring. The 'Computers' option is selected. The main area is titled 'Endpoint Protection - Computer Groups'. A sub-menu for 'Add Computer Group' is open, showing a form to create a new group named 'Sales Operations AU'. It includes fields for 'Group Name' (set to 'Sales Operations AU'), 'Group Description' (empty), and a note stating 'A computer can only be in one group so if you move it to a new group, it will be removed from its current group'. Below this, there are two lists: 'Available Computers' (containing WinClient5, WinClient6, WinClient7) and 'Assigned Computers' (containing WinClient1, WinClient2). At the bottom, a message says 'Computers can only be assigned to **ONE** computer group'.

Name the group and assign the required computers from the available computers list. This list is filtered to show unassigned computers by default, however, you can change this to show all computers or show computers filtered by operating system.

Computers can only be assigned to **ONE** computer group.

Computer Groups

The screenshot shows the Sophos Endpoint Protection - Computer Groups interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Endpoint Protection', 'ANALYSE', 'MANAGE PROTECTION', 'CONFIGURE', and 'MORE PRODUCTS'. Under 'MANAGE PROTECTION', 'Computers' is selected and highlighted in blue. The main area is titled 'Endpoint Protection - Computer Groups' with tabs for 'Computers', 'Unmanaged computers', and 'Computer Groups'. Below the tabs are buttons for 'Add Computer Group', 'Move' (which is highlighted with a red box), and 'Delete'. A list of computer groups is shown, including 'Marketing', 'Reading Office', 'Sales Engineering - macOS - UKI', 'Sales Operations (5)', and 'Sales Operations AUS' (which is checked). An orange arrow points from the 'Move' button to the 'Move group' dialog on the right. The 'Move group' dialog has a title 'Move group' and a sub-section 'Move Sales Operations AUS group to:'. It shows two radio button options: 'Top level' (unchecked) and 'Sub-group' (checked). Below this is a search bar and a list of 'AVAILABLE GROUPS' with items like 'Human Resources - UKI', 'IT UK Windows (1)', 'Marketing', 'Reading Office', 'Sales Engineering - macOS - UKI', 'Sales Operations (5)', and 'Sales Operations AUS'.

If you have a group that is not in the correct place. For example, a top-level group that should be a sub-level group, you can move the group to the correct place.

Select the group you want to move and then select where you want to move it and click **Save**.

Computer Groups

The screenshot displays the Sophos Central Device Management interface. On the left, a sidebar menu includes options like Endpoint Protection, Devices, Computer Groups (highlighted in blue), Policies, Settings, and Support Tickets. The main content area shows two tabs: 'SUMMARY' and 'POLICIES'. Under 'SUMMARY', there's a 'Computer Groups' section with a 'List' button highlighted by a red box. Below it, a 'Group Details' card shows a green checkmark icon, a group name, assigned IP, and a 'Group Members' section listing 'WinClient' and 'WinClient'. To the right, another 'SUMMARY' tab is open, showing a 'Change Computer Group' dialog. This dialog has fields for 'Computer Name' (set to 'winclient'), 'Assigned Group' (set to 'Sales Operations AUS'), and a 'Available Groups' dropdown containing a list of groups. An orange arrow points from the 'More actions' button in the 'Computer Groups' list to the 'Change group' button in the dialog. A large green callout box on the left says 'Edit group membership via Computers > Computer Groups'. A large green callout box on the right says 'Edit individual device group membership via the Device page'.

SOPHOS

Endpoint Protection - Sales Operations AUS

SUMMARY POLICIES

Group Details

Group Description:

Group Members

GROUP MEMBERS

WinClient WinClient

WinClient

SOPHOS

Endpoint Protection

SUMMARY POLICIES

Computer Name: winclient

Assigned To: Sales Operations AUS

Available Groups:

- IT - Admin
- Security Lab - Admin
- Finance - Admin
- Engineering - Admin
- Human Resources - Admin
- IT - Sales
- Marketing
- Meeting Office

More actions

Change group

Start now

Stop now

Reapply

Create New Group

Change Computer Group

Computer Name: winclient

Assigned Group: Sales Operations AUS

Available Groups:

- IT - Admin
- Security Lab - Admin
- Finance - Admin
- Engineering - Admin
- Human Resources - Admin
- IT - Sales
- Marketing
- Meeting Office

Save

Edit group membership via
Computers > Computer Groups

Edit individual device group membership
via the Device page

SOPHOS

You can edit the devices that belong to each computer group using the **Computers Groups** tab and editing the group membership or for individual devices via the **Device** page.

Simulation: Create Computer Groups

In this simulation you will create two computer groups.



LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/ComputerGroups/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/ComputerGroups/1/start.html>

Server Details

The screenshot shows the Sophos Central interface with the 'Servers' tab selected. The left sidebar has 'Devices' highlighted. The main area displays a table of servers with columns for Name, IP, OS, Protection, Last active, and Group. A red box highlights the 'Servers' tab in the top navigation bar.

Name	IP	OS	Protection	Last active	Group
linuxserver1	172.16.16.130	Ubuntu 20.04.4 LTS	Anti-Virus for Linux	Aug 22, 2022 3:02 PM	
WinServer1	172.16.16.10	Windows Server 2019 Standard	Intercept X Advanced for Server with XDR	Aug 22, 2022 2:45 PM	Member S
DC	192.168.1.94	Windows Server 2022 Standard	Intercept X Advanced for Server with XDR	Aug 22, 2022 2:41 PM	Reading D
SRV3	192.168.1.166	Windows Server 2022 Standard	Intercept X Advanced for Server with XDR	Aug 22, 2022 2:41 PM	
training-linux-srv	192.168.1.231	Ubuntu 20.04.4 LTS	Server Protection	Aug 22, 2022 2:11 PM	Reading D
SRV2	192.168.1.245	Windows Server 2022 Standard	Intercept X Advanced for Server with XDR	Aug 20, 2022 11:51 AM	Reading D

Servers are listed in Sophos Central in **Devices > Servers**.

When you install the Sophos Endpoint Agent, the installer recognizes the operating system and automatically places protected servers in the 'Servers' list.

All protected servers are listed with the name, IP address, operating system, and protection status. The list also displays when the servers were last active, the group they are associated with, and the locked down status of the server.

Server Details

The screenshot shows the Sophos Central interface for a server named 'WinServer1'. The left sidebar has 'Sophos Central' and 'MY PRODUCTS' sections. The main area shows 'WinServer1' with a summary card containing a green checkmark icon, the server name, and a status bar. Below the card are buttons for 'Scan Now', 'Lock Down', 'Diagnose', and 'Reset Health Status'. A 'Live Response' button is also visible. The top right has links for 'Help', 'UK Training', and 'Sophos UK - Super Admin'. The main content area has tabs for 'SUMMARY', 'EVENTS', 'STATUS', 'EXCLUSIONS', 'APPLICATIONS', 'LOCKDOWN EVENTS', and 'POLICIES'. Under 'SUMMARY', there's a 'Recent Events' section with log entries from Dec 2, 2022, to Nov 10, 2022. Below that is an 'Agent Summary' section with details like last activity, last update, assigned products (Core Agent, Sophos Intercept X, Server Protection), and version numbers (2022.7.2.1, 2022.13.3, 10.8.11.4).

Selecting a server from the server list will display the server details. Here you can view the **SUMMARY** of the server.

This includes the most recent events, the last Sophos Central activity, the last agent update, and the assigned products. Below the server icon, you can view the server name and operating system. From here you can select to isolate the server, perform a scan, start server lock down or generate a diagnostic file. You can also reset the server health status or start a **Live Response** session if required.

Server Details

The screenshot shows the Sophos Central interface for a device named 'WinServer1'. The left sidebar has 'Sophos Central' at the top, followed by sections for Threat Analysis Center, Log & Reports, People, Dashboards (which is selected), Global Settings, Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Phish Threat. The main area is titled 'WinServer1' and shows a summary of its status: 'Status: Up', 'Windows Server 2016 Data Drives: 100%'. Below this are buttons for 'Scan Now', 'Lock Down', 'Diagnose', and 'Reset health status'. The 'EVENTS' tab is selected, showing a table of events from September 10, 2022, to December 8, 2022. The table includes columns for SEV, TYPE, DATE, and EVENT. The events listed are all related to updates and reboots, with most being 'Update succeeded' or 'Reboot to complete update; computer stays protected in the meantime'. A total of 35 events are shown.

SEV	TYPE	DATE	EVENT
Info	Reboot	Dec 2, 2022 1:35 PM	Reboot to complete update; computer stays protected in the meantime
Info	Reboot	Dec 1, 2022 1:43 PM	Reboot to complete update; computer stays protected in the meantime
Info	Reboot	Nov 24, 2022 5:13 PM	Reboot to complete update; computer stays protected in the meantime
Info	Update	Nov 14, 2022 11:15 AM	Update succeeded
Info	Update	Nov 10, 2022 11:11 AM	Update succeeded
Info	Update	Nov 7, 2022 10:11 AM	Update succeeded
Info	Update	Nov 4, 2022 5:02 PM	Update succeeded
Info	Update	Nov 3, 2022 5:01 PM	Update succeeded
Info	Update	Nov 2, 2022 5:00 PM	Update succeeded
Info	Update	Nov 1, 2022 4:22 PM	Update succeeded
Info	Update	Oct 13, 2022 9:22 AM	Update succeeded
Info	Update	Oct 11, 2022 10:14 AM	Update succeeded

The **EVENTS** tab displays all events for the server. These events can be filtered.

Server Details

The screenshot shows the Sophos Central interface for a device named 'WinServer1'. The left sidebar has a dark theme with various navigation options like Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices (which is selected), Global Settings, Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Phish Threat. The main content area has a light blue header with tabs: SUMMARY, EVENTS, STATUS (which is selected), EXCLUSIONS, APPLICATIONS, LOCKDOWN EVENTS, and POLICIES. Below the header, there's a 'Security Health' section with a green checkmark icon. It lists several items with green checkmarks: 'No malware or potentially unwanted applications', 'Last Sophos Central Activity - 4 days ago', 'Sophos services running' (with a plus sign), and a detailed list of services: Sophos MCS Agent, Sophos Endpoint Defense Service, Sophos File Scanner Service, Sophos MCS Client, Sophos System Protection Service, Sophos File Scanner, Sophos Endpoint Defense, Sophos Network Threat Protection, HitmanPro Alert service, and Sophos NetFilter. To the right of this list is a 'Create forensic snapshot' button with a gear icon. Below the security health section is an 'Alerts' section with the text 'No Alerts'.

The **STATUS** tab displays the server's health. If a server does have an alert or a warning, it can be acknowledged and resolved.

Server Details

The screenshot shows the Sophos Central interface for managing a device named 'WinServer1'. The left sidebar contains navigation links for 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices' (which is selected), 'Global Settings', 'Protect Devices', and 'Account Health Check'. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Phish Threat. The main content area displays the device status as 'Up-to-date' with a green checkmark icon. It includes sections for 'Scan Now', 'Lock Down', 'Diagnose', and 'Reset health status'. A 'SUMMARY' tab is active, showing a message: 'These files and applications are currently excluded from scanning for threats.' Below this, the 'EXCLUSIONS' tab is selected, showing two entries in a table:

DESCRIPTION	SOURCE
C:\users\administrator\SOPHOS\downloads\lpskill.exe Real-time	Policy
C:\users\administrator\SOPHOS\downloads\lpskill.exe Scheduled	Policy

At the bottom of the exclusions table, there is a link to 'Edit Exclusions'.

The **EXCLUSIONS** tab allows you to review the exclusions applied to the server. You can search and filter all exclusions.

Server Details

The screenshot shows the Sophos Central interface for managing a Windows server. The left sidebar has sections for Sophos Central (Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices, Global Settings, Protect Devices, Account Health Check) and My Products (Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, Phish Threat). The main area is titled 'WinServer1' and shows the 'Devices' tab. At the top right are links for Help, UK Training, and Sophos UK Support. Below the title are tabs for SUMMARY, EVENTS, STATUS, EXCLUSIONS, APPLICATIONS (which is selected), LOCKDOWN EVENTS, and POLICIES. A message says 'These applications are currently installed on this server.' A search bar and a table listing 16 applications with their names and versions. A sidebar on the left of the main content area contains buttons for Update, Scan Now, Lock Down, Diagnose, and Reset health status, with 'Scan Now' being the active button.

NAME	VERSION
Chrome Remote Desktop Host	108.0.5359.10
Dropbox	162.4.5419
Google Chrome	108.0.5359.73
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.24.28127	14.24.28127.4
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.24.28127	14.24.28127.4
Mozilla Firefox (x64 en-GB)	105.0.3
Mozilla Maintenance Service	104.0.1
inflarmowNG	1.26.20.24815
PDQ Deploy	19.3.83.0
PDQ Inventory	19.3.83.0
ShareX	14.1.0
Sophos Central AD Sync Utility	5.0.2.71

The **APPLICATIONS** tab allows you to view a list of applications that are currently installed on the server.

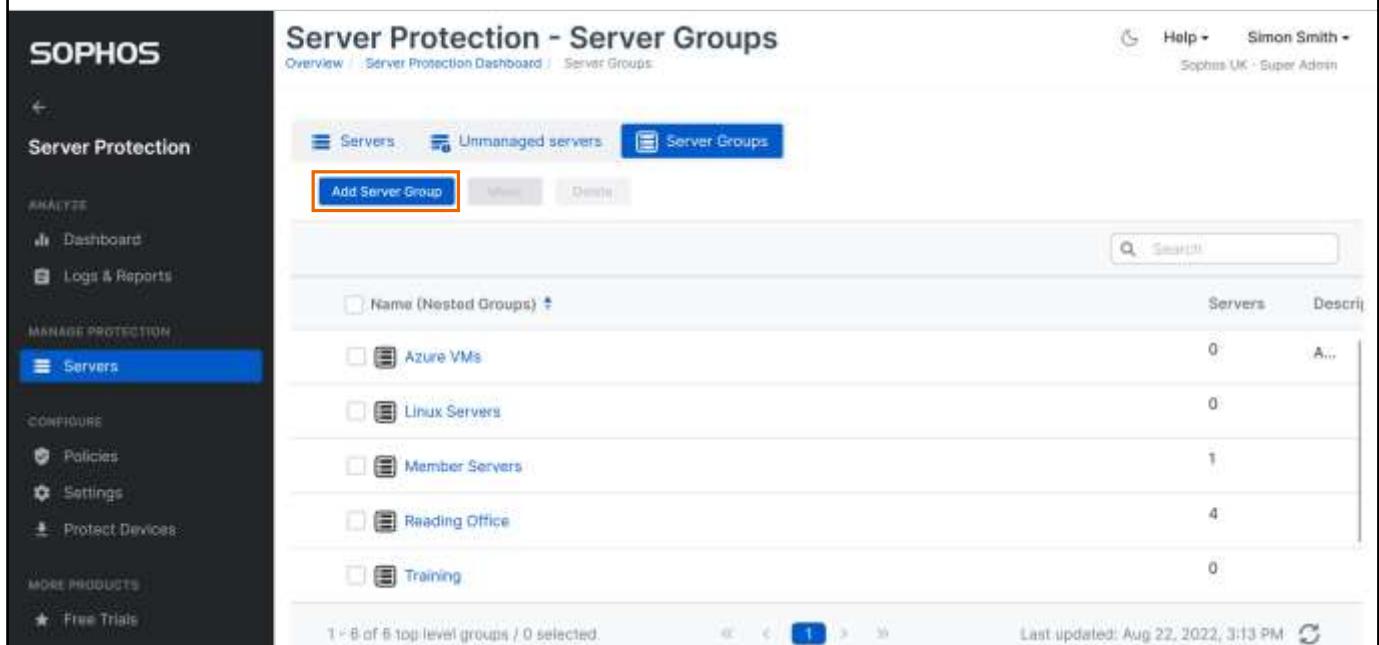
Server Details

The screenshot shows the Sophos Central interface for managing a device named 'WinServer1'. The left sidebar contains navigation links for various protection types: Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Phish Threat. The 'Devices' section is selected. The main panel displays the status of 'WinServer1' (Windows Server 2016 Datacenter) with a green checkmark icon. It includes buttons for 'Scan Now', 'Lock Down', 'Diagnose', and 'Reset health status'. Below this, a 'Policies' tab is selected, showing a list of applied policies:

Type	Name
Server Protection: Threat Protection	Base Policy - Threat Protection
Server Protection: Peripheral Control	Base Policy - Peripheral Control
Server Protection: Application Control	Block Remote control
Server Protection: Web Control	Base Policy - Web Control
Server Protection: Lockdown	Base Policy - Lockdown
Server Protection: Data Loss Prevention	Base Policy - Data Loss Prevention
Server Protection: Update Management	Base Policy - Update Management
Server Protection: Windows Firewall	Base Policy - Windows Firewall
Server Protection: File Integrity Monitoring	Base Policy - File Integrity Monitoring

The **POLICIES** tab displays the policies that are applied to the server.

Server Groups



The screenshot shows the Sophos Central Device Management interface. The left sidebar has a dark theme with the following navigation items:

- SOPHOS
- ←
- Server Protection
- ANALYSE
- Dashboard
- Logs & Reports
- MANAGE PROTECTION
- Servers** (highlighted in blue)
- CONFIGURE
- Policies
- Settings
- Protect Devices
- MORE PRODUCTS
- Free Trials

The main content area is titled "Server Protection - Server Groups". It shows a list of server groups with columns for Name, Servers, and Description. A search bar is at the top right. The "Add Server Group" button is highlighted with a red box.

Name (Nested Groups)	Servers	Description
Azure VMs	0	A...
Linux Servers	0	
Member Servers	1	
Reading Office	4	
Training	0	

At the bottom, it says "1 - 8 of 8 top level groups / 0 selected." and "Last updated: Aug 22, 2022, 3:13 PM".

To make the management of protected servers easier by assigning policies to multiple servers at the same time, you can create server groups.

Server groups are created by navigating to **Server Protection > Servers > Server Groups > Add Server Group**.

Server Groups

The screenshot shows the Sophos Central Device Management interface. The left sidebar has a dark theme with sections like 'ANALYZE', 'MANAGE PROTECTION', and 'SERVICES'. The 'Servers' section is selected. The main area is titled 'Server Protection - Server Groups' and shows a list of server groups: 'Members', 'Reading Office', and 'Training'. A modal window titled 'Add Server Group' is open, containing two radio button options: 'Create new top level group' (selected) and 'Create a group within an existing group.'. Below the options are 'Cancel' and 'Next' buttons, with 'Next' being highlighted with a red box. The status bar at the bottom indicates '1 of 6 top level groups / 0 selected'.

Select whether you want to create a new top level group or to create a group within an existing group. In this example, we will create a new top level group.

Server Groups

The screenshot shows the Sophos Central Device Management interface. On the left, there's a sidebar with various navigation options like 'Dashboard', 'Logs & Reports', 'Servers', 'Policies', 'Settings', 'Protected Devices', 'Trial Products', and 'Free Trials'. The 'Servers' option is currently selected. The main area is titled 'Server Protection - Server Groups' and contains a sub-titled 'Add Server Group'. It has fields for 'Group Name *' (set to 'New York Office') and 'Group Description'. Below these is a note: 'A server can only be in one group so if you move it to a new group, it will be removed from its current group.' There are two sections: 'Available Servers' (containing 'SRV' and 'SRV3') and 'Assigned Servers' (containing 'linuxserver1'). A search bar is also present. At the bottom right, it says 'Last updated: 10/10/2023, 3:13 PM'.

Give the server group a name and assign the servers that will be included in the group.

Server Groups

The screenshot shows the Sophos Central Device Management interface. The left sidebar has sections for ANALYZE (Dashboard, Log & Reports), MANAGE PROTECTION (Servers, selected), and CONFIGURE (Policies, Settings, Protect Devices). The main content area is titled "Server Protection - Server Groups". It shows a list of server groups: "Name (Nested Groups)" (0 servers), "Azure VMs" (0 servers), "Linux Servers" (0 servers), "Member Servers" (1 server), and "New York Office" (1 server). The "New York Office" item is highlighted with a red box. A message at the bottom states: "Servers can only be assigned to **ONE** server group". The top right shows "Help", "Simon Smith", and "Sophos UK - Super Admin". The bottom navigation bar includes "Last updated: Aug 22, 2022, 3:18 PM" and a refresh icon.

Once the server group has been saved, it will be listed in the server groups list.

Remember, a server can only be a member of **ONE** group.

Simulation: Create a Server Group



In this simulation you will create a new server group and assign a server to it.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/ServerGroups/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/ServerGroups/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 1

True or False: A computer can be a member of multiple computer groups.

True

False

SOPHOS

Chapter Review

Create computer and server groups to easily manage protected devices.

Use groups to assign policies to multiple computers and servers at once.

Computers and servers can only be assigned to ONE group.

SOPHOS

Here are the three main things you learned in this chapter.

Create computer and server groups to easily manage protected devices.

Use groups to assign policies to multiple computers and servers at once.

Computers and servers can only be assigned to ONE group.



Getting Started with Sophos Central Device Communication

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3010: Getting Started with Sophos Central Device Communication

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Device Communication

In this chapter you will learn how protected devices communicate management traffic to Sophos Central and how to check the last communication time and date.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

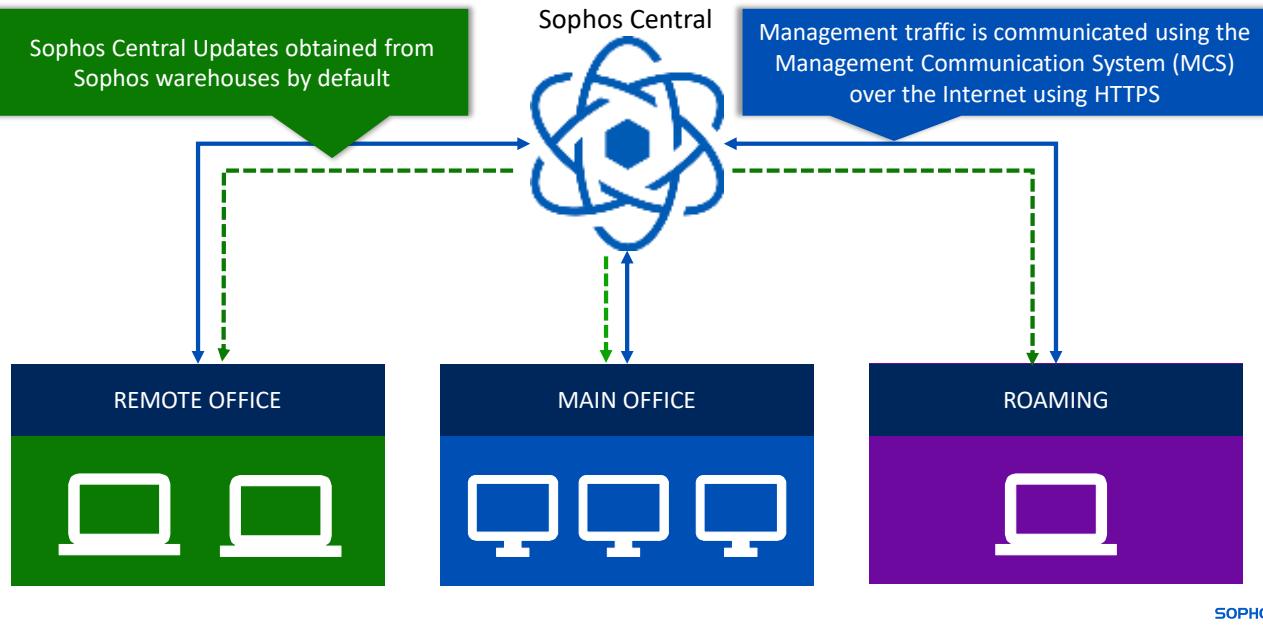
- ✓ How to protect a device from Sophos Central
- ✓ How to manage devices in Sophos Central

DURATION **5 minutes**

SOPHOS

In this chapter you will learn how protected devices communicate management traffic to Sophos Central, and how to check the last communication time and date.

Device Communication

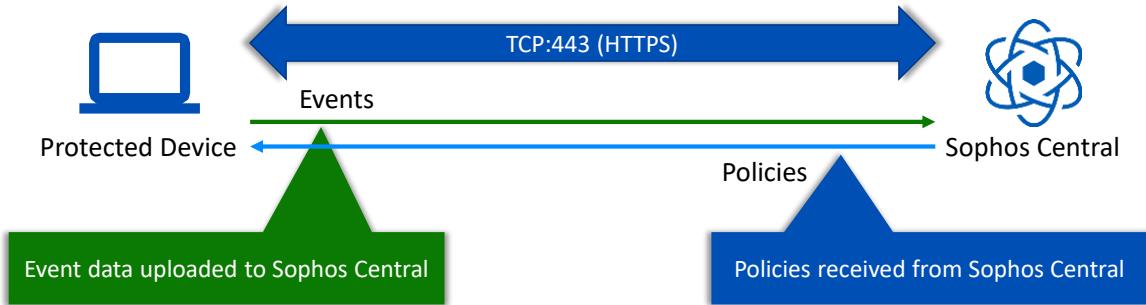


A key benefit of Sophos Central is that it does not matter where protected devices are located. No hardware is required to manage devices. All device management takes place in the cloud-based management system.

Management traffic is communicated between devices and Sophos Central using the Management Communication System (MCS) over the Internet using HTTPS.

By default, all devices obtain the latest threat updates from online Sophos warehouses, however, you can configure a server Update Cache if required.

Management Communication System (MCS)



SOPHOS

We define management traffic as all data sent and received by MCS on a device. Devices use MCS to download new policies from Sophos Central and to upload event and detection data to Sophos Central.

MCS has an adaptor installed for each component of the Sophos Endpoint Agent that allows it to exchange messages, receive policies, and provide events.

Sophos Endpoint Agent Summary

The screenshot shows the Sophos Central Device page for a Windows client named 'WinClient3'. The 'Agent Summary' section displays the last activity (44 minutes ago) and last agent update (10 hours ago, successful). It lists assigned products: Event System (version 2.30.11), System Inventory (version 2.0.25), Endpoint Protection (version 10.8.33.4), and Device Encryption (version 2.30.11). The 'Assigned' column shows checkmarks for Event System, System Inventory, and Endpoint Protection, while Device Encryption has a red 'X' and a 'Assign' button. Below this, the 'Installed component versions' section shows 'No groups' and 'Windows 10 Pro' as the operating system. On the left, there's a sidebar with 'Update now' buttons for Device and Last Response, and a 'More options' menu. A green callout box points to the 'Agent Summary' section with the text: 'View the agent summary details on the device page'. Another green callout box points to the device status icons with the text: 'Device status icons indicate the health status'. To the right, a table maps icons to alert levels: a green checkmark for low-priority alerts, an orange warning sign for medium-priority alerts, and a red warning sign for high-priority alerts.

Icon	Description
	Green checkmark 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.

SOPHOS

Devices communicate their health status back to Sophos Central as well as event, detection, and additional feature data such as web and application control data.

The 'Agent Summary' section on the device page lists the last activity time of the device along with the last time the agent was updated.

You can see which licensed products have been assigned to the device and the version installed.

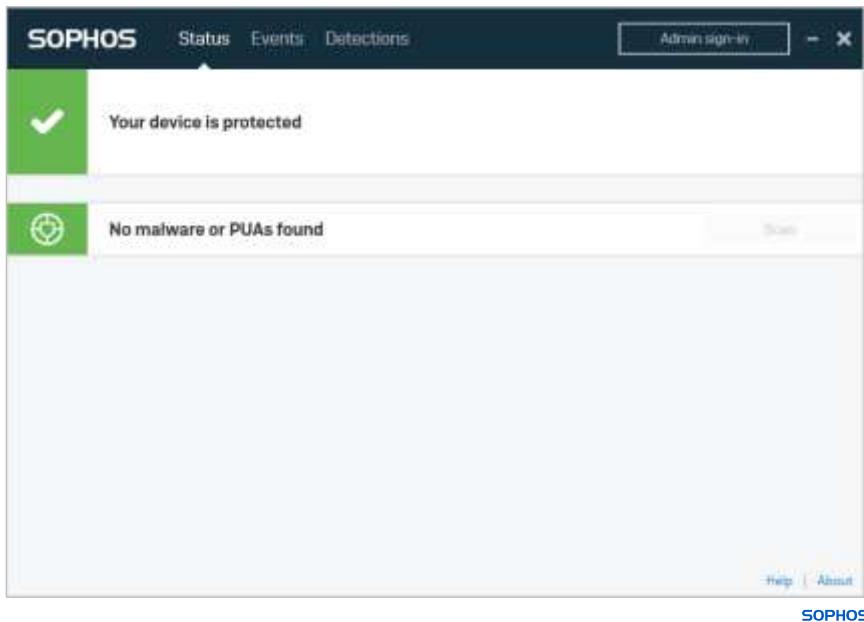
Expanding the 'Installed component versions' displays a full list of all of the components installed. Please note that this is only displayed for Windows devices.

Sophos Endpoint Agent

Status displays the current status of the endpoint agent

Events displays all events that have happened on the device

Detections displays detection history split into categories



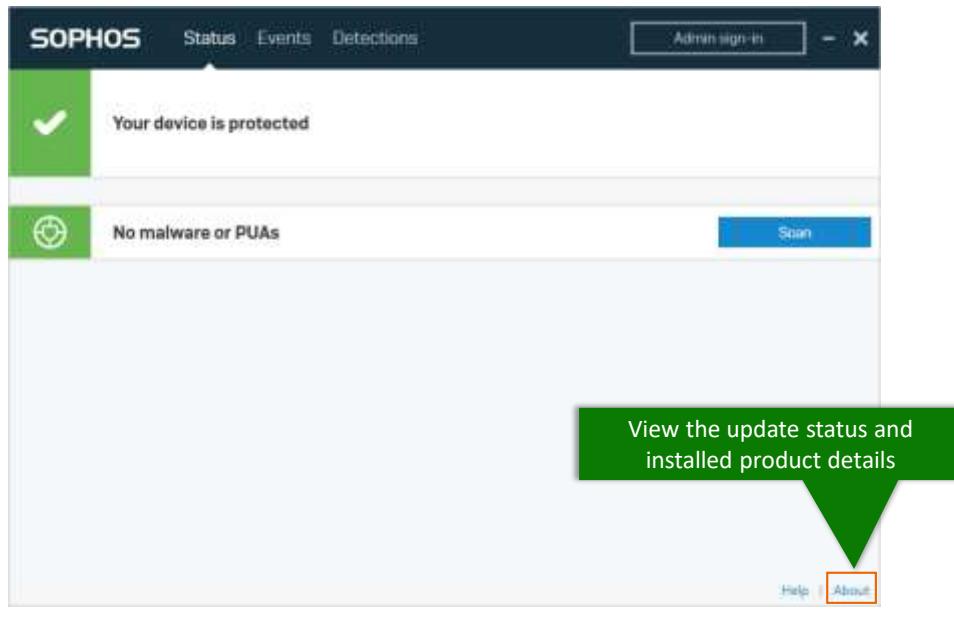
The Sophos Endpoint Agent displays the health status, event and detection information which is communicated back to Sophos Central using MCS.

The agent is accessed from the system tray on a Windows device. Opening the agent displays the **Status** of the device. If there has been a detection that has not been automatically cleaned up, the details of the detection will be displayed.

To view all events that have happened on the device, select the **Events** tab.

The **Detections** tab displays malware and PUA history along with the detection history of the device split in threat categories.

Sophos Endpoint Agent



Clicking **About** displays the 'Update Status' of the device along with the products installed.

Devices receive updates from Sophos Central warehouses by default. Here you can see the date and time of the last update received by the device and whether it was successful.

Update Communication

The screenshot shows the Sophos Central Device Communication interface. At the top, there's a navigation bar with 'SOPHOS' and links for 'Status', 'Events', and 'Detections'. On the right of the nav bar are 'Admin sign-in', a minimize button, and a close button. Below the nav bar is a section titled 'Update Status' with a green checkmark icon and the text 'Last update: 24 June 2022 15:11'. A blue button labeled 'Update Now' is highlighted with a red box and a callout bubble pointing to it, which contains the text 'Force an update to download any software updates'. Below this are sections for 'Products' (listing Core Agent 2.20.11, Endpoint Advanced 10.8.11.4, and Sophos Intercept X 2.0.25) and 'Troubleshooting' (with a link to 'Open Endpoint Self Help Tool'). There's also a 'Community forum' link and a 'Legal Information' section with copyright notice. At the bottom right are 'Help' and 'About' links, and the 'SOPHOS' logo.

An update can be forced locally on a device by clicking **Update Now**. This will force the device to communicate with the update server and download any software updates required.

Management Communication

The screenshot shows the Sophos Central Management Console interface. At the top, there's a dark header bar with the Sophos logo, navigation links for Status, Events, and Detections, and a sign-in button for Admin sign-in. Below the header, the main content area has a light gray background.

Update Status: A green checkmark icon indicates "Last update: 24 June 2022 15:11". A blue "Update Now" button is present.

Products: A table showing software versions: Core Agent 2.20.11, Endpoint Advanced 10.8.11.4, and Sophos Intercept X 2.0.25.

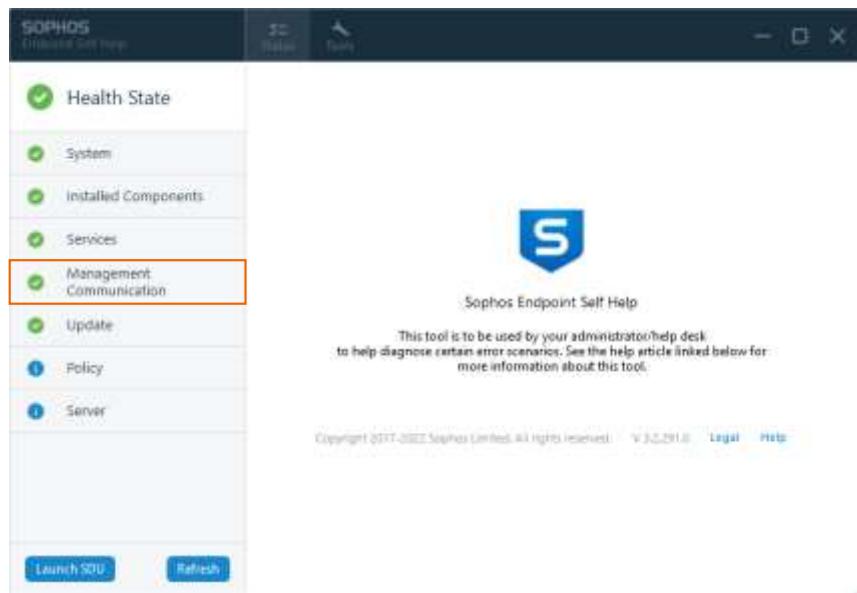
Troubleshooting: A blue "Open Endpoint Self Help Tool" button is highlighted with an orange border. Other options include "Community forum" and "Legal Information".

Footer: Copyright notice: "Copyright 2014-2021 Sophos Limited. All rights reserved." Navigation links for "Help" and "About" are at the bottom right, along with the Sophos logo.

It is important to understand that forcing an update is not the same as the device communicating management traffic.

The Endpoint Self Help Tool can be used to view the last communication time between a device and Sophos Central.

Management Communication



SOPHOS

The Endpoint Self Help Tool is split into categories.

To view the last management communication between a device and Sophos Central select **Management Communication**.

Management Communication

The screenshot shows the Sophos Endpoint Self Help interface. On the left, a sidebar lists various status categories: Health State, System, Installed Components, Services, Management Communication (which is selected and highlighted in light blue), Update, Policy, and Server. Below the sidebar are two buttons: 'Launch SDD' and 'Refresh'. The main content area is titled 'Management Communication'. It displays a green circular icon with a checkmark and the text 'Last Communication' followed by 'Succeeded at 16:01:27 Jun 24, 2022 (UTC+01:00)'. Under 'Connection Details', there are three items: 'Server' (https://mc2-cloudstation-eu-west-1-prm.hydra.sophos.com/sophos/management/ep), 'Server Address' (34.252.218.22), and 'Proxy' (No proxy used). At the bottom, a 'Remediation' section includes a link to a Knowledge Base Article (KB-000036450) and a 'Did this help you?' button with a 'Yes' link.

View the last communication date along with the connection details for management communication

This tab displays the status of the management traffic communication. In this example the communication succeeded.

The connection details provide the name of the Sophos server, the IP address and the proxy address if used. If you have also made use of a Message Relay, the Message Relay DNS will be displayed here.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

What is the system used by devices to communicate management traffic with Sophos Central?

SOPHOS



Question 2 of 3

Which tab in the Endpoint Self Help Tool displays the last communication date and time for management traffic?

Update

Services

Management
Communication

System

SOPHOS



Question 3 of 3

True or False: Clicking Update Now in the Sophos Endpoint Agent forces the device to communicate with the update server and downloads any software updates required.

True

False

SOPHOS

Chapter Review

Management traffic is communicated between devices and Sophos Central using the Management Communication System (MCS) over the Internet using HTTPS.

Devices use MCS to download new policies from Sophos Central and to upload event and detection data to Sophos Central.

To view the last management communication time and date select the Management Communication tab in the Endpoint Self Help Tool.

SOPHOS

Here are the three main things you learned in this chapter.

Management traffic is communicated between devices and Sophos Central using the Management Communication System (MCS) over the Internet using HTTPS.

Devices use MCS to download new policies from Sophos Central and to upload event and detection data to Sophos Central.

To view the last management communication time and date select the Management Communication tab in the Endpoint Self Help Tool.



Sophos Central Tamper Protection

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3015: Sophos Central Tamper Protection

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central Tamper Protection

In this chapter you will learn what Tamper Protection is, what it does and how to recover Tamper Protection passwords.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How devices communicate with Sophos Central
- ✓ How to protect a device with Sophos Central

DURATION 4 minutes

SOPHOS

In this chapter you will learn what Tamper Protection is, what it does, and how to recover Tamper Protection passwords.

What is Tamper Protection?

Prevents the
uninstallation of
the Sophos
Endpoint Agent

Prevents the
modification of
protection settings

Enabled by default

The screenshot shows two views of Sophos Central. The top view is the 'Global Settings' section for 'Tamper Protection'. It includes a note about requiring admin or password access to change settings, a toggle switch for 'Tamper Protection' which is turned on, and a note that you can turn Tamper protection on or off for a specific device from its details page. The bottom view is a 'Devices' list for 'WinClient1', showing basic device information like Group, Operating System, and Processor. A callout box highlights the 'Tamper Protection' status for this device, which is set to 'On - Full Off Tamper Protection'. The status is described as 'This protection is disabled'.

Tamper Protection is primarily used to prevent the modification of protection settings and the uninstallation of the Sophos Endpoint Agent.

Tamper Protection is enabled by default as a global setting. Any attempt to disable Tamper Protection, either by an unauthorized user or by malware triggers an alert in Sophos Central.

Tamper Protection can be disabled for all protected devices, however, this is not recommended. It can be disabled for individual devices which allows you to troubleshoot issues, re-install the agent, or remove the agent if required.

What Does Tamper Protection Prevent?

-  Stopping services from the services UI
-  Killing services and process from the task manager UI
-  Changing service configuration from the services UI
-  Stopping or editing service configuration from the command line
-  Uninstalling and reinstalling the Sophos Endpoint Agent
-  Deleting or modifying Sophos Endpoint Agent files, folders and registry keys

SOPHOS

Tamper Protection's primary function is to prevent the modification of protection settings and the uninstallation of the Sophos Endpoint Agent.

Additionally, it also prevents users from stopping services and processes, changing service configurations and stopping or editing service configuration from a command line. It also prevents the removal or modification of files, folders, and registry keys related to the Sophos Endpoint Agent.

Tamper Protection

WinClient5
Devices : WinClient5

Device Encryption
You haven't assigned Device Encryption to this computer.

Tamper Protection
Tamper Protection : On [Turn off tamper protection](#)
[View password details](#)

Update Cache and Message Relay
Product Update Source : WinServer1
Sophos Central Messaging : WinServer1

Windows Firewall
Windows Firewall : Active(Domain, Private, Public)
Managed by Windows Group Policy : No
Last Active Profile : Domain

Other Registered Firewalls
Sophos Intercept X : Active

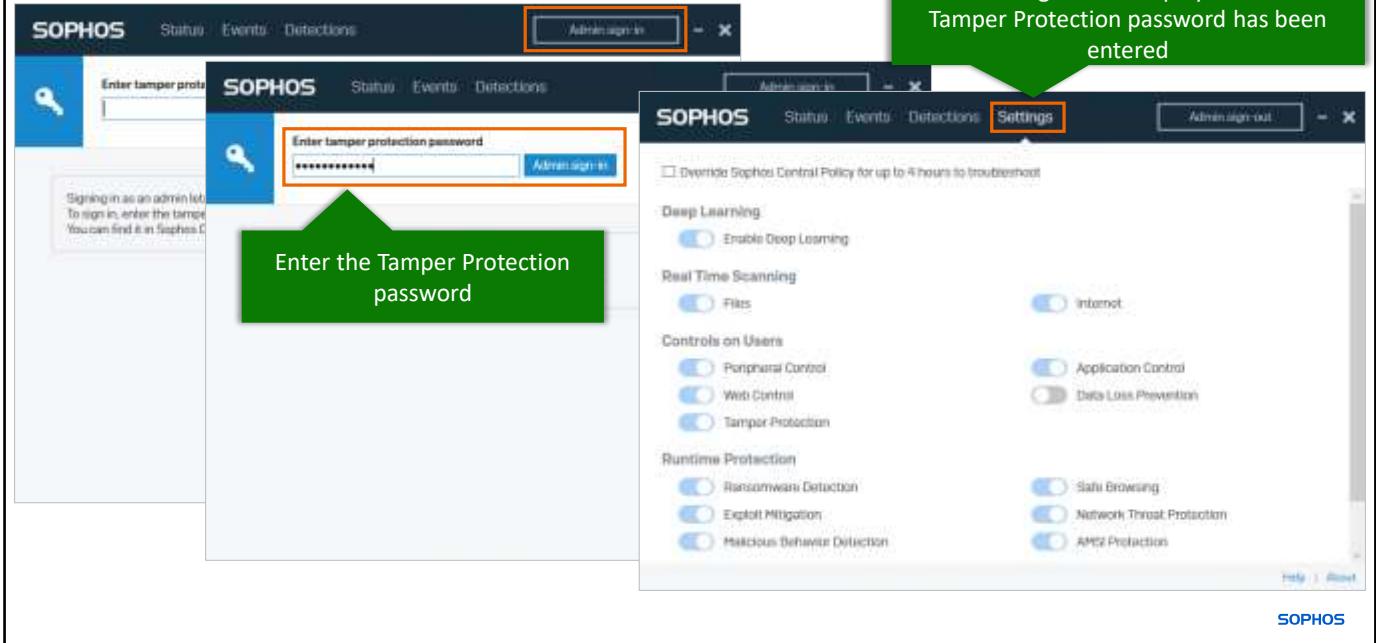
SOPHOS

Each endpoint has a unique Tamper Protection password that can be viewed in Sophos Central on the **Device > SUMMARY** tab.

In the ‘Tamper Protection’ section, click **View password details** to view the Tamper Protection password for the device.

You can generate a new password should this be required.

Tamper Protection



The Tamper Protection password for a device is used to access the settings of the Sophos Endpoint Agent.

This may be required if protection settings need to be modified, or if you need to troubleshoot an issue.

Notice that once the sign-in has been completed, the 'Settings' tab is displayed.

When to Disable Tamper Protection

Recommended scenarios for disabling Tamper Protection

- Performing an upgrade to the operating system of a device
- When re-protecting a device
- When restoring a Windows device to a restore point
- To remove the Sophos Endpoint Agent from a device

SOPHOS

We do not advise turning Tamper Protection off for any devices as this can reduce your protection.

However, there are some scenarios where disabling Tamper Protection may be required. These are:

- If you plan to perform an upgrade to the operating system of a device
- To re-protect a device
- When restoring a Windows device to a restore point
- To remove the Sophos Endpoint Agent from a device

Recover Tamper Protection Passwords

The screenshot shows the Sophos Central interface with the 'Logs & Reports' section selected in the sidebar. A red box highlights the 'Recover Tamper Protection passwords' link under the 'Unified Endpoint Management & Sophos Intercept X for Mobile' heading.

Blocked Applications Shows the blocked applications and the servers/users that tried to access them.	Shows a summary of all emails.
Allowed Applications Shows the applications in your controlled list that were accessed most often and the servers/users that access them.	Malicious Threat Summary Shows a summary of inbound messages that were analyzed for threats using static and dynamic analyses.
Application Control Policy Violators Shows the servers/users that tried to access blocked applications most often and the application they tried to access.	Time of Click Summary Shows a summary of time of click activity.
Data Loss Prevention Policy Violators Shows all activity triggered by data loss prevention rules.	At-risk users Identifies your most at-risk employees.
Windows Firewall Shows the status of firewalls installed on Windows computers and servers.	Data loss prevention policy violations Shows a report of all messages flagged by data loss prevention policies.
Windows Firewall Program Violators Shows programs blocked by an explicit firewall.	Post-delivery summary Shows a summary of all messages removed post-delivery.
Recover Tamper Protection passwords Shows the recently deleted devices, to enable the recovery of Tamper Protection passwords.	Licence usage summary Shows a summary of licence usage.
Unified Endpoint Management & Sophos Intercept X for Mobile	
Unified Endpoint Management Shows how many traditional and mobile devices are managed or unmanaged, as well as details of those devices.	
Sophos Intercept X for Mobile Shows how many mobile devices need attention, have security warnings or are unprotected, as well as details of those devices.	

SOPHOS

Tamper Protection passwords can be recovered if the device has been deleted from Sophos Central.

To recover a Tamper Protection password, navigate to **Logs & Reports > Recover Tamper Protection passwords**.

Recover Tamper Protection Passwords

The screenshot shows the Sophos Central interface with the 'Logs & Reports' section selected. A green callout box points to the 'View password details' link for a device named 'SRV'.

Name (ID)	Deleted At	TAMPER PROTECTION	PASSWORD(S)
SRV Windows Server 2016 Standard	9 days ago	On	View password details
Client1 Windows 10	8 days ago	On	View password details

Displaying 2 of 2 devices.

Passwords are available for devices that have been deleted in the last 90 days. This may be necessary to uninstall the Sophos Endpoint Agent if the device was deleted in Sophos Central, before the agent was uninstalled.

To view the password, select the **View password details** link.

The report option allows you to save it as a custom report and to export it. This is especially useful for providing a recovery plan for accidentally deleted devices. If you regularly save the report, you can recover deleted devices further back than the reports 90 day limit.

Simulation: Test Tamper Protection

In this simulation you will test Tamper Protection.



LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/TamperProtection/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/TamperProtection/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which 2 of the following would allow a single user authorized access to change the Sophos Endpoint Agent settings?

Disabling Tamper Protection for that device only

Rebooting the device in safe mode

Providing administrator rights on the device

Providing the Tamper Protection password for the device

SOPHOS



Question 2 of 3

True or False: All devices have a unique Tamper Protection password.

True

False

SOPHOS

Question 3 of 3



In which scenario would you disable Tamper Protection?

When a new user logs onto a protected device

To remotely update the Sophos Endpoint Agent

To remove the Sophos Endpoint Agent

To remotely access a device

SOPHOS

Chapter Review

Tamper Protection is primarily used to **prevent the modification of protection settings** and the **uninstallation of the Sophos Endpoint Agent**.

Tamper Protection is **enabled globally by default**.

Tamper Protection **passwords can be recovered** for deleted devices.

SOPHOS

Here are the three main things you learned in this chapter.

Tamper Protection is primarily used to prevent the modification of protection settings, and the uninstallation of the Sophos Endpoint Agent.

Tamper Protection is enabled globally by default.

Tamper Protection passwords can be recovered for deleted devices.



Deleting Devices from Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection
CE3020: Deleting Devices from Sophos Central

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Deleting Devices from Sophos Central

In this chapter you will learn how to correctly remove the Sophos Endpoint Agent from protected devices and how to remove devices from Sophos Central.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Removal of apps and features on Windows OS
- ✓ Removal of apps on MacOS
- ✓ How to access Sophos Central
- ✓ How to manage devices in Sophos Central

DURATION **4 minutes**

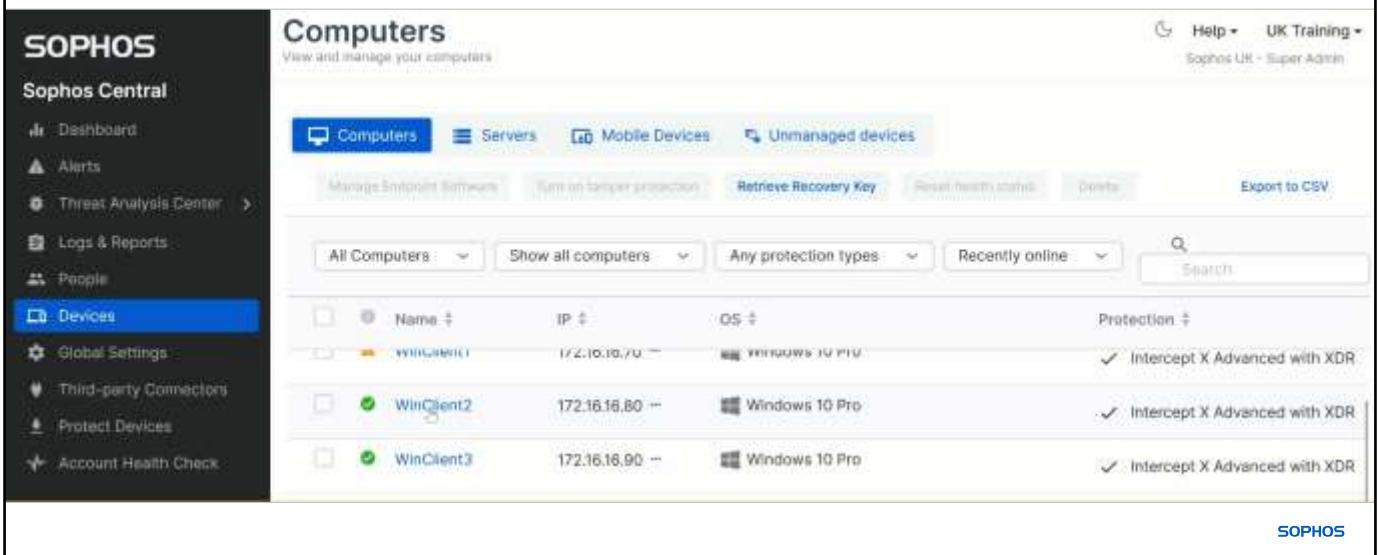
SOPHOS

In this chapter you will learn how to correctly remove the Sophos Endpoint Agent from protected devices, and how to remove devices from Sophos Central.

Deleting Devices

Step 1

Disable Tamper protection for the device in Sophos Central



The screenshot shows the Sophos Central interface with the 'Computers' tab selected. The left sidebar has a 'Devices' section highlighted. The main area displays a list of three devices: 'WinClient1', 'WinClient2', and 'WinClient3'. Each device entry includes its name, IP address, operating system, and protection status. A 'Turn on tamper protection' button is visible above the device list.

Name	IP	OS	Protection
WinClient1	172.16.16.70	Windows 10 Pro	✓ Intercept X Advanced with XDR
WinClient2	172.16.16.80	Windows 10 Pro	✓ Intercept X Advanced with XDR
WinClient3	172.16.16.90	Windows 10 Pro	✓ Intercept X Advanced with XDR

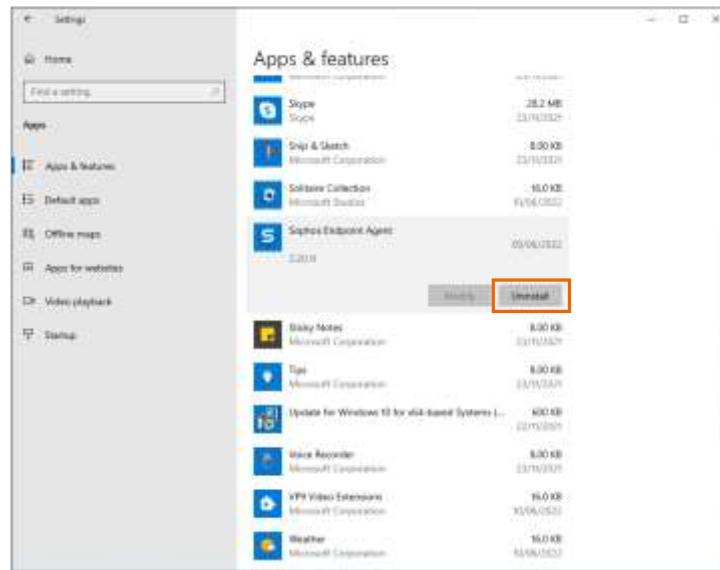
When you need to remove a device from Sophos Central, you first need to uninstall the Sophos Endpoint Agent from the device.

To do this, you must disable Tamper Protection for that device.

Uninstall Sophos Endpoint Agent - Windows

Step 2

Locate the Sophos Endpoint Agent on the device and select to **Uninstall**



SOPHOS

On a Windows device, navigate to the 'Apps & features' menu. Locate the Sophos Endpoint Agent and select **Uninstall**.

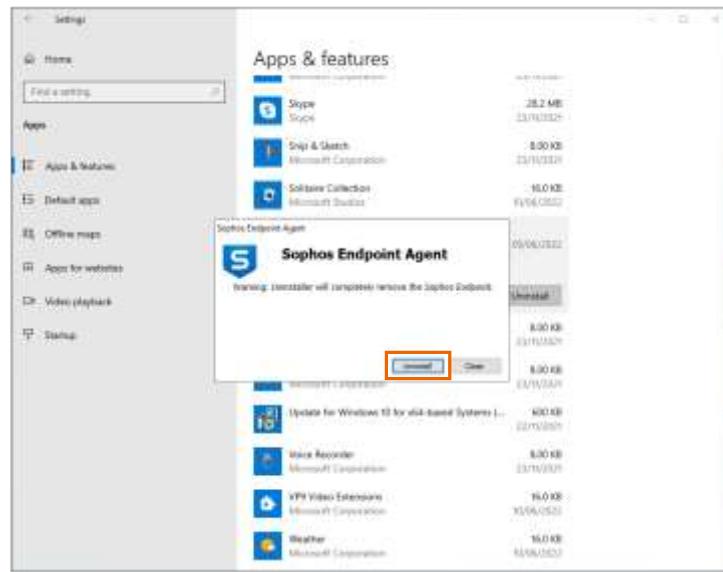
As part of the uninstall process, the Sophos AutoUpdate service is stopped. This cannot be stopped if an update is in progress and therefore the uninstall will fail.

You must ensure that the device is not updating when you uninstall the Sophos Endpoint Agent.

Uninstall Sophos Endpoint Agent - Windows

Step 2

Locate the Sophos Endpoint Agent on the device and select to **Uninstall**



SOPHOS

A confirmation message will be displayed for removal confirmation.

Click **Uninstall**.

Uninstall Sophos Endpoint Agent - Windows

Step 3

Confirmation that the Sophos Endpoint Agent has been removed



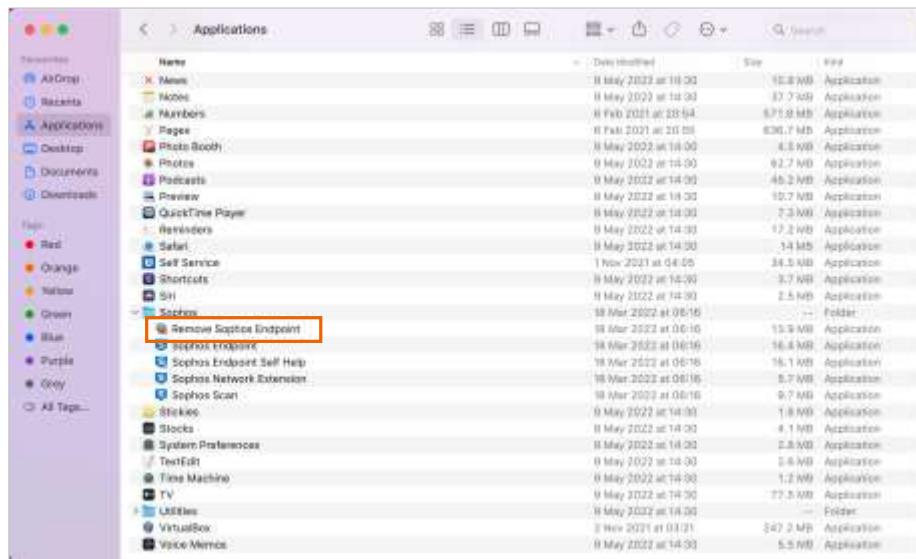
SOPHOS

Once the Sophos Endpoint Agent has been removed successfully, a confirmation message will be displayed on the device.

Uninstall Sophos Endpoint Agent - MacOS

Step 2

Locate the Remove Sophos Endpoint application in Finder



SOPHOS

When the Sophos Endpoint Agent is installed on a macOS device, a **Remove Sophos Endpoint** program is also installed.

To remove the Sophos Endpoint Agent, run **Remove Sophos Endpoint**.

Uninstall Sophos Endpoint Agent - MacOS

Step 2

Click **Continue** to start the removal process



SOPHOS

The removal tool will be opened. Click **Continue**.

Uninstall Sophos Endpoint Agent - MacOS

Step 2

Enter the Tamper Protection password if it has not been disabled in Sophos Central



SOPHOS

If you have not disabled Tamper Protection from Sophos Central for the device, you will need to enter the Tamper Protection password to continue with the removal of the Sophos Endpoint Agent.

Uninstall Sophos Endpoint Agent - MacOS

Step 2

Enter the password for the Device to install the helper



SOPHOS

A prompt to use the 'Install Helper' will be displayed. Enter the device password to start the removal.

Uninstall Sophos Endpoint Agent - MacOS

Step 3

Confirmation that the Sophos Endpoint Agent has been removed

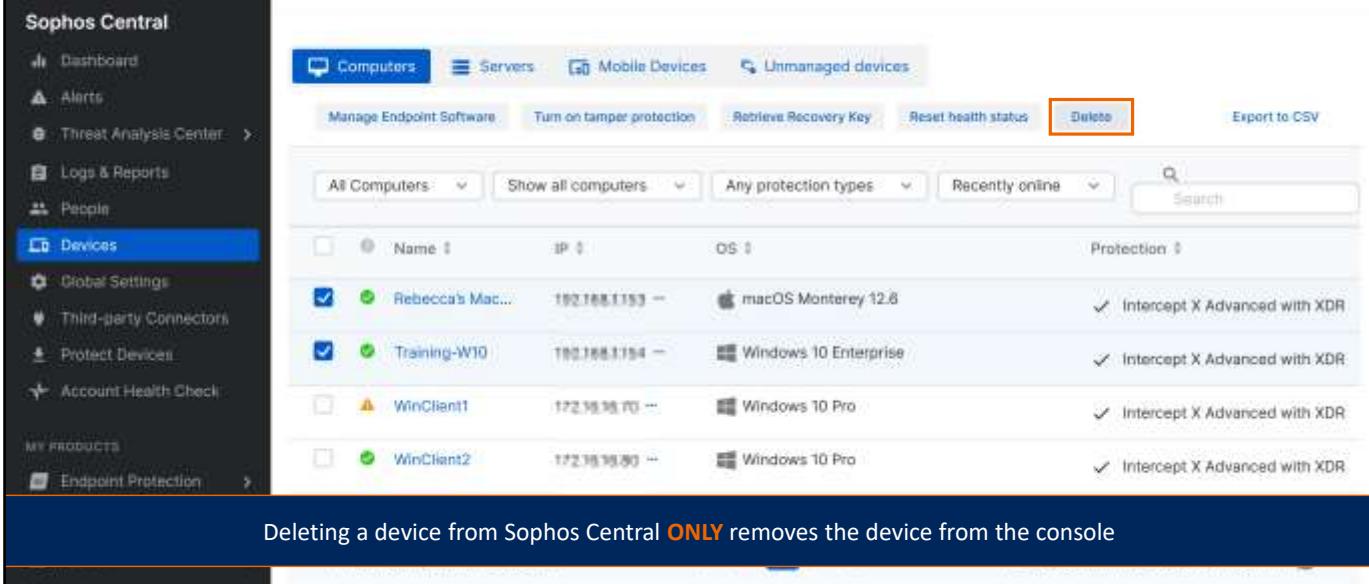


Once the Sophos Endpoint Agent has been removed successfully, a confirmation message will be displayed on the device.

Deleting Devices

Step 4

Delete the device from Sophos Central



The screenshot shows the Sophos Central interface under the 'Devices' section. At the top, there are tabs for Computers, Servers, Mobile Devices, and Unmanaged devices. Below the tabs are several filter and search options: 'Manage Endpoint Software', 'Turn on tamper protection', 'Retrieve Recovery Key', 'Reset health status', and a prominent 'Delete' button which is highlighted with a red box. A 'Search' bar is also present. The main area displays a list of devices with columns for Name, IP, OS, and Protection. Four devices are listed: 'Rebecca's Mac...' (macOS Monterey 12.6), 'Training-W10' (Windows 10 Enterprise), 'WinClient1' (Windows 10 Pro), and 'WinClient2' (Windows 10 Pro). Each device entry includes a checkbox and a small icon indicating its status.

Deleting a device from Sophos Central **ONLY** removes the device from the console

Now that the Sophos Endpoint Agent has been uninstalled from the device, the device can be deleted in Sophos Central.

Navigate to **Devices** from the Sophos Central Dashboard and select the device you want to delete and then click **Delete**. You will see a confirmation message.

Please note that deleting a device from Sophos Central **ONLY** removes the device from appearing in the Sophos Central console. It will not uninstall the Sophos Endpoint Agent from the device itself.



Additional information in
the notes

Supported Uninstall Methods



- Uninstall manually: [KB-000033317](#)
- Uninstall using command line or a batch file: [KB-000035419](#)



- Uninstall manually: [KB-000035097](#)
- Uninstall using removal tool: [KB-000035182](#)
- Uninstall via Terminal: [KB-000033340](#)



- Uninstall manually: [KB-000038632](#)



- Uninstall different Sophos products: [KB-000034722](#)
- How to escalate, upgrade, and uninstall: [KB-000034599](#)

SOPHOS

Sophos have published several supported methods to carry out the uninstallation of the Sophos Endpoint Agent on various platforms.

Ensure that you always follow the supported methods of uninstallation. If you encounter an issue with uninstallation, please seek technical support from Sophos.

[Additional Information]

Windows:

How to uninstall on Windows: <https://support.sophos.com/support/s/article/KB-000033317>

How to uninstall Sophos using the command line or a batch file:

<https://support.sophos.com/support/s/article/KB-000035419>

MacOS:

How to uninstall: <https://support.sophos.com/support/s/article/KB-000035097>

Removal tool: <https://support.sophos.com/support/s/article/KB-000035182>

How to install or uninstall using the terminal: <https://support.sophos.com/support/s/article/KB-000033340>

Linux:

How to perform a manual uninstall: <https://support.sophos.com/support/s/article/KB-000038632>

General Uninstall:

How to uninstall different Sophos products: <https://support.sophos.com/support/s/article/KB-000034722>

How to escalate upgrade and uninstall issues: <https://support.sophos.com/support/s/article/KB-000034599>

000034599

Devices or Users:

How to recover a deleted device or user:

<https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/Devices/RecoverDeletedDevices/index.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

True or False: Tamper Protection must be disabled to remove the Sophos Endpoint Agent.

True

False

SOPHOS



Question 2 of 3

Which Sophos service cannot be running when attempting to remove the Sophos Endpoint Agent?

Sophos MCS Agent

Sophos AutoUpdate

Sophos Health Service

Sophos Live Query

SOPHOS



Question 3 of 3

True or False: Deleting a device from Sophos Central only removes the device, it does not uninstall the Sophos Endpoint Agent.

True

False

SOPHOS

Chapter Review

To **successfully delete** a device from Sophos Central you must **uninstall the Sophos Endpoint Agent** and then **delete the device** from the Console.

Deleting a device from Sophos Central only removes the device, it does not uninstall the Sophos Endpoint Agent.

Only **supported uninstall methods** should be used to remove the Sophos Endpoint Agent.

SOPHOS

Here are the three main things you learned in this chapter.

To successfully delete a device from Sophos Central you must uninstall the Sophos Endpoint Agent and then delete the device from the Console.

Deleting a device from Sophos Central only removes the device, it does not uninstall the Sophos Endpoint Agent.

Only supported uninstall methods should be used to remove the Sophos Endpoint Agent.



Getting Started with Sophos Central Policies

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3505: Getting Started with Sophos Central Policies

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Policies

In this chapter you will learn what Sophos Central policies are. You will learn how to create, clone, and delete policies and how they are assigned.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to navigate sophos Central
- ✓ How devices are protected and managed by Sophos Central

DURATION **8 minutes**

SOPHOS

In this chapter you will learn what Sophos Central policies are. You will learn how to create, clone, and delete policies and how they are assigned.

Sophos Central Policies

Policies are used to define the security settings applied to protected devices

Policies can be assigned to users, computers, servers, and groups

Base policies are pre-configured and contain Sophos' recommended security settings

Base policies are split into categories

SOPHOS

Sophos Central policies are used to define security settings applied to protected devices. Policies can be assigned to users, computers, servers, and groups. Base policies are pre-configured by Sophos and contain recommended security settings.

Base policies are split into feature types which allows for granular control.

Base Policies

- Enforced by default
- Threat Protection Policy is the only policy with recommended security settings applied

The screenshot shows the Sophos Central Policies interface. At the top, there is a note: "Note: The policies at the top of the list override the policies at the bottom of the list." Below this, there are five sections: Threat Protection (1), Peripheral Control (1), Application Control (1), Data Loss Prevention (0), and Web Content (0). Each section contains a table with columns: Name, Status, Type (single / group), and Last modified.

Name	Status	Type (single / group)	Last modified
Base Policy - Threat Protection	✓ Enforced		Jul 18, 2022
Base Policy - Peripheral Control	✓ Enforced		Jul 7, 2022
Base Policy - Application Control	✓ Enforced		Jul 8, 2022
Base Policy - Data Loss Prevention	✓ Enforced		Jul 07, 2022
Web Content			

SOPHOS

Base policies are enforced by default, however, only the threat protection policy is configured with recommended security settings.

This is because the base policies for controlling peripheral devices, applications, websites, and data loss prevention are environment specific.

Creating a Policy

The screenshot shows the Sophos Central interface. On the left, there's a vertical navigation menu with several sections like Alerts, Threat Analysis Center, Log & Reports, People, Devices, Global Settings, Third-party Connectors, Project Review, and Account Health Check. Below these are sections for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Threat Threat. The 'Endpoint Protection' section is expanded, showing sub-options: Dashboard, ANALYST, and威脅 PROTECTION. Under '威脅 PROTECTION', the 'Policies' option is highlighted with an orange box. To the right, a larger window titled 'Endpoint Protection - Policies' is open. It shows a table with one row: 'Name: Base Policy - Threat Protection', 'Status: Enforced', and 'Type (single / group)'. A note at the top says, 'Note: The policies at the top of the list override the policies at the bottom of the list.' At the top right of this window, there's a 'Help' link, a user profile for 'Simon Smith', and a status message 'Sophos UK - Super Admin'. In the top right corner of the main window, there's a blue button labeled 'Add Policy' with an orange border. A large green arrow points from the 'Add Policy' button down to a green box containing the text 'Add new policy'. The bottom right corner of the main window has the 'SOPHOS' logo.

You can configure new policies to override some or all of the settings in a base policy. You can use new policies to apply different settings to different users, devices or servers. You can also create new policies to test new features for specific devices.

To create a new policy in Sophos Central navigate to the product in the left-hand menu. Once in the product menu, select **Policies** from the left-hand menu.

To create a new policy, click **Add Policy**. In this example we are creating an **Endpoint Threat Protection** policy.

Creating a Policy

Endpoint Protection Policies

Add Policy

Choose the feature type of the policy you want to create.

Feature *

Threat Protection

Type *

User (policies follow users across their devices)

Device (policies are assigned to device regardless of logged on user)

User Policies
Follow users across their devices

Add Policy

Choose the feature type of the policy you want to create.

Feature *

Threat Protection

Type *

User (policies follow users across their devices)

Device (policies are assigned to device regardless of logged on user)

Device Policies
Assigned to device(s) regardless of
the logged on user

SOPHOS

Select the feature you want to create the policy for. In this example, we have selected **Threat Protection**.

For endpoint protection policies, you will also need to select whether the policy will be a user or a device policy. User policies follow users across their devices, whereas device policies are assigned to devices regardless of the logged on user.

Creating a Policy

The screenshot shows the Sophos Endpoint Protection interface for creating a new computer policy. The left sidebar has 'Endpoint Protection' selected under 'ANALYST'. The main window title is 'Endpoint Protection - Create New Computer Policy'. It shows a warning message: 'This policy does not apply to any users.' Below this are two sections: 'Available Users' and 'Assigned Users'. The 'Available Users' section lists ten users: Adam Jones, Bill May, Bob Whitey, Anna Green, Anna Brown, Barbara House, Carly Fossils, Carter (User Admin), and Dan Hillbilly. There are no users assigned to the policy yet.

The options of assigning the policy will depend on the type of policy created. For example, a server protection policy can only be applied to specific servers or server groups.

Creating a Policy

The screenshot shows the Sophos Central interface for creating a new computer policy. The left sidebar has 'Endpoint Protection' selected under 'ANALYSE'. The main window title is 'Endpoint Protection - Create New Computer Policy'. It shows '0 USERS' and '0 GROUPS' and has a 'SETTINGS' tab selected, indicated by a blue border. A green bar at the top says 'Your policy settings give you the protection we recommend.' Below are sections for 'Live Protection', 'Deep Learning', 'Real-time Scanning - Local Files and Network Shares', and 'Real-time Scanning - Internet'. Each section contains several configuration options with checkboxes. The bottom right corner of the window has the 'SOPHOS' logo.

On the **SETTINGS** tab, you can configure the policy to your specifications.

New policies will have Sophos' recommended security settings automatically applied.

There are some security settings that are not applied automatically. You can configure these based on your requirements and can also configure schedule scanning, device isolation, and policy exclusions.

Creating a Policy

Automatically disabling a policy is useful if you want to apply a temporary policy to users

New policies are automatically enforced. If you want to bypass the policy, you must amend the setting on the **POLICY ENFORCED** tab.

You can select to automatically disable the policy at a specific time. This is useful if you want to apply a temporary policy to users.

Creating a Policy

The screenshot shows the Sophos Central interface for Endpoint Protection Policies. The left sidebar has 'Endpoint Protection' selected under 'ANALYST'. The main area is titled 'Endpoint Protection - Policies' and shows four sections: Threat Protection (2), Peripheral Control (1), Application Control (1), and Data Loss Prevention (1). In the Threat Protection section, 'IT Threat Protection' is highlighted with an orange border. In the Data Loss Prevention section, a new policy 'Data Loss Prevention' has been added, indicated by a green checkmark and a 'Load policy' button.

Name	Status	Type (single / group)	Last modified
IT Threat Protection	✓ Enforced	User (O365)	Jul 28, 2022
Base Policy - Threat Protection	✓ Enforced		Jul 28, 2022

Name	Status	Type (single / group)	Last modified
Base Policy - Peripheral Control	✓ Enforced		Jul 7, 2022

Name	Status	Type (single / group)	Last modified
Base Policy - Application Control	✓ Enforced		Jul 8, 2022

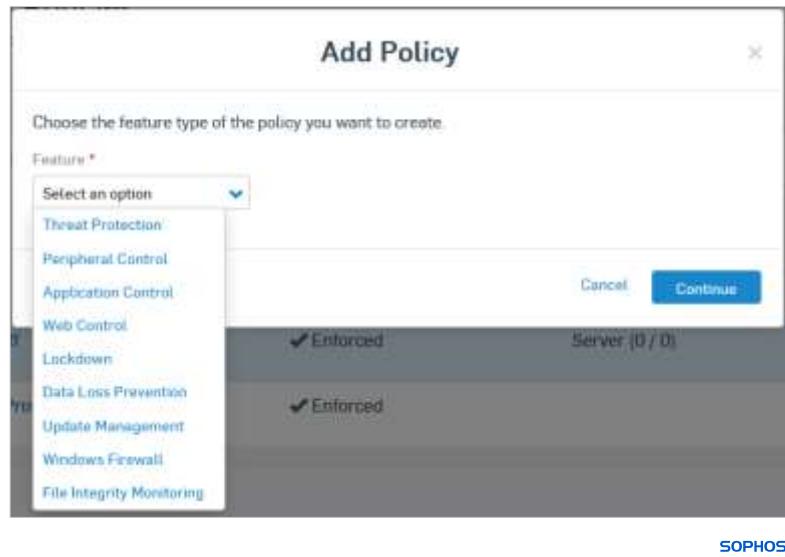
Name	Status	Type (single / group)	Last modified
Data Loss Prevention	✓ Enforced		Jul 28, 2022

New policies are saved into the feature policy list they were created in.

Server Policies

Server Protection Policies

- Only assigned to specific servers or server groups



Server protection policies are always device based. When you add a new server policy, it can only be assigned to specific servers or server groups. Base policies for threat protection, peripheral, application, and web control, data loss prevention, and update management have been modified where appropriate for server use.

There are additional policies for servers that allow you to manage Server Lockdown and File Integrity Monitoring.

New Features

The screenshot shows a browser window for 'Sophos Central' displaying the 'What's new in Sophos Central' page. A green banner at the top right of the page reads 'Not all security features are enabled by default'. Below the banner, there is a section titled 'SSL/TLS decryption of HTTPS websites' with a note about enabling it. A large green arrow points from this banner to a callout box on the right.

Not all security features are enabled by default

SSL/TLS decryption of HTTPS websites

Decrypt HTTPS websites using SSL/TLS. If enabled it also turns on HTTPS decryption for Web Control.

Note: You can exclude websites from decryption in the global settings pages.

Note: This setting applies to Windows servers running version 2.20 (or later) of the Core Agent.

Applies To

What's new in Sophos Central

We regularly update Sophos Central with improvements or new features. You can see the details here.

Latest features

Account Health Check enhancement

You can now easily see if any of your scanning exclusions or threat protection policy settings are reducing your protection. [Read more](#)

New root certificates for Sophos products

The next Sophos Endpoint and Server Protection update for Windows will contain new root certificates. Activate automatic root certificate updating to ensure successful installation. [Read more](#)

Cloud Optix now available in the EU

Sophos Cloud Optix is now available from our Sophos Central EU data center in Germany. [Read more](#)

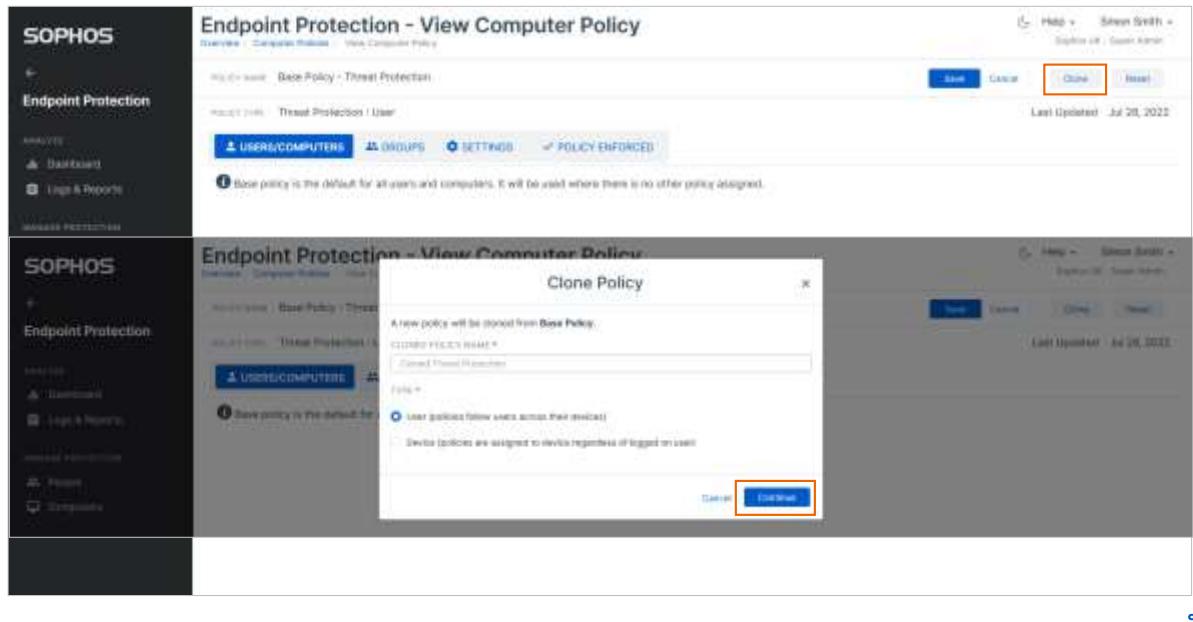
SOPHOS

It is important to understand that not all new threat protection features are enabled by default. This is because enabling new functionality without warning could have unexpected consequences.

A banner notification is added to Sophos Central announcing any new security features. You can make an informed decision regarding the enablement of new features on all protected devices, or only a couple at a time to monitor the effect the security feature has.

You can also access information on any new features by browsing the 'What's new!' help menu.

Cloning a Policy



SOPHOS

You can create a new policy by cloning an existing policy. In this example, we are cloning the threat protection base policy.

To clone a policy, open the policy you want to clone. In the top-right, click **Clone**.

You must re-name the policy, for endpoint protection policies you will also need to select either user or device and then click **Continue**.

Cloning a Policy

The screenshot shows the Sophos Endpoint Protection interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Endpoint Protection', 'ANALYSE', 'Logs & Reports', 'MANAGE PROTECTION' (with 'People' and 'Computers' options), and 'CONFIGURE' (with 'Policies' selected, indicated by a blue background). The main content area is titled 'Endpoint Protection - View Computer Policy' and shows 'Overview / Computer Policy / View Computer Policy'. It displays a policy named 'Cloned Threat Protection' (Policy Type: Threat Protection - Device) with 0 computers and 0 groups assigned. A prominent button labeled 'POLICY BYPASSED' is highlighted in blue. Below it, a note states: 'None of the settings of this policy will be applied to assigned targets. They will get their settings from the highest priority policy they are assigned to and which is not bypassed.' A tooltip explains: 'If you want to deactivate a specific setting, you need to re-enable this policy and set the relevant setting to off in the settings tab.' At the bottom of the page, a dark banner contains the text: 'Cloned policies are **not automatically enforced**. You **must enforce a cloned policy** for it to applied'.

It is important to note that when cloning a policy, it will not be automatically enforced. You must manually enforce a cloned policy for it to be applied.

To do this, select the **POLICY BYPASSED** tab and toggle the policy setting. This will enforce the policy.

Policy Precedence

- Policies are applied in the order they appear
- Sophos Central uses a first match approach

The screenshot shows the Sophos Central interface for managing policies. On the left is a dark sidebar with navigation options like Devices, User & Groups, Network Protection, and Policies (which is selected). The main area is titled 'Server Protection - Policies' and contains four sections: Threat Protection (1), Peripheral Control (1), Application Control (2), and Web Control (0). Each section has a table with columns for Name, Status, Server/Device Group, and Last modified. A green arrow points down to the table in the Threat Protection section, highlighting the order of policies.

Name	Status	Server/Device Group	Last modified
Automatic Cleaner OFF	Enabled	Server 01 / N	Aug 9, 2021
Base Policy - Threat Protection	Enabled		Mar 26, 2022

Name	Status	Server/Device Group	Last modified
Base Policy - Peripheral Control	Enabled		Mar 20, 2018

Name	Status	Server/Device Group	Last modified
Windows Activation Service	Enabled	Server 01 / N	Sep 30, 2018
Base Policy - Application Control	Enabled		Mar 27, 2022

Name	Status	Server/Device Group	Last modified

Policy settings can be received from multiple policies. The order the policies appear in Sophos Central dictate the order they are applied to protected devices.

Policies are processed using a first match approach, this means that the first policy that matches either the user, user group, device or server, or device or server group it was assigned to will be used.

Managing Policies

The screenshot shows the Sophos Central interface for managing Endpoint Protection Policies. The left sidebar has 'Endpoint Protection' selected under 'ANALYSIS'. The main area is titled 'Endpoint Protection - Policies' and shows a table of Threat Protection policies. A note at the top says: 'Note: The policies at the top of the list override the policies at the bottom of the list.' The table has columns for Name, Status, Type (single / group), and Last modified. The policies listed are: 'Contractors - Threat Protection' (Enforced, Computer ID / 1, Jul 28, 2022), 'IT Threat Protection' (Enforced, User (0 / 0), Jul 28, 2022), 'HR Threat Protection' (Enforced, Computer ID / 1, Jul 28, 2022), and 'Base Policy - Threat Protection' (Enforced). Below the table, it says 'Peripheral Control (1)'. The top right shows 'Help', 'Simon Smith - Sophos UK | Super Admin', 'Add Policy', and 'Delete' buttons.

Name	Status	Type (single / group)	Last modified
Contractors - Threat Protection	Enforced	Computer ID / 1	Jul 28, 2022
IT Threat Protection	Enforced	User (0 / 0)	Jul 28, 2022
HR Threat Protection	Enforced	Computer ID / 1	Jul 28, 2022
Base Policy - Threat Protection	Enforced		Jul 28, 2022

We recommend that you place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device where you wanted an individual policy to apply.

The base policy is always at the bottom, and is applied to any users, devices or servers that aren't covered by policies higher in the list.

You can re-arrange the policy list by clicking on a policy and dropping it into the position you want it.

Deleting a Policy

The screenshot shows the Sophos Central interface for Endpoint Protection Policies. The left sidebar has 'Endpoint Protection' selected. The main area displays a table of policies categorized by type: Threat Protection (4), Peripheral Control (1), and Application Control (1). A note at the top states: 'Note: The policies at the top of the list override the policies at the bottom of the list.' The 'Delete' button for each policy is highlighted with an orange border.

Name	Status	Type (single/group)	Last modified
IT Threat Protection	Enforced	User (0/3)	Jul 20, 2022
Contaminant - Threat Protection	Enforced	Computer (0/0)	Jul 20, 2022
HR Threat Protection	Enforced	Computer (0/0)	Jul 20, 2022
Base Policy - Threat Protection	Enforced		Jul 20, 2022
Base Policy - Peripheral Control	Enforced		Jul 20, 2022
Base Policy - Application Control	Enabled		Jul 20, 2022

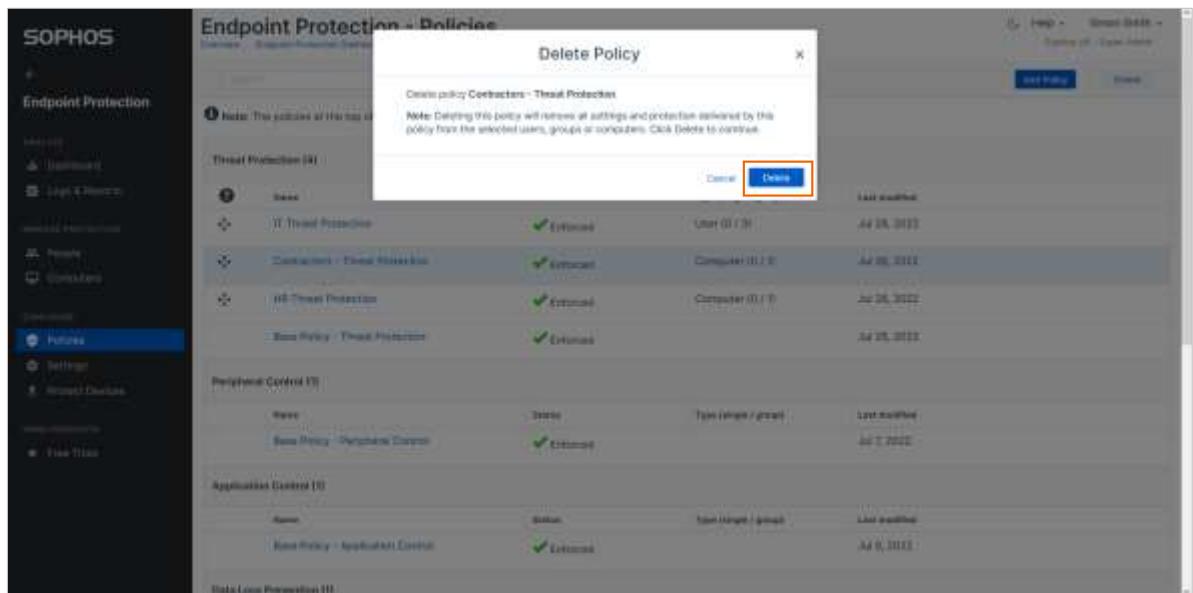
Base policies **CANNOT** be deleted or disabled

SOPHOS

Policies that are created or cloned can be deleted. Base policies cannot be deleted or disabled.

To delete a policy, select it from the list and click **Delete**.

Delete a Policy



Confirm that you want to delete the policy by clicking **Delete**.

SOPHOS

Deleting a Policy

The screenshot shows the Sophos Central interface for Endpoint Protection Policies. The left sidebar has 'Endpoint Protection' selected under 'ANALYST'. The main area is titled 'Endpoint Protection - Policies' and shows four sections: Threat Protection (3), Peripheral Control (1), Application Control (1), and Data Loss Prevention (0). The Threat Protection section lists three policies: 'IT Threat Protection' (status Enforced, last modified Jul 20, 2022), 'HE Threat Protection' (status Enforced, last modified Jul 20, 2022), and 'Base Policy - Threat Protection' (status Enforced, last modified Jul 20, 2022). The 'Base Policy - Threat Protection' row is highlighted with a red box. A delete icon is visible in the top right corner of this row. The bottom right corner of the main area contains the 'SOPHOS' logo.

Name	Status	Type (single / group)	Last modified
IT Threat Protection	Enforced	User (0 / 3)	Jul 20, 2022
HE Threat Protection	Enforced	Computer (0 / 0)	Jul 20, 2022
Base Policy - Threat Protection	Enforced		Jul 20, 2022

The policy has been removed from the policy list.

General Policy Recommendations



Use default settings within a policy where possible



Consider the role of the endpoint when changing default policy settings or creating new policies



Use Sophos Central base policies when possible



Set options on individual devices only when requiring temporary configuration



Create separate groups for devices that require long-term special configuration

SOPHOS

When configuring policies, we generally recommend the following:

- Use the default settings within a policy where possible
- Consider the role of the device when creating new policies
- Use the base policies where possible
- Set options on individual devices when making temporary configuration changes
- Create separate groups for devices that require long term special configuration

Please note that policy changes should be limited and precise so that the effects can be evaluated. They should be applied to a small group of devices for testing before being applied to all protected devices.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

True or False: New security features are enabled in the threat protection policy by default.

True

False

SOPHOS

Question 2 of 3

Match the policy to the behaviour.

Cloned Policy

Automatically enforced

New Policy

Automatically bypassed

Question 3 of 3



Complete the sentence.
The threat protection base policy is configured with...

Sophos' strict settings

All security features enabled

All security features disabled

Sophos' recommended
settings

SOPHOS

Chapter Review

Sophos Central **policies** are used to **define security settings** applied to protected devices. Policy settings can be received from multiple policies and are **processed using a first match approach**.

Base policies are **pre-configured** by Sophos to contain the **recommended security settings** and **cannot be deleted or disabled**.

New and cloned policies can be used to **apply different settings to different users, groups and devices**.
New policies are **automatically enforced** and **cloned policies** are **automatically bypassed**.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos Central policies are used to define security settings applied to protected devices. Policy settings can be received from multiple policies and are processed using a first match approach.

Base policies are pre-configured by Sophos to contain the recommended security settings and cannot be deleted or disabled.



Getting Started with the Sophos Central Threat Protection Policy

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3510: Getting Started with the Sophos Central Threat Protection Policy

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Threat Protection Policy

In this chapter you will learn which features are included in the threat protection policy.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to protect and managed devices in Sophos Central
- ✓ What Sophos Central policies and are and how they are assigned and managed

DURATION **20 minutes**

SOPHOS

In this chapter you will learn which features are included in the threat protection policy.

Threat Protection Policy

The screenshot shows the Sophos Central interface for managing threat protection policies. On the left, a sidebar menu includes options like Endpoint Protection, ANALYZE, and SETTINGS. The main content area is titled 'Endpoint Protection - View Computer Policy' and shows the 'Threat Protection' tab selected. It displays various policy settings, including 'Live Protection' and 'Deep Learning', both of which are currently enabled. A prominent green banner at the bottom of the page contains the text 'CAUTION! Changing the recommended settings could reduce your protection'.

The threat protection policy protects against malware, risky file types and websites, and malicious network traffic.

The threat protection base policy is automatically configured with Sophos' recommended security settings. These provide the best protection without complex configuration including:

- The detection of known malware
- Live lookups for the latest malware known to Sophos
- Proactive detection of unknown malware
- And, the automatic clean up of malware

Think carefully before you change the recommended settings because doing so may reduce your protection.

Threat Policy Check

The screenshot shows the Sophos Central interface for managing threat protection policies. On the left, a sidebar navigation menu includes 'Endpoint Protection' (selected), 'Analytics' (Dashboard, Logs & Reports), 'Manage Protection' (People, Computers), 'Cloud Work' (selected, Policies, Settings, Protect Devices), and 'Help' (Free Trial). The main content area is titled 'Endpoint Protection - View Computer Policy' under 'Threat Protection / User'. It displays several policy sections: 'User-recommended settings' (with a note: 'Your policy settings give you the protection we recommend.'), 'Live Protection' (with options like 'Use Live Protection to check live threat information from SophosLabs.com'), 'Deep Learning' (with 'Enable next-gen'), 'Real-time Scanning - Local Files and Network Shares' (with 'Enable real-time scanning' and 'Remote File' options), and 'Real-time Scanning - Internet'. At the top right, there are buttons for 'Save', 'Cancel', 'Close', and 'Reset', and a status message 'Last Updated: Jul 26, 2022'. The bottom right corner features the 'SOPHOS' logo.

The threat protection policy is checked by Sophos automatically. Sophos checks the configuration of each threat protection policy to see if the settings match Sophos recommendations.

Threat Policy Check

The screenshot shows the Sophos Server Protection - View Server Policy interface. On the left, there's a sidebar with 'Server Protection' selected under 'ANALYST'. The main area displays '0 SERVERS' and '0 GROUPS' under 'Threat Protection - Devices'. A banner at the top right says 'POLICY ENFORCED'. Below it, a note states: 'Some policy settings are turned off or misconfigured, or some exceptions are made. You don't have the protection we recommend.' Under 'Intercept X Advanced for Server', there's a note: 'Note: If you enable any Intercept X Advanced Security features, servers assigned to this policy will use an Intercept X Advanced for Server license.' The 'Runtime Protection' section contains several settings with checkboxes, many of which are highlighted with green checkmarks. A note below one setting says: 'This setting only applies to servers you add to the View Server Protection Feature GAP. Join the GAP now.' The 'Applies To' section shows icons for Windows, Linux, and Mac.

If a setting does not match, you will see a banner message indicating the policy settings do not match the recommended protection. Additionally, the setting that is misconfigured or not applied will be highlighted.

Any setting that is turned off in the threat protection policy must be carefully considered as the security of any protected devices will be compromised.



Additional information in
the notes

Live Protection

The screenshot shows the Sophos Endpoint Protection interface under 'View Computer Policy'. The left sidebar has 'POLICIES' selected. The main area shows 'Live Protection' settings with a note: 'Your policy settings give you the protection we recommend.' A red box highlights the 'Live Protection' section, which includes a toggle switch for 'Use Live Protection to check the latest threat information from SophosLabs online', a checkbox for 'Use Live Protection (using scheduled scans)', and a note: 'Note: The data may leave your geographic region and be shared with Sophos engineers.' A green callout box points to this note with the text 'Live lookups to SophosLabs database'. Other sections shown include 'Deep Learning' and 'Real-time Scanning - Local Files and Network Shares'.

Whilst the settings in the threat protection policy are automatically enabled, it is useful to understand what they mean.

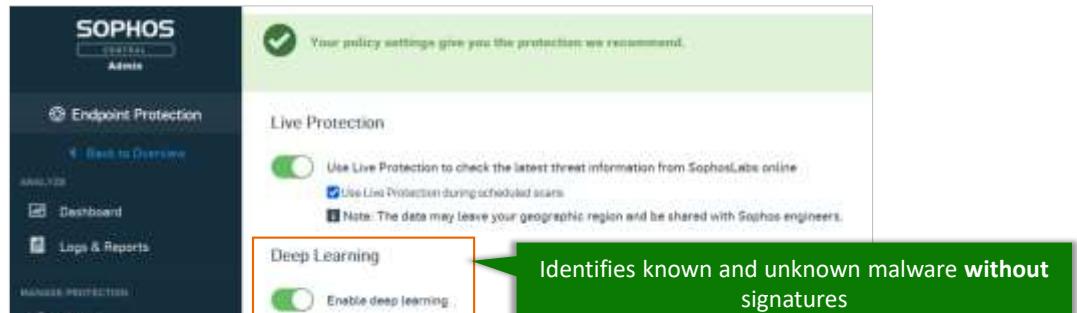
Sophos Live Protection is used to determine whether a file is malicious. It provides instant lookups against the latest known malware. Live Protection means that virus definition files do not have to be downloaded to each device ensuring that the latest information is used.

Live Protection is enabled for on-demand and scheduled scanning by default in the threat protection policy.

[Additional Information]

Sophos Threat Center: <https://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas>

Portable Executable (PE) Scanning



AppID Application identifier given to an application that sits within a category

Machine Learning Score An ML or ML PUA score between 0 and 100. An ML score over 30 is considered malicious

File Reputation Score A score between 0 and 100. 0 indicates a bad reputation, 100 indicates a clean file

SOPHOS

Deep learning uses advanced machine learning to detect threats. It can identify known and previously unknown malware without using signatures.

When a PE file is scanned, it returns three pieces of data:

- The **AppID** which is the application identifier given to an application that sits within a category
- The **machine learning score** which is also known as the ML or ML PUA score. This is a number between zero and one hundred. If a file has an ML score of over 30 it will be considered malicious. If a file has a ML PUA score of below 20, it is considered a PUA
- The **file reputation score**. If a file has a reputation score of zero this indicates a bad reputation. If a file has a reputation score of one hundred, the file is considered clean

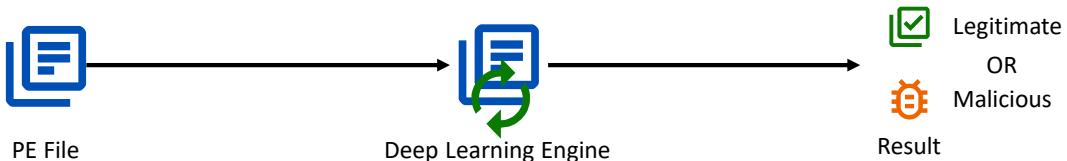
Please note that a file will return a reputation score of one hundred if you have excluded the file either globally or through a policy.



Additional information in
the notes

Portable Executable (PE) Scanning

- Deep learning is enabled by default in the Threat Protection policy
- Evaluates files based on characteristics



SOPHOS

The deep learning engine evaluates files based on the information returned, determining if the file is legitimate or malicious. If the file is categorized as malicious, it is removed from the device.

PE scanning is enabled by default in the threat protection policy.

[Additional Information]

For more information about the reputation scores for files please see knowledge base article **KB-000037118**. <https://support.sophos.com/support/s/article/KB-000037118>

Real-Time Scanning – Files and Shares

The screenshot shows the Sophos Central Admin interface. On the left, there's a sidebar with various navigation options like 'Dashboard', 'Logs & Reports', 'People', 'Computers', 'Policies', 'Settings', and 'Protect Devices'. The 'Policies' option is currently selected. The main area is titled 'Live Protection' and contains sections for 'Live Protection', 'Deep Learning', and 'Real-time Scanning - Local Files and Network Shares'. The 'Real-time Scanning' section is highlighted with a red border. It includes a toggle switch for 'Enable real-time scanning' and a checkbox for 'Remove files'. A green callout box with the text 'Scans files as they are accessed' points to this section. Below it is another green callout box with the text 'On-demand scans' pointing to the 'On-demand scans' section in the interface.

Real-time scanning of files and network shares scans files when they are accessed. File access will be denied if the file is determined to be malicious. Remote files means that files in network shares are scanned.

Real-time scanning is also used when an on-demand scan is initiated on a protected device.

Web Protection

The screenshot shows the 'Real-time Scanning - Internet' section of the Sophos Central Threat Protection Policy. It includes settings for scanning downloads, blocking malicious websites (which is highlighted with a red border), and detecting low-reputation files. A dropdown menu for 'ACTION TO TAKE ON LOW-REPUTATION DOWNLOADS' shows 'Prompt user' selected. Under 'REPUTATION LEVEL', 'Recommended' is checked. To the right, a green callout box states: 'If a user attempts to access a malicious website, the site will be blocked'. Below this, a browser window shows a blocked website: 'High Risk Website Blocked' at 'sophos-test.com/test/websitedir.html'. The page content says 'High Risk Website Blocked' and 'Access has been blocked as the item C:\Generic-4 has been found on this website. Return to the page you were previously viewing.' A 'Return to previous page' button is also visible. A large green arrow points from the 'Web protection is enabled by default in the threat protection policy' text to the 'Block access to malicious websites' setting.

Real-time Scanning - Internet

Scan downloads in progress

Block access to malicious websites

Detect low-reputation files

ACTION TO TAKE ON LOW-REPUTATION DOWNLOADS

Prompt user

REPUTATION LEVEL

Recommended

If a user attempts to access a malicious website, the site will be blocked

High Risk Website Blocked

sophos-test.com/test/websitedir.html

High Risk Website Blocked

Access has been blocked as the item C:\Generic-4 has been found on this website.

Return to the page you were previously viewing.

Return to previous page

Web protection is enabled by default in the threat protection policy

SOPHOS

Web protection protects users against malicious websites and downloads. It checks the reputation of a URL or IP address that is being accessed. All major Internet browsers are supported.

Web protection utilizes Sophos Extensible List (SXL) lookups and settings for web protection are configured in the threat protection policy in the 'Realtime scanning – Internet' section.

Download Reputation

The screenshot shows the 'Real-time Scanning - Internet' section of the policy configuration. It includes three toggle switches: 'Scan downloads in progress' (on), 'Block access to malicious websites' (on), and 'Detect low-reputation files' (on). Below these are dropdown menus for 'ACTION TO TAKE ON LOW-REPUTATION DOWNLOADS' (set to 'Prompt user') and 'REPUTATION LEVEL' (set to 'Recommended'). A green callout box points to the 'Detect low-reputation files' switch with the text: 'Detect low reputation files is enabled by default in the threat protection policy'.

<http://sophostest.com> can be used to test the download reputation settings

The screenshot shows a Sophos Endpoint alert window. The title bar says 'SOPHOS Endpoint'. The main content area has a yellow warning icon and the text 'Low reputation download detected'. It states 'Downloaded file(s) with low reputation. We recommend that you delete the file(s.)'. At the bottom, it shows '04:50 low.exe' and two buttons: 'Delete' and 'Trust'. A green callout box points to the alert message with the text: 'http://sophostest.com can be used to test the download reputation settings'.

SOPHOS

'Detect low-reputation files' warns if a download has a low reputation. All downloaded files are checked to determine the file type. If the file is an executable, for example a .exe file, a full reputation lookup is performed. A file's reputation is determined by performing a file checksum lookup from the device against known files and their reputation created by SophosLabs.

You can edit the 'detect low-reputation files' setting. The default is to prompt the user, however, you can change this to log the event only. You can also determine the reputation level which is automatically configured to recommended, however, this can be changed to strict.

Please note that if you set the reputation level to strict, all medium and low reputation files will be detected which may cause issues for users. You can use sophostest.com to test the reputation settings for various website categories.

Remediation

The screenshot shows the Sophos Central Admin interface. On the left, there's a sidebar with 'Endpoint Protection' selected. The main area has two sections: 'Remediation' and 'Runtime Protection'. The 'Remediation' section contains two green toggle switches: 'Automatically clean up malware' (with a note about exceptions) and 'Enable Threat Graph creation'. A callout box points to this section with the text: 'Malicious files are automatically cleaned up and if necessary a Threat Graph created'. The 'Runtime Protection' section includes settings for protecting documents from ransomware and applications like Microsoft Office and media. A callout box points to the 'Events' tab on the right with the text: 'All detection and clean up actions are logged on the Events tab of the Sophos Endpoint Agent'. The 'Events' tab is open, showing a list of log entries with columns for Date, Source, and Description. Examples include 'Access to location https://malicious.com/cleaner.exe file was blocked for user [REDACTED]' and 'Threat cleanup up: [REDACTED]'. A green arrow points from the 'Events' tab to the list of log entries.

Malicious files are automatically cleaned up and if necessary a Threat Graph created

All detection and clean up actions are logged on the **Events** tab of the Sophos Endpoint Agent

Date	Source	Description
10/09/2022 10:00:08	[REDACTED]	Access to location https://malicious.com/cleaner.exe file was blocked for user [REDACTED]
10/09/2022 10:00:09	[REDACTED]	Access to location http://malicious.com/cleaner.exe file was blocked for user [REDACTED]
10/09/2022 10:00:10	[REDACTED]	Access to location https://malicious.com/cleaner.exe file was blocked for user [REDACTED]
10/09/2022 10:00:11	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:12	[REDACTED]	Threat cleanup up: [REDACTED]
10/09/2022 10:00:13	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:14	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:15	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:16	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:17	[REDACTED]	Threat cleanup up: [REDACTED]
10/09/2022 10:00:18	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:19	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:20	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:21	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:22	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:23	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:24	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:25	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:26	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:27	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:28	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:29	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:30	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:31	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:32	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:33	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:34	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:35	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:36	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:37	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:38	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:39	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:40	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:41	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:42	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:43	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:44	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:45	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:46	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:47	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:48	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:49	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:50	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:51	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:52	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:53	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:54	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:55	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:56	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:57	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:58	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:59	[REDACTED]	Threat cleanup up:
10/09/2022 10:00:59	[REDACTED]	File enumeration from hash monitored.

By default, detected malware will automatically be cleaned up. All detection and clean up actions are displayed in the **Events** tab of the Sophos Endpoint Agent.

If a PE file is detected as malicious it will be cleaned up even if automatic clean up has been disabled, the file is quarantined and can be restored in the case of a false positive.

Threat graphs are created by default for some detections where necessary. Threat graphs can assist with investigations into malicious activity.

Runtime Protection - CryptoGuard

- Monitors specific file types in specific locations for malicious actions that indicate an attack
- Creates just-in-time copies of the files in a cache
- Terminates the process generating the behaviour If malicious
- Restores any encrypted files from the cache

The screenshot shows the Sophos Central web interface. On the left, a dark sidebar menu includes 'Dashboard', 'Logs & Reports', 'Manage Protection' (with 'People' and 'Computers' options), 'CONTROLS' (with 'Policies' selected, shown in blue), 'Settings', and 'Protect Devices'. The main content area has a light background. At the top, a section titled 'Protect document files from ransomware (CryptoGuard)' contains three checked checkboxes: 'Protect from remotely run ransomware', 'Protect from encrypting File System attacks', and 'ACTION TO TAKE ON RANSOMWARE DETECTION' (with 'Terminate Process' selected). A note below says 'This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. Join the EAP now.' Below this, another section titled 'Protect from master boot record ransomware' also has three checked checkboxes: 'Protect critical functions in web browsers (Safe Browsing)', 'Mitigate exploits in vulnerable applications', and 'Protect web browsers' (which further includes 'Protect web browser plugin', 'Protect Java applications', 'Protect media applications', and 'Protect office applications'). The bottom right corner of the interface features the 'SOPHOS' logo.

The runtime protection features detect suspicious or malicious behaviour or traffic.

CryptoGuard protects against remotely run ransomware and file encryption. It does this by monitoring specific file types in specific locations looking for actions that indicate a ransomware attack. One indication could be a process that opens and writes to multiple files in a short period of time.

If an action like this is detected, just-in-time copies of the targeted files are created and stored in a local cache on the device. If CryptoGuard determines the action as malicious, the process is terminated.

Once the attack has been prevented, CryptoGuard restores any files it can from the cache. For some detections, a threat graph will be created to determine how the attack process started along with identifying events happening on the device that may relate to the root cause of the attack.

Runtime Protection - WipeGuard



Protect from master boot record ransomware

- Prevents attack that target the master boot record
- Prevents bootkit installation

WIPEGUARD



Some forms of ransomware overwrite the master boot record which leaves the operating system in an unbootable state.

The MBR is a code stored in the first sectors of a hard disk drive. It holds information about the disk partitions and launches the operating systems boot loader. Without access to the MBR, the device is unable to determine which disk partition contains the operating system or how to start it.

WipeGuard prevents attacks that target the master boot record and prevents rootkit installation. A bootkit is a variant of a rootkit that infects a devices start up code and can be used to attack full disk encryption systems.

Runtime Protection - Safe Browsing



Protect critical functions in web browsers (Safe Browsing)

Safe Browsing protects against exploits and is enabled by default in the threat protection policy



- For example, man-in-the-browser (MitB) which infects a web browser by exploiting browser security vulnerabilities
- This allows an attacker to modify web pages, modify transaction content or insert additional transactions



- Safe browsing monitors the crypto, network and presentation DLLs of a browser to detect when another application is interfering
- Safe browsing only warns the user that a browser compromise was detected
- The browser session is not terminated but the administrator is provided with event information

SOPHOS

Internet browser exploits are a class of threat where an attacker targets a vulnerability in either the Internet browser or in an application that browser calls to process a web request, such as Flash Player or Java.

An example of this is a Man-in-the-Browser attack. A form of Internet threat that infects an Internet browser by taking advantage of vulnerabilities in browser security. This allows an attacker to modify the web pages, modify transaction content or insert additional transactions.

Safe Browsing monitors the crypto, network, and presentation DLLs of a browser to detect when another application is interfering. Safe Browsing only warns the user that the browser was compromised. It will initiate a scan but will not terminate the browser session, and the administrator is provided with event information to support an investigation.

Runtime Protection - Mitigate Exploits

- Protect applications prone to malicious exploitation



SOPHOS

Mitigate exploits in vulnerable applications protects applications which are prone to being exploited for malicious intent.

Runtime Protection - Process Protection

The screenshot shows a configuration panel for 'Protect processes'. A green toggle switch is turned on. Below it is a list of checked options:

- Prevent process hollowing attacks
- Prevent DLLs loading from untrusted folders
- Prevent credential theft
- Prevent registry credential theft (with a note: "This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. Join the EAP now")
- Prevent code cave utilisation
- Prevent APC violation
- Prevent privilege escalation

A green callout box on the right side states: "Identifies the attack technique and prevents it".



Attacker migrates from process to process in order to establish persistence.

Intercept X protects against this by identifying the attack technique and preventing it.

SOPHOS

If an attacker has gained access to a device, the malicious code they can use is only useful whilst the process they have targeted is running.

If the process is terminated, the communication with the attacker is also stopped. An attacker will attempt to move to another running process on the device to maintain a connection. This type of process migration is common practice for attackers.

Sophos protects against this by identifying the technique being used and preventing it.

Runtime Protection

Dynamic shellcode protection

Validate CTF Protocol caller

Prevent side loading of insecure modules

 This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. [Join the EAP now](#)

Protect browser cookies used for MFA sign-in

 This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. [Join the EAP now](#)

Dynamic shellcode protection

Detects behaviour of covert remote access agents

Validate CTF Protocol caller

Intercepts and blocks applications that attempt to exploit CTF on Windows devices

SOPHOS

These four protection features are enabled by default through the threat protection policy.

Dynamic shellcode protection detects the behaviour of covert remote access agents and prevents attackers from gaining control of the network.

Validate CTF Protocol caller intercepts and blocks applications that attempt to exploit a vulnerability on Windows devices. This vulnerability, CTF, allows non-administrative and unauthorized users to hijack any Windows process, including applications that are running in a sandbox.

Runtime Protection

- Dynamic shellcode protection
- Validate CTF Protocol caller
- Prevent side loading of insecure modules
 - Windows This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. [Join the EAP now](#)
- Protect browser cookies used for MFA sign-in
 - Windows This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. [Join the EAP now](#)

Prevent side loading of
insecure modules

Detects behaviour of covert remote access agents

Protect browser cookies
used for MFA sign-in

Prevents unauthorized applications from decrypting the AES keys used to encrypt MFA
cookies

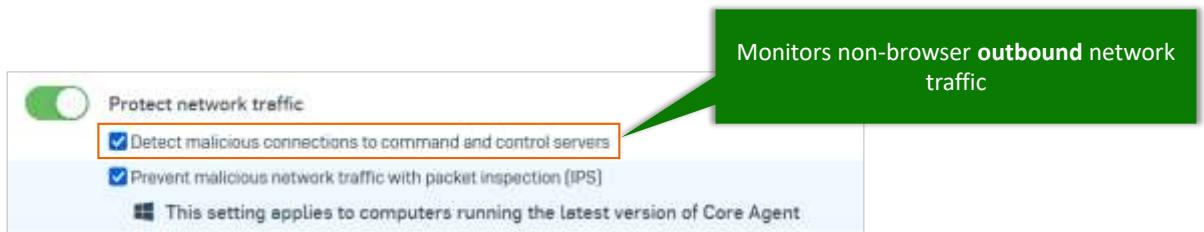
SOPHOS

Prevent side loading of insecure modules prevents an application from side-loading a malicious DLL that poses as a DLL that serves as a proxy to maintain compatibility between older applications and new operating system versions. Attackers may place malicious DLLs to manipulate this functionality, or bypass Tamper Protection and remove the Sophos Endpoint Agent.

Protect browser cookies used for MFA sign-in prevents unauthorized applications from decrypting the AES key used to encrypt MFA cookies.

Runtime Protection - Malicious Traffic Detection

- Detects processes which attempt to connect **outbound** to known bad URLs and malware sites
- **Reports traffic** to trigger memory scans
- If a HP/Mal detection is triggered, the threat is automatically cleaned up



SOPHOS

Malicious Traffic Detection monitors outbound web traffic that does not originate from a browser. It monitors HTTP traffic for signs of connectivity to known bad URLs and other malware sites.

If malicious traffic is detected, it can be an early indicator that a new piece of malware may be present. If a process attempts to connect to a known malware URL, the traffic is reported and can trigger memory scans. If this results in a detection, the threat will be cleaned up.

[Additional Information]

Sophos provides a test script for malicious traffic detection that can be downloaded from Knowledge base article **KB-000035314**. <https://support.sophos.com/support/s/article/KB-000035314>

Runtime Protection - Malicious Traffic Detection

- Traffic is scanned for known attacks
- Blocks threats before they can infect the Operating System or targeted application



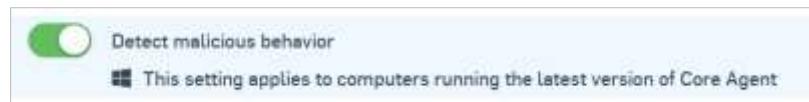
SOPHOS

Malicious Traffic Detection makes use of packet inspection to scan inbound and outbound network traffic for known attacks.

If an attack is detected, it is blocked. This protects against lateral movement as well as external attacks.

Runtime Protection - Detect Malicious Behaviour

- Scans **inbound** and **outbound** network traffic for **malicious behaviour patterns**
- If an attack is detected in outbound traffic, it could indicate a botnet attack



Inbound traffic

Communication sent **from a remote device** to a device inside the network

Outbound traffic

Communication sent from a device inside the network **to a remote device**

SOPHOS

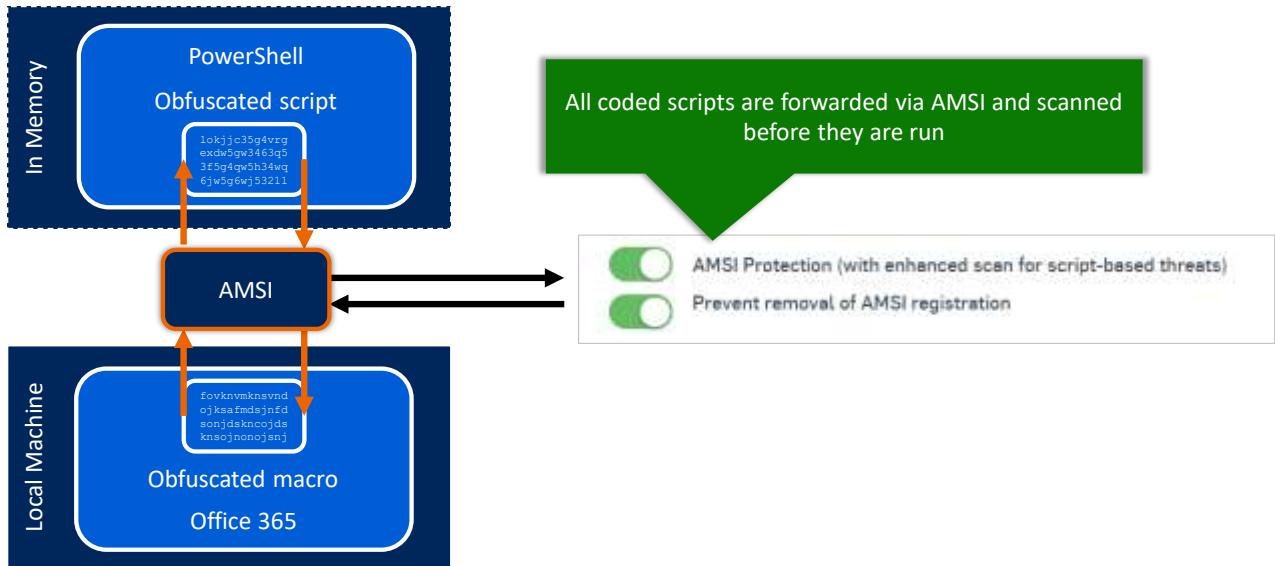
The detect malicious behaviour feature scans inbound and outbound network traffic for malicious attack behaviour patterns. If an attack is detected in outbound traffic, it could be an indicator that the device is being used as part of a botnet attack to communicate with other devices on the network.

Inbound traffic is communication sent from a remote device outside of the network to a device inside the network.

Outbound traffic is communication sent from a device inside the network to a remote device outside of the network.



Runtime Protection - AMSI Protection



SOPHOS

Anti-Malware Scan Interface (AMSI) is a versatile interface standard that allows applications and services to integrate with any anti-malware product, it is agnostic of anti-virus vendors.

Microsoft designed AMSI so that all scripts, statements of support applications, and languages can be scanned whether originating from a local file or executed in memory. For example, a PowerShell script can be called directly from a URL and executed in memory. When Sophos registers their AMSI provider, all AMSI calls are passed to the Sophos Endpoint Agent so that all executed code is scanned, regardless of whether it is run in memory or from a local file.

Malicious, and sometimes benign scripts, are often obfuscated. Usually, an obfuscated script is used to prevent users from viewing sensitive data like passwords, however, malware authors obfuscate their scripts hoping that anti-malware vendors will not detect or scan the code. Sophos protects against this type of attack by scanning all scripts which are forwarded via AMSI before they are run. The application used to run the code are notified of any threat detected and an event is logged.

[Additional Information]

To find out what data is collected by AMSI, please see knowledgebase article **KB-000038919**:
<https://support.sophos.com/support/s/article/KB-000038919>

Activity

Ransomware threat examples



Do you notice anything the threats have in common?

	BitPaymer	SamSam	Ryuk	Dharma	GandCrab
Type	Targeted	Targeted	Targeted	Targeted	RaaS
Deployment	RDP	RDP	RDP	RDP	RDP/Email/Exploit Kits
Targets	Medium/large organizations	Medium/large organizations	Medium/large organizations	Small organizations	Any
Typical ransom demand	\$50,000-\$1M+	\$40,000	\$100,000	\$5,000	\$1,000-\$8,000+
Frequency of attacks	Multiple a week	1+ a day	Multiple a week	Multiple a day	Frequency is unknown due to anyone being able to use the kit, however it is very popular
Desired damage	All servers	All servers and endpoints	All servers	Critical servers	Any
Regions affected	Global	Global with highest % in US	Global	Global	Global
Can be decrypted without paying	No	No	No	No	Some variants but mostly not
Payment method	Bitcoin arranged via email, sometimes dark web onion site	Bitcoin arranged via dark web onion site	Bitcoin arranged via email	Bitcoin arranged via email	Bitcoin arranged via dark web onion site
Additional insights	Spends time to ensure all backups are deleted before the attack	Has a history of targeting healthcare	Spends time to ensure all backups are deleted before the attack; attempts to disable antivirus	Manually attempts to disable antivirus before attacking	Regular updates and support from the developers; recently released all the encryption keys for Syrian victims of GandCrab and said Syria would not be targeted anymore

Here are few examples of ransomware.

Do you notice anything the threats have in common?

Activity



The common factor is **RDP**

	BitPaymer	SamSam	Ryuk	Dharma	GandCrab
Type	Targeted	Targeted	Targeted	Targeted	RaaS
Deployment	RDP	RDP	RDP	RDP	RDP/Email/Exploit Kits
Targets	Medium/large organizations	Medium/large organizations	Medium/large organizations	Small organizations	Any
Typical ransom demand	\$50,000-\$1M+	\$40,000	\$100,000	\$5,000	\$1,000-\$8,000+
Frequency of attacks	Multiple a week	1+ a day	Multiple a week	Multiple a day	Frequency is unknown due to anyone being able to use the kit, however it is very popular
Desired damage	All servers	All servers and endpoints	All servers	Critical servers	Any
Regions affected	Global	Global with highest % in US	Global	Global	Global
Can be decrypted without paying	No	No	No	No	Some variants but mostly not
Payment method	Bitcoin arranged via email, sometimes dark web onion site	Bitcoin arranged via dark web onion site	Bitcoin arranged via email	Bitcoin arranged via email	Bitcoin arranged via dark web onion site
Additional insights	Spends time to ensure all backups are deleted before the attack	Has a history of targeting healthcare	Spends time to ensure all backups are deleted before the attack; attempts to disable antivirus	Manually attempts to disable antivirus before attacking	Regular updates and support from the developers; recently released all the encryption keys for Syrian victims of GandCrab and said Syria would not be targeted anymore

The common factor is RDP. Many of the millions of RDP servers connected to the Internet are protected by only a username and password, and many of those passwords are weak enough to be guessed. Correctly guess a password on just one of those devices and you are into an organization's network.

It is not a new technique, and it sounds almost too simple to work, yet it is popular enough to support criminal markets selling both stolen RDP credentials and compromised devices. The technique is so successful that the criminals are crippling organizations with targeted ransomware, demanding five-figure ransoms.

Server Protection

The screenshot shows the Sophos Central interface for Server Protection. On the left, a dark sidebar menu includes 'Dashboard', 'Logs & Reports', 'Servers', 'Policies' (which is selected and highlighted in blue), 'Settings', and 'Protect Devices'. The main content area is titled 'Server Protection - View Server Policy' for 'Base Policy - Threat Protection'. It shows a 'POLICY FLOW' section with tabs for 'SERVERS' (selected), 'GROUPS', 'SETTINGS', and 'POLICY ENFORCED'. A green checkmark indicates 'Your policy settings give you the protection we recommend.' Below this, the 'Intercept X Advanced for Server' section contains a note about licensing and several protection options. To the right, a large green callout bubble points to a column labeled 'Applies To' which lists 'Windows', 'Linux', and 'Mac OS'. An orange box highlights this column. The bottom right corner of the interface features the 'SOPHOS' logo.

The threat protection policy for servers includes the same protection features as the endpoint policy, however, some features have been adapted for server use.

In the server threat protection policy, a column indicator is included down the right-hand side to indicate which features apply to which platforms.



Additional information in
the notes

Server Protection

The screenshot shows the Sophos Central interface for 'Server Protection'. On the left sidebar, 'Policies' is selected. The main pane displays various protection features with toggle switches. One feature, 'Enable CPU branch tracing', is highlighted with an orange border. To its right, there is a note: 'This setting only applies to servers you add to the New Server Protection Features EAP. Join the EAP now.' A vertical column of green checkmarks is visible on the far right.

Setting	Status
Protect processes	Enabled
Prevent process hijacking attacks	Enabled
Prevent DLLs loading from untrusted folders	Enabled
Prevent credential theft	Enabled
Prevent registry credential theft	Enabled
Prevent code cache utilization	Enabled
Prevent APC violation	Enabled
Prevent privilege escalation	Enabled
Enable CPU branch tracing	Enabled (highlighted)
Dynamic shieldcode protection	Enabled
Validate CTF Protocol calls	Enabled
Prevent side loading of insecure modules	Enabled
Protect browser cookies used for MFA sign-in	Enabled
Linux runtime detections	Enabled
Deep Learning	Enabled
Enable deep learning	Enabled
Remediation	Enabled
Enable Threat Graph creation	Enabled

There are additional protection features including the server treat protection policy.

Enable CPU branch tracing is an optional feature of Intel processors that allows tracing of processor activity for detection. We support it on Intel processors with the various architectures. If there is a legitimate hypervisor on the server, it is not supported.

Linux runtime detections provide runtime visibility and threat detection for Linux server workloads and containers. You can manage these alerts in the Threat Analysis Center.

Enable Security Heartbeat, this sends server health reports to each Sophos Firewall registered with your Sophos Central account. If more than one firewall is registered, reports go to the nearest one available. If a report shows that a server may be compromised, the firewall can restrict its access.

[Additional Information]

Intel processor supported architectures: Nehalem, Westmere, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Goldmont, SkyLake, and Kaby Lake.

Advanced Settings

The screenshot shows the Sophos Central Threat Protection Policy interface. The left sidebar has sections for Endpoint Protection, ANALYZE, and CONFIGURE. Under CONFIGURE, 'Policies' is selected. The main content area is titled 'Advanced Settings' with a note: 'We recommend that you leave these set to the defaults. However, you might want to change them temporarily. Learn more.' A button 'View advanced settings' is shown. An orange box highlights the following settings:

- Turn on anti-ransomware protection and all exploit mitigations ?
- Scan trusted installations
- Block email attachment file types that are currently associated with malware

Below these is a dropdown 'Deep learning detection level: Default'. Another orange box highlights:

- Track network connections
- Turn on event logging
- Generate file hashes remotely for event logging
- Periodically scan across memory in the background

Other sections visible include 'SSL/TLS decryption of HTTPS websites' (with a note about excluding websites from decryption), 'Device Isolation' (with a note about isolating computers on red health), and a large blue banner at the bottom stating 'We do **not** recommend changing these settings'.

Advanced settings are for testing and troubleshooting use only.

We **do not recommend** changing these settings.

SOPHOS

SSL/TLS Decryption of HTTPS Websites

- Not enabled by default
- Decrypts and checks the contents of HTTPS websites for threats

SSL/TLS decryption of HTTPS websites

Decrypt HTTPS websites using SSL/TLS. If enabled it also turns on HTTPS decryption for Web Control

ⓘ Note: You can exclude websites from decryption in the [global settings pages](#)
 ⓘ This setting isn't available for all customers yet. For details, see [knowledgebase article KB-000043550](#)

SOPHOS

Selecting to decrypt websites using SSL/TLS means that the contents of HTTPS websites are decrypted and checked for threats.

If a website is determined to be risky it will be blocked. The Sophos Endpoint Agent will display a message to the user which gives them the option to submit the website to SophosLabs for re-assessment.

Please note that if decryption is enabled, it applies to the devices, device groups, users, and user groups the policy is assigned to. It is also applied to web control checks for all assigned targets.

Device Isolation

- Not enabled by default
- A device with a red health status will automatically isolate from the network
- Access to the network and Internet are disconnected
- Communication with Sophos Central is still enabled

Device Isolation

 Allow computers to isolate themselves on red health

i Note: If a computer has red health, it will isolate itself from the network. It will still communicate with Sophos Central.

SOPHOS

Device isolation is not enabled by default.

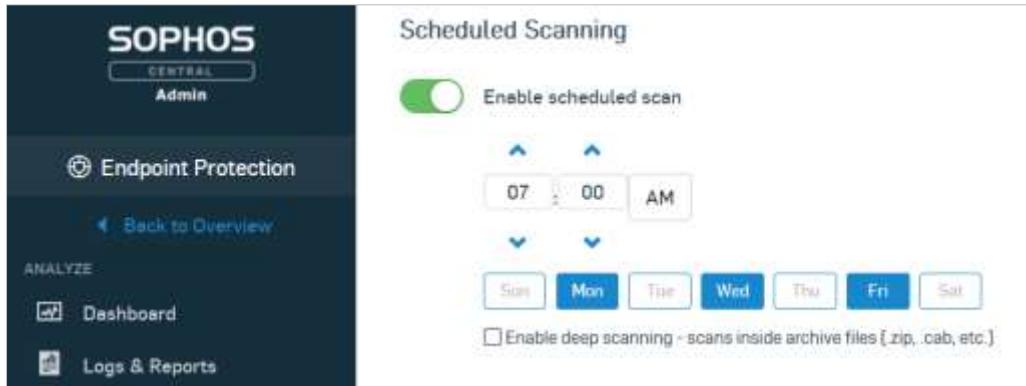
When enabled, it allows devices to isolate from the network automatically if the health status of the device is red. Once isolated, the device cannot access the network or the Internet. It will however still communicate with Sophos Central.

Once the health state of the device is healthy, either green or amber, the device isolation will be removed automatically. Access to the network and Internet will be restored.

Device isolation protects the network from lateral movement attacks.

Scheduled Scanning

- Not enabled by default
- The scheduled scan time is the time on the device, not UTC time
- Deep scanning may increase system loads



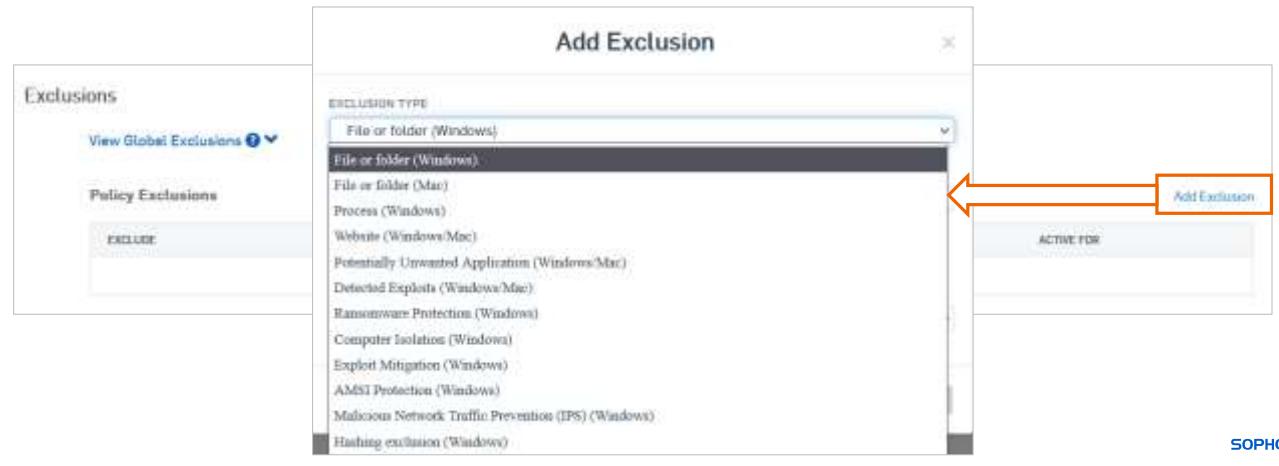
SOPHOS

Scheduled scanning is not automatically enabled. It can be enabled and a schedule can be set. Please note that the scheduled scan time displayed is the time on the device, not UTC time.

If you select to enable deep scanning, the scheduled scan will scan inside archive files. This may increase the system load and make the scan time significantly slower. We recommend that if you choose to enable deep scanning, your schedule is configured so that the scanning takes place outside of active hours to minimize any disruption to users.

Policy Exclusions

- Not enabled by default
- Exclude files, folders, websites, and applications from threat scanning
- Excluded items will still be checked for exploits

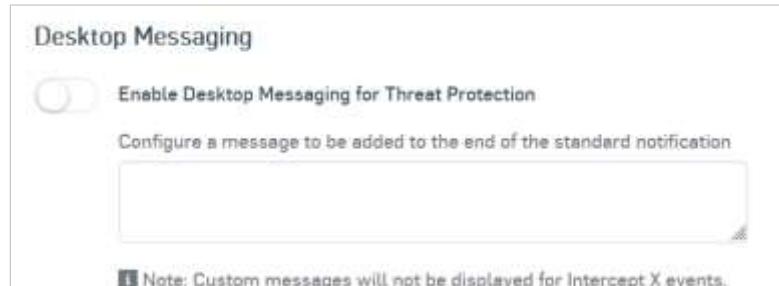


You can exclude files, folders, websites, and applications from threat scanning. Any exclusions applied in a threat protection policy are only used for the assigned devices or users of that policy.

Excluded items will still be checked for exploits, however, you can stop checking for a detected exploit by using an exploit exclusion.

Desktop Messaging

- Enter a custom notification message
- The custom message will be displayed after the standard notification



SOPHOS

In the 'Desktop Messaging' section, you can add a custom message that will be displayed at the end of any standard notification.

If you leave the message box empty, the standard message will be displayed.

Simulation: Test the Threat Protection Policy



In this simulation you will test some of the features of the Threat Protection policy using the recommended settings.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/TestThreatProtection/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/TestThreatProtection/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which protection feature checks suspicious files during on-access scanning against the latest malware database?

Deep Learning

Dynamic shell code
protection

Live Protection

Detect Malicious Behaviour

SOPHOS



Question 2 of 3

What type of activity does CryptoGuard detect as an indicator that ransomware may be active?

A process that changes the Windows file encryption settings

A process that communicates with known bad URLs

A process that matches the behaviour of known exploits

A process that opens and writes files in a short period of time

SOPHOS



Question 3 of 3

Match the protection feature with the correct description.

WipeGuard



Performs instant in-the-cloud checking for file characteristics

Live Protection



Checks the reputation of URL and IP addresses

Safe Browsing



Protects a device from having its master boot record encrypted

SOPHOS

Chapter Review

The threat protection policy **protects against malware, risky file types, websites, and malicious network traffic.**

Some configuration features are **not** enabled by default.

You can exclude files, folders, websites, and applications from scanning for threats. **Excluded items will be scanned for exploits.**

SOPHOS

Here are the three main things you learned in this chapter.

The threat protection policy protects against malware, risky file types, websites, and malicious network traffic.

Some configuration features are not enabled by default.

You can exclude files, folders, websites, and applications from scanning for threats. Excluded items will be scanned for exploits.



Getting Started with the Sophos Central Peripheral Control Policy

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3515: Getting Started with the Sophos Central Peripheral Control Policy

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Peripheral Control Policy

In this chapter you will learn what the peripheral control policy is, what it does, and how it can be configured.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to manage protected devices
- ✓ What policies are and how they are assigned

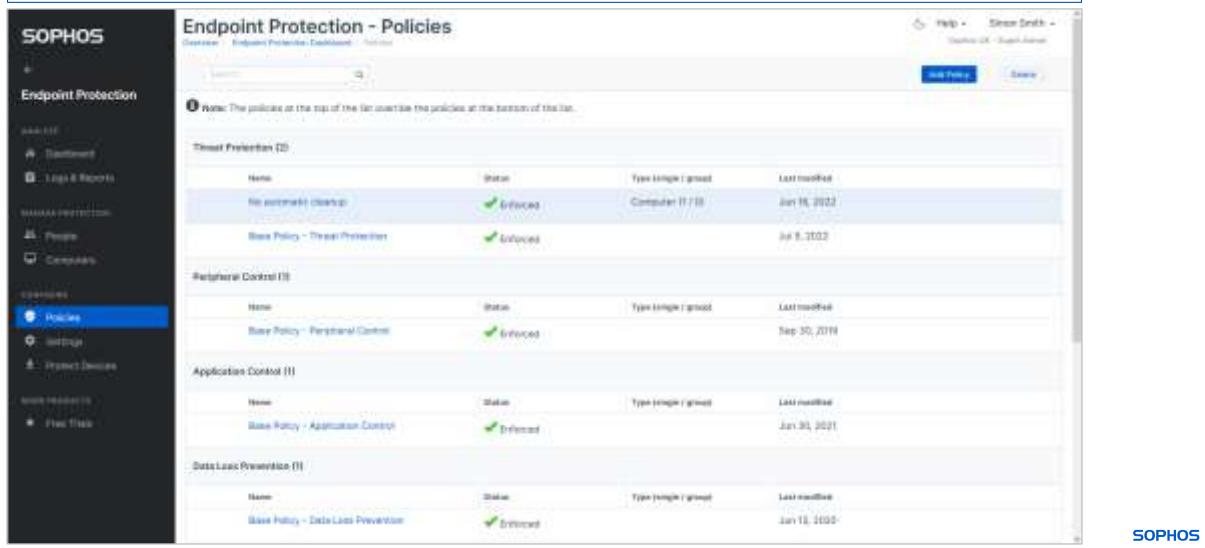
DURATION **4 minutes**

SOPHOS

In this chapter you will learn what the peripheral control policy is, what it does, and how it can be configured.

Peripheral Control

Restricts access to removable devices and can be used to prevent the use of untrusted devices which may contain malware



The screenshot shows the Sophos Central interface for managing Endpoint Protection Policies. The left sidebar has a dark theme with categories like Endpoint, Threat Protection, Devices, and Policies (which is selected). The main area is titled "Endpoint Protection - Policies". It displays four sections: Threat Protection (with one policy listed), Peripheral Control (with one policy listed), Application Control (with one policy listed), and Data Loss Prevention (with one policy listed). Each policy row includes columns for Name, Status (green checkmark), Type (single/group), and Last modified date.

Name	Status	Type (single/group)	Last modified
Re: peripheral (shared)	Enabled	Computer IT 718	Jan 18, 2023
Base Policy - Threat Protection	Enabled		Jan 8, 2023
Base Policy - Peripheral Control	Enabled		Sep 30, 2019
Base Policy - Application Control	Enabled		Jan 30, 2021
Base Policy - Data Loss Prevention	Enabled		Jan 18, 2023

Peripheral control restricts access to removable devices such as USB drives. It can be used to prevent the use of untrusted devices, which may contain malware.

Peripheral control is managed using the peripheral control policy. By default, the peripheral control policy is not configured.

Peripheral Control

The screenshot shows the Sophos Central interface for managing computer policies. On the left, a sidebar lists 'Endpoint Protection' under 'ANALYST' and 'POLICIES' (which is selected). The main area is titled 'Endpoint Protection - View Computer Policy' and shows the 'Peripheral Control' tab selected. A green callout box points to the 'Monitor but do not block' radio button under 'Manage Peripherals'. Below this, a table lists various peripheral types and their detection counts.

Peripheral Type	Detections
Bluetooth	0 detected
Barcode removable storage	0 detected
Floppy drive	8 detected
Infrared	0 detected
Modem	0 detected
Optical drive	16 detected
Removable storage	0 detected
Wireless	4 detected
WMPATH	5 detected

The management of peripheral devices is configured in the **SETTINGS** tab of the policy.

The option to ‘Monitor but do not block’ should be selected to allow all peripheral device use across the network. Any peripheral devices used will be detected and logged, collecting information about the devices in use. This allows you to make an informed decision regarding control.

Peripheral Control

The screenshot shows the Sophos Endpoint Protection interface under the 'Computer Policies' section. On the left, a sidebar lists 'Endpoint Protection', 'ANALYST', 'MANAGE FEDERATION', 'COMPLIANCE', and 'POLICIES'. The 'POLICIES' tab is selected. In the main area, the title is 'Endpoint Protection - View Computer Policy' with a subtitle 'Base Policy - Peripheral Control'. A sub-header 'Policy Level: Peripheral Control / User' is shown. Below this, tabs for 'USERS/COMPUTERS', 'GROUPS', 'SETTINGS' (which is selected), and 'POLICY ENFORCED' are visible. A green callout box highlights the 'SETTINGS' tab. The main content area is titled 'Manage Peripherals - set your peripheral settings below' and includes a note 'Monitor but do not block (all peripherals will be allowed)'. A link 'Get more info by peripheral type and add exemptions' is also present. A table lists peripheral types and their status: Allow (Bluetootch - 1 detected), Read-Only (Secure removable storage - 0 detected), Block (Floppy drive - 8 detected), Allow (Infrared - 0 detected), Allow (Modem - 0 detected), Allow (Optical drive - 10 detected), Allow (Removable storage - 0 detected), Allow (Wireless - 4 detected), and Block Bridged (WIFI - 5 detected). A blue bar at the bottom right of the screenshot says 'SOPHOS'.

Control peripheral device use on protected devices.

- Block
- Allow
- Read-only

When the peripheral control setting is change to 'control access', each category of device can be set to allow or block. Additionally, secure removable storage, floppy drives, and optical drives all have the option of read-only. For wireless devices, the option to block bridged network is available.

In this example, if a floppy drive is used on a protected device, the drive will be blocked based on this policy.

Peripheral Control

The screenshot shows the Sophos Central interface for Peripheral Control. On the left, a sidebar menu includes 'Endpoint Protection', 'Analytics', 'Manage Devices', 'Core Setup', and 'About Sophos'. Under 'Core Setup', 'Policies' is selected, highlighted in blue. Below the sidebar, there's a section for 'Desktop Messaging' with a toggle switch for enabling it. The main content area is titled 'Peripheral Exemptions' and contains a table with columns: PERIPHERAL, MODEL/ID, REFERENCE ID, POLICY, and INDEX BY. A green callout box points to the 'PERIPHERAL' column header with the text 'Exempt individual devices from the control settings'. An orange box highlights the 'Add Exemptions' button in the top right corner of the exemptions table. A note at the bottom of the exemptions table says, 'You do not have any exemptions. Use the "Add Exemptions" to start adding exemptions.' The Sophos logo is in the bottom right corner.

Exemptions can be made for individual devices. Any devices added to the exemption list are not subject to the control settings in the policy. This allows you to apply less restrictive controls for individual devices when required.

To add an exemption click **Add Exemptions**.

Peripheral Control

The screenshot shows the Sophos Central interface under the 'Peripheral Control' section. On the left, there's a sidebar with navigation options like 'Endpoint Protection', 'Compliance', 'Logs & Reports', 'Advanced Monitoring', 'People', 'Computers', 'Devices', 'Policies' (which is selected), 'Settings', 'Present Devices', 'Policy Resources', and 'Free Trials'. The main area is titled 'Add Peripheral Exemptions' and contains a table titled 'Detected Peripherals'. The table has columns for 'PERIPHERAL TYPE', 'NAME/ID', 'DESCRIPTION', and 'MODEL ID'. It lists several entries, including optical drives, a floppy disk drive, and a hard disk drive, all from 'AD\administrator' on 'VMware VMWare VMWare' with 'SATA' model IDs. A green callout box on the right states: 'All peripheral devices that have been detected are listed'.

PERIPHERAL TYPE	NAME/ID	DESCRIPTION	MODEL ID
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	SATA	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	CD/DVD	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	Optical Drive	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	Blu-ray Disc	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	Worm	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	MDF/UDF	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Optical drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	June 24, 2022 1:43 PM	SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Floppy drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	WHOLEDISK\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	FDC\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100
Floppy drive	AD\administrator\SCSI\IDE\VMware VMWare\VMware_SATA_C0000100	June 8, 2022 1:19 PM	FDC\SCSI\IDE\VMWARE\VMWARE_SATA_C0000100

This detected peripherals list shows all peripheral devices that have been detected on protected devices. This makes it easier to set consistent exemptions for all devices.

The list can be filtered by time or peripheral type.

Peripheral Control

The screenshot shows the Sophos Central interface for Peripheral Control. On the left, a sidebar lists navigation options: Endpoint Protection, Devices, Logs & Reports, Network Diagnostics, Peripherals, Computers, Dashboard, Policies (which is selected), Settings, Product Details, Help Resources, and Feedback. Below the sidebar, a message says "Desktop Messaging" with a toggle switch labeled "Enable Desktop Messaging for Peripheral Control". The main content area is titled "Add Peripheral Exemptions" and displays a table of "Detected Peripherals". The table has columns: PERIPHERAL TYPE & NAME, LAST SEEN, OWNER, MODEL, and ACTION(S). The data shows six entries for Floppy drives, all owned by Adam Jones, with the model listed as FDC(GENERIC,FLOPPY,D,16F). At the bottom right of the table are "Cancel" and "Add Exemption(s)" buttons.

PERIPHERAL TYPE & NAME	LAST SEEN	OWNER	MODEL	ACTION(S)
Floppy drive	John 8, 2022 5:10 PM	TRAINING-WDQuinn	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)
Floppy drive	Adam Jones	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)	
Floppy drive	Adam Jones	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)	
Floppy drive	John Smith	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)	
Floppy drive	Steve Smith	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)	
Floppy drive	Lucy Fox	Floppy disk drive	FDC(GENERIC,FLOPPY,D,16F)	

Select the device or devices you want to exempt from the control settings and click **Add Exemption(s)**.

Peripheral Control

The screenshot shows the Sophos Central interface for Peripheral Control. On the left, a sidebar menu includes 'Endpoint Protection', 'Analytics' (with 'Dashboard' and 'Logs & Reports'), 'Manage Permissions' (with 'People' and 'Connections'), 'Create Policy' (with 'Policy' selected), 'Settings', 'Protect Device', 'View Resources', and 'Free Trials'. The main area has a title 'Configure access by peripheral type and add exemptions'. It lists detected peripherals: Bluetoooth (0 detected), Secure removable storage (0 detected), Floppy drive (0 detected), Infrared (0 detected), Monitor (0 detected), Optical drive (0 detected), Removable storage (0 detected), Wireless (4 detected), and MTP/PTP (0 detected). Below this is a table titled 'Peripheral Exceptions'. A row for a 'Floppy drive' (Model ID: F0C1GENERIC_FLOPPY...) has its 'POLICY' set to 'Allow' and its 'ENFORCE BY' dropdown set to 'Model ID' (with 'Model ID' and 'Instance ID' options). A green callout box with a black border and white text states: 'Do not set a stricter access policy for an individual peripheral than for it's peripheral type'. The Sophos logo is in the bottom right corner.

In the 'Policy' column you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral. You should not set a stricter access policy for an individual peripheral than its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.

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).

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of the following best describes peripheral control?

Monitors and restricts file transfers containing sensitive data

Block specific applications from running on protected devices

Prevents the use of untrusted devices that may contain malware

Controls access to websites based on website category

SOPHOS



Question 2 of 3

Which option in the Peripheral Control policy should be selected if you want to **allow and log** the use of all peripheral devices across a network?

Disable peripheral control

Monitor but do not block

Control access by peripheral type

SOPHOS



Question 3 of 3

True or False: The Peripheral Control base policy is not configured by default.

True

False

SOPHOS

Chapter Review

Peripheral control **restricts access to removable devices** and can be used to prevent the use of untrusted devices which may contain malware.

Peripheral control is **managed using the peripheral control policy** which is **not configured by default**. The option to '**Monitor but do not block**' is useful to **allow and log** all peripheral device use across a network.

Exemptions can be configured for individual peripheral devices, any **exemptions are not subject to the control settings of the peripheral control policy**.

SOPHOS

Here are the three main things you learned in this chapter.

Peripheral control restricts access to removable devices and can be used to prevent the use of untrusted devices which may contain malware.

Peripheral control is managed using the Peripheral Control policy which is not configured by default. The option to 'Monitor but do not block' is useful to allow and log all peripheral device use across a network.

Exemptions can be configured for individual peripheral devices, any exemptions are not subject to the control settings of the peripheral control policy.



Getting Started with the Sophos Central Application Control Policy

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3520: Getting Started with the Sophos Central Application Control Policy

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Application Control Policy

In this chapter you will learn how to monitor applications used, and how to configure the application policy to control the use of applications.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to manage protected devices in Sophos Central
- ✓ How to assign base policies to users and groups

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how to monitor applications used, and how to configure the application policy to control the use of applications.

Application Control

Prevents users from running applications and improves security by controlling the types of applications that are allowed which reduces the possibility of exploit attacks.



The screenshot shows the Sophos Endpoint Protection - Policies interface. On the left, there's a navigation sidebar with options like Dashboard, Audit & Reports, People, Components, and Policies (which is selected). The main area is titled "Endpoint Protection - Policies" and contains four sections: Threat Protection (2), Peripheral Control (0), Application Control (0), and Data Loss Prevention (0). The Application Control section is highlighted with a red border. It lists two policies: "Ras Policy - Application Control" (Status: Enabled, Type: Computer / Group, Last modified: Jun 10, 2022) and "Ras Policy - Data Loss Prevention" (Status: Enabled, Type: Computer / Group, Last modified: Jun 15, 2022). The top right of the interface includes links for Help, Support Tickets, Sophos UK, Sophos Admin, and a "Add Policy" button.

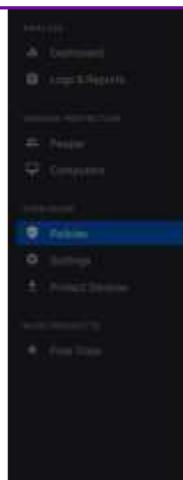
SOPHOS

Application control is used to prevent users from running applications that could be considered unsuitable for business use. For example, games or instant messaging applications. It also improves security by controlling the type of applications that are allowed which reduces the possibility for exploit attacks.

Application control is not enabled by default.

Application Control

Application List



A screenshot of the 'Add/Edit Application List' dialog box. At the top, it says 'Select Protection - View Computer Policy'. Below that is a search bar and a note: 'Search for an application... Supply names and update the list of applications you can select from.' The main area is a list of applications under the 'CATEGORY' 'System tool'. There are two checkboxes at the top of the list: 'SELECT ALL APPLICATIONS (SYSTEM TOOL)' (unchecked) and 'Microsoft Windows Contact Import Tool' (unchecked). To the right of the list are 'Cancel' and 'Save to List' buttons. A green callout box with a black border and white text says 'Select all applications included in the category'. Another green callout box with a black border and white text says 'Select individual applications'. A grey arrow points from the 'Save to List' button towards the bottom right of the dialog.

SOPHOS

Applications are controlled using the application control policy.

On the **SETTINGS** tab in the policy, select **Add/Edit List**. This opens a list of application categories. You can select an entire category or a single application within a category. This allows you to control all applications of a specific type, or control an individual application. A full list of the applications in a category will be displayed when you select an application category. In this example we have selected the 'System tool' category.

We recommend that you 'SELECT ALL APPLICATIONS' to begin with. You can refine your selection once you have detected the applications being used.

Click **Save to List** and repeat this process for each category you want to control.

Application Control

Application List



Sophos supplies and updates the list of applications you can select from.

CATEGORY	SELECTED / TOTAL	CONTROLS NEW APPS
Runtime Environment	0 / 9	<input type="checkbox"/> SELECT ALL APPLICATIONS (SYSTEM TOOL)
Screen capture tool	0 / 28	<input type="checkbox"/> Microsoft Network Speed Test
Screen saver Application	0 / 91	<input type="checkbox"/> Microsoft PowerShell
Security Tool	0 / 60	<input type="checkbox"/> Microsoft PowerShell ISE
Software Updater	0 / 22	<input type="checkbox"/> Microsoft Windows Camera App
System tool	0 / 240	<input type="checkbox"/> Microsoft Windows Contact Import Tool
Terminal client	0 / 7	<input type="checkbox"/> Microsoft Windows Contacts
Tethered connection tool	0 / 15	<input type="checkbox"/> Microsoft Windows Phone App
Toolbar	0 / 83	<input type="checkbox"/> Microsoft Windows Sticky Keys
WPS Office	0 / 100	<input type="checkbox"/> Microsoft WPS Office

Select to add new applications that are added to the category

SOPHOS

The option to include any new applications added to a category is available. This means that if an application is added to the category you have selected to control, it will also be controlled with the action specified.

Sophos supplies and maintains the list of applications and categories.

Application Control

The screenshot shows the Sophos Central application control policy configuration page. On the left, a sidebar lists navigation items: ANALYZE (Dashboard, Logs & Reports), MANAGE (Network, People, Connections), and CONFIGURE (Policies, Settings, Protect Device). The Policies item is selected and highlighted in blue. The main content area displays a table of detected applications:

Category	Count
Used connection tools	15 / 15
Used Program launcher	8 / 8
Virtualisation application	28 / 28
Voice over IP	42 / 42

Below the table, there is a section titled "Detection Options" with two toggle switches:

- Detect controlled applications when users access them (You will be notified)
- Allow the detected application
- Block the detected application
- Detect controlled applications during scheduled and on-demand scans

Further down, there is a note: "You can request applications to be added by Sophos: Application Control Request".

Under "Desktop Messaging", there is another toggle switch:

- Enable Desktop Messaging for Application Control

Instructions for configuring a message are provided: "Configure a message to be added to the end of the standard notification". A note at the bottom states: "Note: Custom messages will not be displayed for Intercept X events."

SOPHOS

We recommend that you detect the applications being used on your network first and then decide which applications you want to control access to.

Application Control

The screenshot shows the Sophos Central Application Control interface. On the left, a sidebar menu includes ANALYZE, MANAGE, and CONFIGURE sections. The CONFIGURE section is expanded, showing Policies (selected), Settings, Prevent Device, and Alert Requests. Under Policies, there are tabs for Application Control, Threat Protection, and Endpoint Protection. The Application Control tab is selected. The main content area displays 'Detect applications' statistics: 7 / 7 for Direct clients, 15 / 15 for Shared connection pool, 32 / 33 for Web Program launcher, and 0 / 0 for Virtualization application and Voice over IP. Below this is a 'Detection Options' section with three toggle switches:

- Detect controlled applications when users access them (You will be notified) (unchecked)
- Allow the detected application (selected)
- Detect controlled applications during scheduled and on-demand scans (unchecked)

A callout bubble points to the third option with the text: "Uses the scanning options set in the Threat Protection policy".

At the bottom of the interface, there is a note: "You can request applications to be added by Sophos: Application Control Request".

On the far right, the word "SOPHOS" is visible.

We recommend that you enable the 'detect controlled applications during scheduled and on-demand scans' option. This setting uses the scheduled scanning and on-demand scanning settings that have been applied in the threat protection policy.

Application Control

The screenshot shows the Sophos Central Application Control interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports' (which is selected and highlighted in blue), and 'People'. A large arrow points from the text 'Detect applications' towards this sidebar. The main content area is titled 'Logs' and contains a section titled 'General Logs'. Under 'General Logs', there are two items: 'Events' and 'Audit Logs'. The 'Events' item is highlighted with an orange border and described as 'Shows all security events, such as malware detections, on your devices and let you filter them to generate reports.' The 'Audit Logs' item is described as 'Record of all activities and changes made to the system.' At the bottom of the interface, a dark blue navigation bar shows the path 'Overview > Logs & Reports > Events'. In the bottom right corner, the word 'SOPHOS' is visible.

Detect applications

Logs

General Logs

Events
Shows all security events, such as malware detections, on your devices and let you filter them to generate reports.

Audit Logs
Record of all activities and changes made to the system.

Overview > Logs & Reports > Events

SOPHOS

Once all protected devices have completed at least one scan, you will have a list of all applications that are being used.

Navigate to **Overview > Logs & Reports > Events**.

Application Control

The screenshot shows the Sophos Central Application Control interface. On the left, a sidebar lists various security modules: Threat Analysis Center, Logs & Reports (selected), People, Devices, Global Settings, Third-party Connectors, Project Devices, and Robust Health Check. Below this is a section for IT PRODUCTS: Enterprise Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Host Threat. A large green arrow points from the text "View detected applications" to the main content area.

Events Report

Detect applications

Choose period: Outlast

From: Jul 4, 2022 To: Jul 8, 2022

Specify time range within past 30 days

Update

Show event types: Type ISB

Checked items are included in the event results:

- Type ISB
- Runtime Detections (0)
- Application Control (11)
- Malware (0)

Search by event source

Search by Computer or Device name

Search by Date range

View detected applications

Save as Custom Report Export

ID	Date	Source	User	Event Details	Device	Server
1	Jul 8, 2022 9:39:57 AM	Controlled application detected: Microsoft Word...	TRAININGDEMO\administrator		WinClient	IT-EU
2	Jul 8, 2022 9:31:48 AM	Controlled application detected: OneDrive (SkyO...	TRAININGDEMO\administrator		WinClient	IT-EU
3	Jul 8, 2022 9:31:33 AM	Controlled application detected: Microsoft You ...	TRAININGDEMO\administrator		WinClient	IT-EU
4	Jul 8, 2022 9:31:33 AM	Controlled application detected: Microsoft Skyp...	TRAININGDEMO\administrator		WinClient	IT-EU

Displaying 11 out of 98

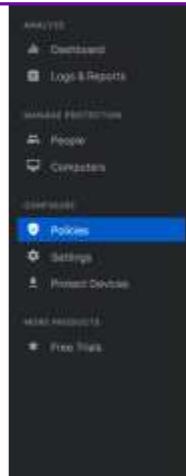
SOPHOS

In the list of event types, clear all the checkboxes except **Application Control**. Detected applications are shown in the list of events.

From here, you can make a note of any applications you want to continue using on the network. The report can be exported to excel and can be saved as a custom report if required.

Application Control

Controlling Applications



A screenshot of the Sophos Central 'Point Protection - View Computer Policy' page. The top navigation bar includes 'Help', 'Logout', 'Silvia Reith', 'Dashboard', and 'Super Admin'. Below the sidebar, the main content area has a title 'Point Protection - View Computer Policy' and a sub-section 'Application Control (true)'. It shows a table with one row: 'CONTROLLED APPLICATIONS' (1 / 240), 'SELECTED ITEMS' (Microsoft PowerShell), and 'CONTROLLED APPS' (empty). Below this is a 'Detection Options' section with three toggle switches: 'Detect controlled applications when users access them (You will be notified)', 'Allow the detected application', and 'Block the detected application' (which is highlighted with a red box). A green callout box points to this third option with the text 'Select to block controlled applications'. At the bottom, there's a note: 'You can request applications to be added by Sophos Application Control Request'.

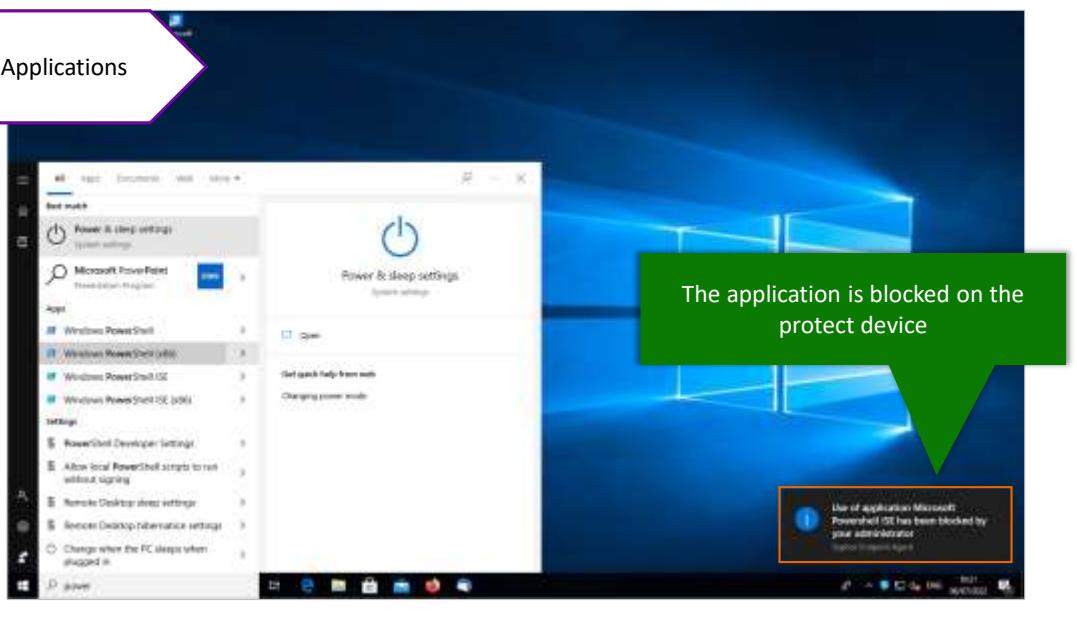
SOPHOS

Now that you have a list of applications being used, you can modify the application list in the application control policy to match your requirements.

In this example, only the PowerShell application is selected and the detection setting is changed to block the application.

Application Control

Controlling Applications



SOPHOS

On a protected device, when a user opens the blocked application, a message will appear advising that the application has been blocked.

Application Control

The screenshot shows the Sophos Central Application Control Requests interface. On the left, a sidebar menu includes 'Analytics', 'Dashboards', 'Logs & Reports', 'Manage Permissions', 'People', 'Connections', 'Core Setup', 'Policy' (which is selected), 'Settings', 'Protect Device', 'Alerts & Events', and 'Free Trials'. The main content area has a header 'Application Control / User' with tabs for 'COMPUTERS', 'GROUPS', 'SETTINGS' (which is selected), and 'POLICY ENFORCEMENT'. Below this, a table lists 'CONTROLLED APPLICATIONS' with 'SELECTED / TOTAL' showing 2 / 240. One row is highlighted: 'System tool'. Under 'DETECTION OPTIONS', there are two radio buttons: 'Allow the detected application' (selected) and 'Block the detected application'. A note states: 'You can request applications to be added by Sophos Application Control Request.' Under 'DESKTOP MESSAGING', there is a note: 'Enable Desktop Messaging for Application Control' with a checkbox, followed by a text input field and a note: 'Configure a message to be added to the end of the standard notification'. A note at the bottom says: 'Note: Custom messages will not be displayed for Intercept X events.' The bottom right corner features the 'SOPHOS' logo.

You can submit an application control request to Sophos if you want to control an application that isn't included in the current application list or if you believe an application is in the wrong category.

Click the **Application Control Request** link. A new tab will be opened, select **Application Control**. Fill in the details about the control request and submit it to Sophos.

Potentially Unwanted Applications

PUA

Not malicious but unsuitable for business networks

PUA detection

Enabled by default
Blocked and an event is logged

Scanning exclusions

Applications can be excluded globally or in specific policies

Add Exclusion

EXCLUSION TYPE: Potentially Unwanted Application (Windows/Mac)

VALUE*: PsExec

You can exclude PUAs by name (shown in the detection message and on our website), e.g. "PsExec" or "Cam'n Abel"

Cancel Add Another Add

SOPHOS

Potentially unwanted application (PUA) is a term used to describe applications that, while not malicious, are generally considered unsuitable for business use. The major PUA classifications are:

- Adware
- Non-malicious spyware
- Remote administration tools

Please note that certain applications that fall into the PUA category may be considered useful by some users.

PUA scanning is enabled by default. If a PUA is detected, it will be blocked, and an event logged. You can then configure either an exclusion for the application in **Global Settings** or in a specific policy to allow the PUA if it is required.

Potentially Unwanted Applications

Allowed Applications

The screenshot shows the 'Allowed Applications' section of the Sophos Central interface. On the left is a sidebar with 'Global Settings' selected. The main area displays two rows of allowed applications:

DATE	APPLICATION	NAME	DEVICE	ALLOWED BY	COMMENTS
Jul 8, 2022 10:50 AM	PsExec64.exe	TRAINING-WT07anner	Training-WT07	SHA-256: a9af00db398d4x7 e2fe0f9c1ccf2a10fd7968d8 7e05fb8d0de5c847a14ffaa4	
Oct 23, 2018 4:35 PM		Not applicable		Path: C:\users\vteskop\articulate	Articulate allowed

Global Settings > Allowed Applications

SOPHOS

Detected applications that are not controlled can be allowed. An application can be added to the global allowed applications list by navigating to **Global Settings > Allowed Applications**.

Click add apps by path and add the application you want to allow.

Potentially Unwanted Applications

Alternatively, applications can be allowed following a detection.

On the device **EVENTS** tab, the detection event for the application will be logged. Click **Details** to allow the application.

Potentially Unwanted Applications

Allowed Applications



SOPHOS

The event details display the detection data. You can allow the application by using the SHA-256, the certificate, or the file path.

You can also indicate why you want to allow the application and add any comments explaining why the application is being allowed.

Configure and Test Application Control



In this simulation you will clone the application control policy and configure the policy to block telnet clients. You will test the policy following configuration.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/TestAppControl/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/TestAppControl/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Which of the following statements best describes Application Control?

It can control access to websites based on the website category

It can block specific applications from running on protected devices

It can monitor and restrict file transfers containing sensitive data

It can prevent the use of removable media on protected devices

SOPHOS

Question 2 of 2

Which log displays any detected applications?

Chapter Review

Application control is used to **prevent users from running applications** that could be considered unsuitable for business use.

You can select an entire **application category** or a **single application** within a category. This allows you to control all applications of a specific type, or control an individual application.

We recommend that you **detect the applications being used** on your network **first**, and then decide which applications you want to control access to.

SOPHOS

Here are the three main things you learned in this chapter.

Application control is used to prevent users from running applications that could be considered unsuitable for business use

You can select an entire application category or a single application within a category. This allows you to control all applications of a specific type, or control an individual application.

We recommend that you detect the applications being used on your network first, and then decide which applications you want to control access to.



Getting Started with the Sophos Central Web Control Policy

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3525: Getting Started with the Sophos Central Web Control Policy

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Web Control Policy

In this chapter you will learn how website access can be controlled using the web control policy.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to manage devices in Sophos Central
- ✓ How to view, create and assign policies in Sophos Central

DURATION **10 minutes**

SOPHOS

In this chapter you will learn how website access can be controlled using the web control policy.

Web Control and Web Protection

Web Control

- Control website access based on website category
- Configured in the Web Control policy
- Specify an action for each website category (allow, warn, or block)
- Exceptions can be created via tags or category override

Web Protection

- Blocks access to malicious websites
- Configured in the Threat Protection policy
- IP and domain exclusions can be applied

SOPHOS

There are two types of protection for devices accessing Internet resources. These are web control and web protection.

Web control can allow, warn, or block websites based on their category and is configured in the web control policy whilst web protection blocks access to malicious websites. This setting is enabled by default and can be found in the threat protection policy.

This chapter focuses on web control.

Web Control

- Used to define which website categories can be accessed
- Control access to inappropriate websites
- Assists with compliance and liability coverage

The screenshot shows the Sophos Central web interface under the Endpoint Protection section. The left sidebar has a 'Policy' tab selected. The main area displays a table of policies across five categories: Application Control (1), Data Loss Prevention (1), Web Control (1), Update Management (1), and Windows Firewall (1). The 'Web Control (1)' row is highlighted with an orange border. The table columns include Name, Status, Type (single/group), and Last modified.

Name	Status	Type (single/group)	Last modified
Basic Policy - Firewall Central	Enabled	Type: single group	Jul 1, 2023
Basic Policy - Application Central	Enabled	Type: single group	Jul 1, 2023
Basic Policy - Data Loss Prevention	Enabled	Type: single group	Jul 1, 2023
Basic Policy - Web Control	Enabled	Type: single group	Jun 26, 2023
Basic Policy - Update Management	Enabled	Type: single group	Jun 26, 2023
Basic Policy - Windows Firewall	Enabled	Type: single group	Jun 26, 2023

SOPHOS

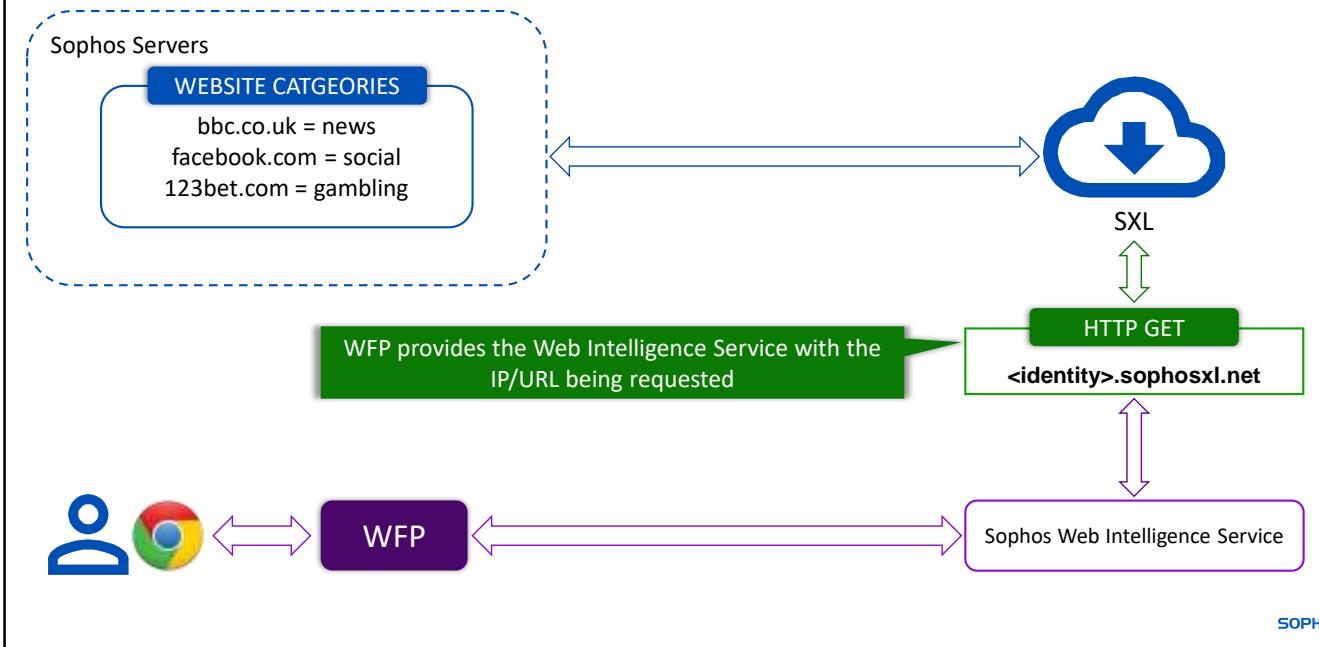
The web control policy is used to define which categories of websites can be accessed.

This allows you to control access to inappropriate websites and assists with compliance and liability coverage for inappropriate web browsing.



Additional information in
the notes

Web Control



Web control is one of several components that uses the Windows Filtering Platform (WFP) to integrate with networking applications such as Internet browsers.

Web control uses HTTP to contact the WFP, the information provided is used to perform SXL lookups to determine the category of a website. Web control utilizes Sophos Extensible List (SXL) lookups to provide the most up-to-date protection. The main purpose of SXL is to extend the protection offered on the endpoint by providing access to a wider amount of detection data and information when needed. It will allow lookups against live data using a checksum.

This diagram shows this in action:

1. Firstly, a user attempts to open a web page, in this example using the Chrome browser
2. WFP grabs the URL or IP address being requested
3. Finally, the Sophos Web Intelligence service performs the SXL lookup which checks the website category

[Additional Information]

A full list of SXL lookup types can be found in Knowledge base **KB-000034570**.

<https://support.sophos.com/support/s/article/KB-000034570>

Web Control

The screenshot shows the Sophos Central interface for creating a new policy named 'Base Policy - Web Control'. The policy type is set to 'Web Control'. The 'SETTINGS' tab is selected, showing several configuration options:

- Web Control:** A toggle switch is off, with a note: "Ignore the settings in this section of the policy. Note: If HTTPS decryption is turned on in the Threat Protection policy for a device, it will also be used for Web Control policy checks on the same device. You can exclude sites from decryption on the Settings page."
- Additional security options:** A toggle switch is on, with a dropdown menu set to "Let me specify". A callout box says: "Configure access to advertisements, uncategorized sites and risky downloads".
- Acceptable web usage:** A toggle switch is on, with a dropdown menu set to "Keep it clean". A callout box says: "Control the sites users are allowed to visit".
- Protect against data loss:** A toggle switch is on, with a dropdown menu set to "Allow data sharing". A callout box says: "Configure data loss settings".
- Log web control events:** A toggle switch is off.
- Control sites tagged in Website Management:** A toggle switch is off.

At the bottom, there is a note: "You have not added any website with filters. Click the Add New button to add a web filter." A green bar at the bottom right says "Add New".

The web control policy is split into sections;

- Additional security options. Configure access to advertisements, uncategorized sites and risky downloads
- Acceptable web usage controls the sites that users are allowed to visit
- Protect against data loss is used to configure data loss settings

Web Control

The screenshot displays the Sophos Central Web Control interface. It includes sections for 'Acceptable use', 'Protect against data loss', and 'Additional security options'. Each section has a dropdown menu with pre-configured settings like 'Block', 'Allow', or 'Let me specify'. A green callout box points to the 'Let me specify' option in the 'Acceptable use' dropdown, with the text 'Select from pre-configured settings'. Another green callout box points to the 'Let me specify' option in the 'Protect against data loss' dropdown, with the text 'Configure customized settings'. A third green callout box points to the 'View more' link in the 'Additional security options' section, with the text 'Configure the action to take for each website category'.

Select from pre-configured settings

Configure the action to take for each website category

Configure customized settings

SOPHOS

The settings are pre-configured, however, these can be changed to suit your requirements. To change the options select **Let me specify** from the drop-down menu in each section.

You can define the action to allow, warn, or block websites. Clicking the **View more** option will expand each section so you can view the website categories in more detail.

Web Control



- This setting enables the recording of any restricted website accessed by users
- It records any time a user proceeds past a warning message

SOPHOS

The option to log web control events is recommended. This setting will record any time a user browses to a site that has been blocked. It will also record any time a user browses to a site that has a warning control applied. This allows you to review the users that visit a warning category site, and more importantly when they proceed past the warning message to access the site.

Web Control

The screenshot shows the Sophos Central interface for managing web control policies. On the left, a sidebar lists 'Endpoint Protection' features like Firewall, Threat Protection, and Web Control. The 'Web Control' section is selected. The main pane displays the 'Web Control' policy settings. Under 'Additional security options', the 'Block adult content' rule is highlighted with a red box. A callout bubble from this rule points to a green box containing the text: 'Any website that is included in that category will be blocked based on the policy settings'. Another callout bubble from the 'Website Blocked' message points to a green box containing the text: 'Website category rules in the Web Control policy'. The 'Website Blocked' message shows a URL (www.bogusstores.com) and a link to 'Return to previous page'. The bottom right corner of the interface has the 'SOPHOS' logo.

When a web control policy is applied, all websites accessed will be checked to confirm the website category. This is then compared to the policy settings which will then either allow or block access to the site or warn the user about the site they are trying to access.

It is important to note that web control settings don't apply to websites you've excluded. When creating an exclusion for a website, create a policy exclusion in the threat protection policy.

Website Management

The screenshot shows the Sophos Central web interface. On the left is a dark sidebar with the Sophos logo and navigation links: Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings. The Global Settings link is highlighted with a blue bar at the bottom of the sidebar. The main content area has a white background with a grey header bar. The header bar contains the text "Global Settings > Website Management". Below the header, there are several sections: "General" (with "Synchronized Security" and "Tamper Protection" sub-sections), "Website Management" (which is highlighted with an orange border), and "Proxy Configuration". The "Website Management" section includes the sub-instruction "Manage, categorize, and tag websites for use with Web Control and Web Gateway features". At the bottom right of the main content area is the word "SOPHOS".

Global Settings > Website Management

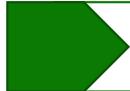
SOPHOS

Website management can be used to extend and customize website filtering.

Website Management

 Control websites not in one of the Sophos categories

 Tag websites to put them in group and use policies to control these website groups for specific users

 Override the Sophos category for a website. This changes the website's category for all users

SOPHOS

You can use website management 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

If you think Sophos has put a website in the wrong category, you can request that Sophos change the category. We recommend that you submit a change request rather than overriding the category.

Website Management

The screenshot shows the Sophos Central interface for managing web control policies. On the left, a dark sidebar lists 'Endpoint Protection' (Dashboard, Logs & Reports), 'Identity Protection' (People, Computers), 'Policies' (selected), 'Settings', 'Protect Devices', and 'Free Trials'. The main panel shows a policy named 'Base Policy - Web Control' with 'Web Control' enforced. It includes sections for 'Additional security options' (Block risky downloads, Acceptable web usage, Protect against data loss, Log web control events), and a 'Control sites tagged in Website Management' section where 'Company Media' is listed with an 'Allow' action. A green callout box points to this section with the text: 'Specify the action for website tags in the Web Control policy'.

You can create a tag for a website and specify the action for that website tag in the web control policy. This will allow access to the specific website whilst still blocking the category it belongs to.

Let's look at how this works.

Website Management

The screenshot shows the Sophos Central interface with the 'Website Management' page selected. The left sidebar has 'Global Settings' highlighted. The main area displays a list titled 'Website Management' with a note: 'To customize control for specific websites, add them to this list. Tag them to create groups of sites, like custom categories, that you can control in individual policies, or override the Sophos category for a site to change it for all your users!'. A search bar at the top says 'website'. Below it is a table with columns 'TAGGED' and 'CATEGORY'. A message in the center states 'You currently don't have any websites tagged.' At the bottom, it says '0 Websites Tagged / 0 Selected'. The Sophos logo is in the bottom right corner.

In this example, we are going to allow access to vimeo.com whilst blocking access to other streaming media category websites.

We start by adding the website to the website management list in Sophos Central. We add the website along with the override category, in this example, streaming media and then give the website a new tag. In this example 'Allowed company media'. It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.

Please note that entries in the website list can be single URLs, full domains, IP addresses, CIDR ranges, or even top level domains. Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.

Website Management

The screenshot shows the Sophos Central interface for managing website policies. On the left, a sidebar lists 'Endpoint Protection' features like Dashboard, Logs & Reports, People, Computers, and Policies. The 'Policies' option is selected and highlighted in blue. The main content area is titled 'Web Control' and contains several policy sections:

- Web Control**: A note states: "Enhance the settings in this section of the policy. Note: If HTTPS decryption is turned on in the Threat Protection policy for a device, it will also be used for Web Control policy checks on the same device. You can exclude sites from decryption on the Settings page."
- Additional security options**: Includes a dropdown for "Block risky downloads" with "View Details".
- Acceptable web usage**: A section titled "Let me specify..." with "Hide Details". It includes three categories:
 - Productivity-related categories**: Shows "Allow" with "View More".
 - Social Networking**: Shows "Allow" with "View More".
 - Adult and potentially inappropriate categories**: Shows "Block" with "View More".
- Categories likely to cause excessive bandwidth usage**: A table showing categories and actions:

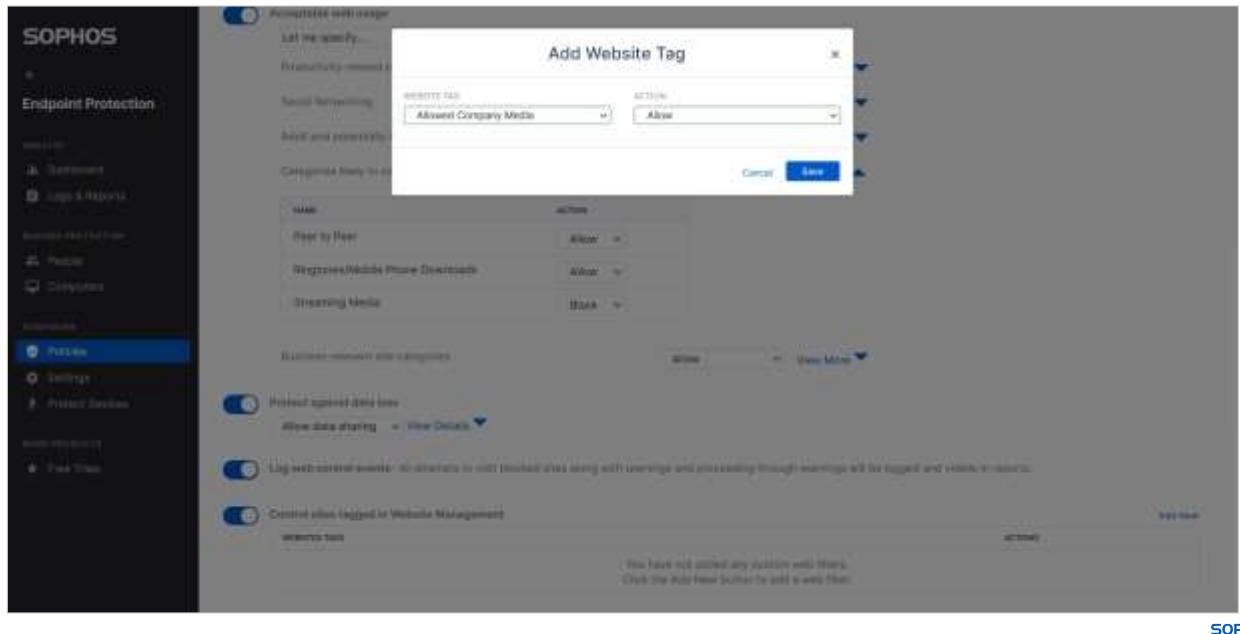
NAME	ACTION
Peer-to-Peer	Allow
Ringtones/Mobile Phone Downloads	Allow
Streaming Media	Block
- Business-related site categories**: Shows "Allow" with "View More".

SOPHOS

Add the website tag to the web control policy and set an action.

Here we will first set the action for the streaming media category to block.

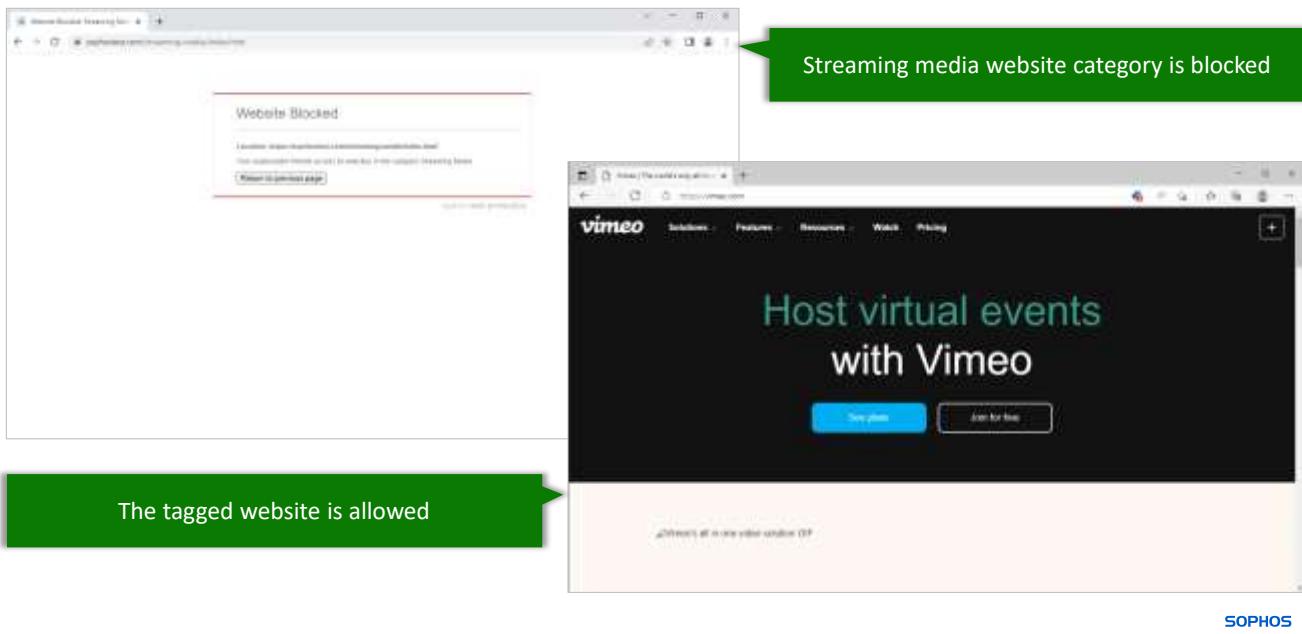
Website Management



In the 'Control sites tagged in Website Management' section, click **Add New** and select the 'WEBSITE TAG' you created from the drop-down menu and select an 'action'.

In this example, we set the action to **Allow**.

Website Management



Once the policy has been applied to a protected device, when the user browses to a website categorized as streaming media, the site is blocked. In this example we have used the sophostest.com site to test the policy.

When we browse to vimeo.com, the site is allowed. It maybe necessary to add multiple website entries to allow the full functionality of the website. In this example, the vimeo.com site does not display the full webpage correctly.

Website Management

The screenshot shows the Sophos Central interface. On the left, a sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under the Devices section, 'WinClient1' is selected. The main area is titled 'WinClient1' and shows the 'Events' tab selected. The interface includes a summary bar with tabs for SUMMARY, EVENTS (which is active), STATUS, and POLICIES. Below this is a search bar with filters for 'From' (May 21, 2022) and 'To' (Aug 10, 2022). A note says 'Display date range within last 90 days'. To the right is a 'View Events Report' link. The main content area displays a list of 967 events, each with a timestamp, event type (FW), and URL. Most URLs are from 'vimeocdn.com' and are blocked due to the 'Streaming Media' category. Other URLs include sophos.net, config.edgeskype.coex, vimeo.com, and yfrog.com.

NR	FWR	DATE	URL
1		Aug 10, 2022 1:48 PM	https://vimeocdn.com/appshell/marketing/_next/static/chunks/webpack-5ce0e592d29899ef7.js blocked due to category 'Streaming Media'
2		Aug 10, 2022 1:48 PM	https://i.vimeocdn.com/custom_asset/fbbde48e510ec8c3a437a3a35824d7ead blocked due to category 'Streaming Media'
3		Aug 10, 2022 1:48 PM	https://vimeo.com/ blocked due to category 'Streaming Media'
4		Aug 10, 2022 1:48 PM	https://sophos.net/com/streaming-media/index.html blocked due to category 'Streaming Media'
5		Aug 10, 2022 1:48 PM	https://config.edgeskype.coex/config/v1/Edge/0.0.1293.54 blocked due to category 'Streaming Media'
6		Aug 10, 2022 1:48 AM	https://config.edgeskype.coex/config/v1/Edge/0.0.1293.54 blocked due to category 'Streaming Media'
7		Aug 10, 2022 10:16 AM	https://console-events.vimeocdn.com/9d1/pageview blocked due to category 'Streaming Media'
8		Aug 10, 2022 8:41 AM	https://151.107.92.30/ blocked due to category 'Streaming Media'
9		Aug 10, 2022 8:40 AM	https://i.vimeocdn.com/custom_asset/fbbde48e510ec8c3a437a3a35824d7ead blocked due to category 'Streaming Media'
10		Aug 10, 2022 8:40 AM	https://151.107.92.30/ blocked due to category 'Streaming Media'
11		Aug 10, 2022 8:40 AM	https://vimeo.com/sophos blocked due to category 'Streaming Media'
12		Aug 10, 2022 8:27 AM	https://vt.google.com/vt/veppuqf130/%7B6A6B0345-D384-463C-AFF1-A68D9E530F96%7D%264=%10%2B1F236021-F1B2-98
13		Aug 10, 2022 8:28 AM	https://vt.google.com/generalm_204 blocked due to category 'Streaming Media'

In Sophos Central, locate the device and select the **EVENTS** tab. The block events will be displayed.

Website Management

The screenshot shows the Sophos Central interface for managing website policies. On the left, a sidebar menu includes options like Dashboard, Alerts, Threat Analytics, Logs & Reports, People, Devices (selected), Global Settings, Third-party Connectors, Protect Devices, Account Health Check, Reporting, Report Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and IPsec Threat.

The main area displays a summary of blocked events. A modal window titled "Events" is open, showing a list of 997 events from Aug 18, 2022, to Aug 19, 2022. The events list includes:

Date	Action	URL
Aug 18, 2022 1:49 PM	Blocked	https://www.vineco.com/custom_asset/fbd48e910ec8c8c437a3a95fc4d7ca0
Aug 18, 2022 1:49 PM	Blocked	https://vineco.com/
Aug 18, 2022 1:45 PM	Blocked	https://vineco.com/
Aug 18, 2022 1:43 PM	Blocked	https://sophos.net/streaming-media/index.htm
Aug 18, 2022 1:40 PM	Blocked	https://config.edge.skype.com/config/v1/Edge/704.0.1293.54
Aug 18, 2022 1:39 AM	Blocked	https://config.edge.skype.com/config/v1/Edge/704.0.1293.54
Aug 18, 2022 1:15 AM	Blocked	https://team1-events.vineco.com/vdl/pageview
Aug 18, 2022 8:41 AM	Blocked	https://v1.vineco.com/
Aug 18, 2022 8:40 AM	Blocked	https://vineco.com/customasset/fbd48e910ec8c8c437a3a95fc4d7ca0
Aug 18, 2022 8:40 AM	Blocked	https://v1.vineco.com/101.18.70.81
Aug 18, 2022 8:33 AM	Blocked	https://vineco.com/sophos
Aug 18, 2022 8:27 AM	Blocked	https://vt.google.com/vt/vepgui/100D%7B8A6BC945-D184-AF1-MEDRC30F9E%7D%26id%7B7BF236021-F102-9B
Aug 18, 2022 8:28 AM	Blocked	https://vt.google.com/generate_204

A context menu is open over one of the event entries, listing options such as "Open URL", "Open URL in New Tab", "Open URL in New Window", "Open URL in New Private Window", "Bookmark", "Save Log File", "Copy", "Copy URL", "Copy Selection", and "Search Google for 'https://vineco.com/'".

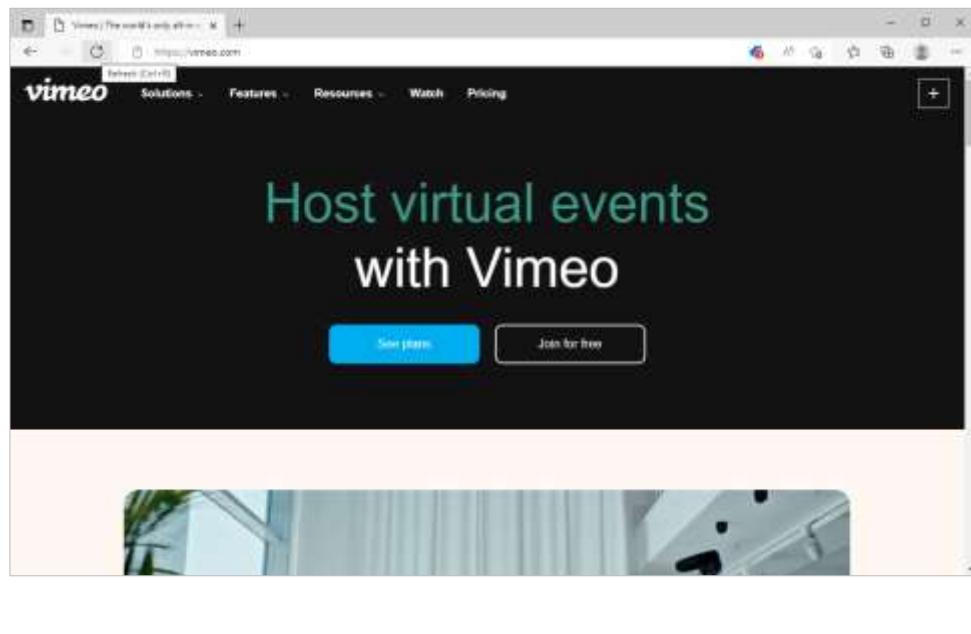
Select the website that is being blocked and copy it.

Website Management

The screenshot shows the Sophos Central interface with the 'Website Management' tab selected. A modal window titled 'Add Website Customization' is open. In the 'URL' field, the URL 'http://vimeo.com/expo100marketing/_next/static/chunks/welcomestatic/0228660f.js' is entered. The 'CATEGORY' dropdown is set to 'Streaming Media'. Below it, a 'SELECT THIS' dropdown has 'All' selected. A 'COMMENTS' field contains the text 'Allowed Company Media'. At the bottom right of the modal are 'Cancel' and 'Save' buttons.

Add the URL as a new website entry. Ensure you set the website tag as the same as the previous entry as this is already configured in the web control policy.

Website Management



SOPHOS

When you then refresh the website on the device, the page will load successfully.



Additional information in
the notes

SSL/TLS Decryption of HTTPS Websites

All websites must be encrypted (HTTPS) to be secure, Sophos can only scan the contents of a secure website if it can be decrypted first

With SSL/TLS decryption of HTTPS websites enabled, Sophos can intercept the connection from the Internet browser and inspect the inbound and outbound traffic which is monitored and protected

SSL/TLS decryption of HTTPS websites is not enabled by default. Either enable it in the Threat Protection policy or via Global Settings

Global Settings > SSL/TLS decryption of HTTPS websites

SOPHOS

In modern web browsers, all sites must be HTTPS encrypted to be secure. It is only possible to scan the contents of a secure website if it can be decrypted first. SSL/TLS decryption of HTTPS websites enables the scanning of IPv6 and HTTPS websites.

This works by intercepting the connection from an Internet browser and inspecting both the inbound and outbound traffic which is monitored and protected.

HTTPS websites will not be scanned by default, this feature must be enabled either in the threat protection policy or via **Global Settings > SSL/TLS decryption of HTTPS Websites**. When this setting is enabled, it will enable HTTPS decryption for web protection as well as web control.

[Additional Information]

Further information about this setting can be found in the help here:

<https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/GlobalSettings/DecryptHTTPS/index.html>

HTTPS Website Exclusions

The screenshot shows the Sophos Central interface under 'Global Settings'. A green callout box highlights the 'Categories excluded from HTTPS decryption' section, which lists several categories like Downloads, Firewall & Installation, Health & Maintenance, and Web Search & Content Filtering, each with a toggle switch set to 'On'. Below this is a table titled 'Websites excluded from HTTPS decryption' with one entry: 'www.sophos.com'. An orange border surrounds this table.

Decrypt SSL/TLS decryption of HTTPS websites for Windows computers in the 'New Endpoint Protection Features' Early Access Program.

Decrypt HTTPS websites using SSL/TLS (IEAP only)

Note: You can configure decryption of HTTPS websites for your other Windows computers and servers in the threat protection policy.

On this page, you can exclude sites or categories of sites from decryption.

Note: Exclusions prevent some checks by your policies. However, we'll still run any checks that don't need decryption.

Categories excluded from HTTPS decryption

Name	Status
Downloads	<input checked="" type="checkbox"/>
Firewall & Installation	<input checked="" type="checkbox"/>
Health & Maintenance	<input checked="" type="checkbox"/>
Web Search & Content Filtering	<input checked="" type="checkbox"/>
Web-based E-mail	<input checked="" type="checkbox"/>

Websites excluded from HTTPS decryption

Exclude	Comment	X
www.sophos.com		

Add exclusion

Websites that fail to load and websites that require client certificates will need to be excluded from HTTPS decryption. These websites and website categories can be excluded in the global setting.

You can add domain names, IP addresses, or IP address ranges to be excluded by clicking **Add Exclusion** at the bottom right. Categories set to allow in the web control policy will also be added to categories excluded from HTTPS decryption. By adding a website exclusion, all subdomains will also be excluded from HTTPS decryption.

Configure and Test a Web Control Policy



In this simulation you will configure and test a Web Control policy.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/TestWebControl/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/TestWebControl/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of the following statements best describes Website Management?

Controls when websites are decrypted before scanning

Used to extend and customize website filtering

Monitors inbound and outbound traffic

SOPHOS



Question 2 of 3

True or False: When enabled, the 'log web control events' setting will **only** record when a user browses to a site that has been blocked.

True

False

SOPHOS

Question 3 of 3

Match the feature to its description.

Web Protection

DROP

Allow, warn, or block websites based on the website category

Web Control

DROP

Blocks access to malicious websites

Chapter Review

Web control allows you to **control access to inappropriate websites** and assists with compliance and liability coverage for inappropriate web browsing.

The web control **policy is pre-configured**, however, the policy can be changed when required.

Web control settings **do not apply to excluded websites**.

SOPHOS

Here are the three main things you learned in this chapter.

Web control allows you to control access to inappropriate websites and assists with compliance and liability coverage for inappropriate web browsing.

The web control policy settings are pre-configured and can be changed to suit your requirements. To change the options select **Let me specify** from the drop-down menu in each section.

Web control settings do not apply to excluded websites.



Getting Started with the Sophos Central Data Loss Prevention Policy

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3535: Getting Started with the Sophos Central Data Loss Prevention Policy

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with the Sophos Central Data Loss Prevention Policy

In this chapter you will learn how Sophos Central helps to protect against data loss. You will learn how to apply content control lists, rules, and pre-configured templates in the data loss prevention policy.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to manage protected devices
- ✓ How to manage Sophos Central policies

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how Sophos Central helps to protect against data loss. You will learn how to apply content control lists, rules, and pre-configured templates in the data loss prevention policy.



Additional information in
the notes

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) controls accidental data loss by restricting what type of data and file types can be transferred inside and out of an organization

Content Control Lists (CCL)

- Define content to be matched
- Use Sophos defined CCLs or custom CCLs

Rules

- **File** rule: match against a file name or file type
- **Content** rule: match against a CCL

Destination

- Removable storage devices
- Applications, Internet browsers, email clients etc.

Action

- Allow or block transfer
- Allow transfer if user confirms

SOPHOS

Data loss prevention (DLP) controls accidental data loss by restricting what type of data and file types can be transferred inside and outside of an organization. For example, preventing a user sending sensitive data outside of an organization.

DLP achieves this by using Content Control Lists (CCLs) which are a set of conditions that describe file content. File and content rules can be used in a Content Control List to determine what type of data can be transferred. These are applied to protected devices through the DLP policy.

DLP allows you to specify how sensitive data can be transferred and what action to take if the rule is violated. Please note that DLP will not work with encrypted data unless the application process is trusted by the encryption software to give visibility.

[Additional Information]

For more information about the limitations of DLP, see Knowledge base article **KB-000033860**.

<https://support.sophos.com/support/s/article/KB-000033860>

Content Control Lists (CCLs)

Global Settings > Content Control Lists

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item highlighted. The 'Content Control Lists' section is outlined with a red border. A green callout box points to this section with the text: 'View pre-defined CCLs and create or import your own'.

SOPHOS
Sophos Central
Dashboard
Alerts
Threat Analysis Center
Logs & Reports
People
Devices
Global Settings (highlighted)
Third-party Connectors
Protect Devices

HTTPS Updating
Manage whether updating is performed using the secure HTTPS protocol.

Configure email alerts
Manage email alerts for admins.

Encryption Recovery Key Search
Get a device encryption recovery key by entering a volume or recovery identifier.

Admin Isolated Devices
See which devices you've isolated and remove them from isolation.

Forensic Snapshots
Configure forensic snapshots, which get data to help you investigate potential threats.

Malware Sample Submission
Configure uploading malware sample submissions to Sophos.

Data Loss Prevention
Rules
Create rules to reuse across multiple policies.

Content Control Lists
Create content control lists to reuse across multiple policies. (outlined with red border)

User Access
Manage users' access to Sophos Central Self Service.

SOPHOS

A Content Control List can describe a single type of data, for example, a postal address or a social security number. Alternatively, it can contain a combination of data types.

SophosLabs provides a set of Content Control List definitions for common financial and personally identifiable data types, for example, credit card numbers or email addresses. Advanced techniques, such as checksums, are used in SophosLabs CCLs to increase the accuracy of sensitive data detection.

Content Control Lists can be found by navigating to **Global Settings > Content Control Lists**.

Content Control Lists (CCLs)

The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected. The main content area is titled 'Manage Content Control Lists' and displays a table of existing CCLs. A tooltip is visible over the entry for 'Bank account details [Australia]', providing a detailed description of the list's purpose and content.

Name	Region	Source	Action
Ailment, disease and diagnosis phrases [global]	Global, USA	SophosLabs	
Bank account details [Australia]	Australia	SophosLabs	
Bank account details [Brazil]	Brazil	SophosLabs	
Bank account details [Canada]	Canada	SophosLabs	
Bank account details [Denmark]	Denmark	SophosLabs	
Bank account details [France]	France	SophosLabs	
Bank account details [Germany]	Germany	SophosLabs	
Bank account details [Iceland]	Iceland	SophosLabs	
Bank account details [Hong Kong]	Hong Kong	SophosLabs	

SOPHOS

The CCLs defined by SophosLabs cannot be edited, however, you can submit a request to Sophos for a new CCL or to provide feedback on existing CCLs.

To view a description of each list, hover over the information icon. The Content Control List can be filtered by region, source, or type.

You can add your own Content Control List by creating a new custom list or by importing a list.

Rules

The screenshot shows the Sophos Central Global Settings interface with the 'Rules' section selected. The left sidebar has 'Global Settings' highlighted. The main area displays 'Manage Data Loss Prevention Rules' with two sections: 'FILE rule' (highlighted with a green box) and 'CONTENT rule' (highlighted with a green box). The 'FILE rule' section shows a table with columns 'Source', 'Type', 'Action', and 'Target'. The 'CONTENT rule' section also shows a similar table.

FILE rule
Controls the transfer of file types or file names

CONTENT rule
Controls the transfer of types of content

Rules are used to define the action taken if a user interacts with a specific data type. Rules can be added and managed via **Global Settings > Rules**.

A content rule is a rule that controls the transfer of certain types of data whereas a file rule controls the transfer of certain file types or file names.

Rules can also be added when a custom CCL is created and when a DLP policy is configured.

Data Loss Prevention Policy

The screenshot shows the Sophos Central interface for managing computer policies. On the left, a sidebar menu under 'Endpoint Protection' includes 'Dashboard', 'Logs & Reports', 'Manage Permissions', 'Code Work', and 'Policies'. The 'Policies' item is highlighted with a blue box. The main content area is titled 'Endpoint Protection - View Computer Policy' and shows a 'Base Policy - Data Loss Prevention' page. At the top right, there are buttons for 'Save', 'Cancel', 'Close', and 'Delete'. A status bar at the bottom right indicates 'Last Updated: Jun 13, 2020'. The central part of the screen displays the 'Data Loss Prevention / User' tab, which is selected. It contains several tabs: 'USERS/COMPUTERS' (selected), 'GROUPS', 'SETTINGS' (with a checked 'POLICY ENFORCED' checkbox), and 'POLICY FROM SOPHOS TEMPLATE'. A green callout box points to the 'SETTINGS' tab with the text 'Enable the use of rules for data transfers'. To the right, there's a 'Create Custom Policy' section with a 'Create Custom Policy' button.

Enable the use of rules for data transfers

Endpoint Protection > Policies > Data Loss Prevention

SOPHOS

The Data Loss Prevention policy uses CCLs, content, and file rules to define a set of conditions that specify what data is allowed to be transferred both internally and outside of an organization.

The DLP policy is not enabled by default, enable the 'Use rules for data transfers' option to start configuring the policy.

Data Loss Prevention Policy

The screenshot shows the Sophos Endpoint Protection interface for viewing a computer policy. On the left, there's a sidebar with 'Endpoint Protection' selected. The main area is titled 'Endpoint Protection - View Computer Policy' and shows a 'Policy Rules' section. It has two main options: 'Create Policy from Sophos Template' (using standard templates like 'Europe') and 'Create Custom Policy' (using configurable file and/or content rules). A green callout box labeled 'Make use of Sophos templates' points to the first option, and another green callout box labeled 'Create a custom policy' points to the second. A blue bar at the bottom states 'Content and file rules can be used in multiple policies'. The bottom right corner has the 'SOPHOS' logo.

When you enable the use of rules for data transfers you can either select from the existing Sophos templates that cover standard data protection for organization activities across multiple regions, or you can select to create a custom policy. This is useful if you have specific requirements.

DLP policies can include one or more rules that specify matching conditions and actions when a rule is matched. When a DLP policy contains several rules, a file that matches any of the rules configured will violate the policy.

Content and file rules can be used in multiple policies.

Creating a Policy from a Sophos Template

The screenshot shows the Sophos Endpoint Protection interface. On the left, a sidebar menu includes 'Endpoint Protection', 'Analytics', 'Manage Protection', 'Cloud Work', and 'Help'. Under 'Cloud Work', 'Policies' is selected and highlighted in blue. The main content area is titled 'Endpoint Protection - View Computer Policy' and shows a 'Base Policy - Data Loss Prevention' page. At the top right, there are buttons for 'Save', 'Cancel', 'Close', and 'Issue'. Below these are tabs for 'USERS/COMPUTERS', 'GROUPS', 'SETTINGS', and 'POLICY ENFORCER'. A green callout box points to the 'Create from Template' button, which is located in the 'Create Policy from Sophos Template' section. This section also includes a note about using templates for standard data protection rules and dropdown menus for 'Region' (set to 'UK') and 'Template' (set to 'General organization activities (UK)'). Another green callout box points to these dropdown menus. To the right, there is a 'Create Custom Policy' section with a 'Create Custom Policy' button.

Select the region from the first drop-down menu and then select the available template from the second drop-down menu.

Click **Create from Template** to configure the DLP policy.

Creating a Policy from a Sophos Template

The rules are automatically applied in the template

SOPHOS

Endpoint Protection

Analyze

Logs & Reports

Manage Permissions

People

Computers

Code Work

Policies

Settings

Project Details

Help & Support

Free Trials

Data Loss Prevention - User

LAST UPDATED: Jun 18, 2020

SETTINGS POLICY ENFORCED

Use rules for data transfers

DESCRIPTION

Rules

General organisation activities [UK] - Bank account details [UK] - 1 ⓘ

General organisation activities [UK] - Personal sensitive data [UK] - 1 ⓘ

General organisation activities [UK] - Person identification numbers [UK] - 1 ⓘ

General organisation activities [UK] - Continuation of contact details [UK] - 1 ⓘ

General organisation activities [UK] - Person or banking identifiers with contact details [UK] - 1 ⓘ

General organisation activities [UK] - Restricted information [UK] - 1 ⓘ

Messages For End Users

Message when the file transfer needs to be confirmed by the user

Message when the file transfer is blocked

SOPHOS

The rules listed are automatically applied as part of the selected template.

Creating a Policy from a Sophos Template

The screenshot shows the Sophos Endpoint Protection interface. On the left, a sidebar menu includes 'Endpoint Protection', 'Analytics', 'Manage Protection', 'Data Loss', and 'Help & Support'. The 'Data Loss' section is currently selected. The main panel displays a 'Data Loss Prevention - Local' configuration page. At the top, there are tabs for 'USERS/COMPUTERS', 'GROUPS', 'SETTINGS' (which is selected), and 'POLICY ENFORCEMENT'. A toggle switch is set to 'Use rules for data transfers'. Below this, a 'DESCRIPTION' field is empty. A green callout box with the text 'Add additional rules if required' points to a 'Add' button in a dropdown menu. The dropdown menu also lists 'Add Existing Rule', 'New Content Rule', and 'New File Rule'. The 'Rules' section lists several items under 'General organization activities [UK]': 'Bank account details [UK] - 1', 'Personal sensitive data [UK] - 1', 'Person identification numbers [UK] - 1', 'Contact details [UK] - 1', 'Person or banking identifiers with contact details [UK] - 1', and 'Restricted information [UK] - 1'. The 'Messages For End Users' section contains two options: 'Message when the file transfer needs to be confirmed by the user' and 'Message when the file transfer is blocked'.

To add additional rules, you can select an existing rule that you have already configured or select to create a new content or file rule.

Creating a Policy from a Sophos Template

The screenshot shows the Sophos Endpoint Protection interface. On the left, a sidebar menu includes 'Endpoint Protection', 'Analytics', 'Logs & Reports', 'Manage Permissions', 'Code Work', 'Policies' (which is selected), 'Settings', 'Protect Devices', and 'Help & Support'. The main panel displays a list of rules under the 'Rules' section, such as 'General organisation activities (UK) - Bank account details (UK) - 1' and 'General organisation activities (UK) - Continuation of contact details (UK) - 1'. Below the rules, there are sections for 'Messages For End Users' containing two options: 'You must confirm that you want to send this message.' and 'This message has been blocked by the IT Department for your security.' A green callout box points to the second message option with the text 'Edit the message for end users'.

You can add text to the message shown on protected devices when a rule is triggered. This will either be a confirmation or a block notification depending on the action configured in the rule.

Click on the link to configure the messages.

Creating a Policy from a Sophos Template

The screenshot shows the Sophos Endpoint Protection interface. On the left, a sidebar menu includes 'Endpoint Protection' (selected), 'Analytics' (Dashboard, Logs & Reports), 'Manage Protection' (People, Computers), 'Data Loss' (Policy selected, Settings, Protect Devices), and 'Helpdesk' (Free Trial). The main content area is titled 'Endpoint Protection - View Computer Policy' under 'Computer Policies'. It shows a 'Base Policy - Data Loss Prevention' for 'User' level. The 'SETTINGS' tab is selected. A toggle switch is set to 'On' with the label 'Use rules for data transfers'. Below this, there are two message sections: 'FILE TRANSFER CONFIRMATION MESSAGE' containing 'You must confirm that you want to send this message.' and 'FILE TRANSFER BLOCK MESSAGE' containing 'This message has been blocked by the IT Department for your security.' Both messages have character count indicators (52/100 and 89/100) and a 'Finish' button at the bottom right.

You can edit the messages to your requirements.

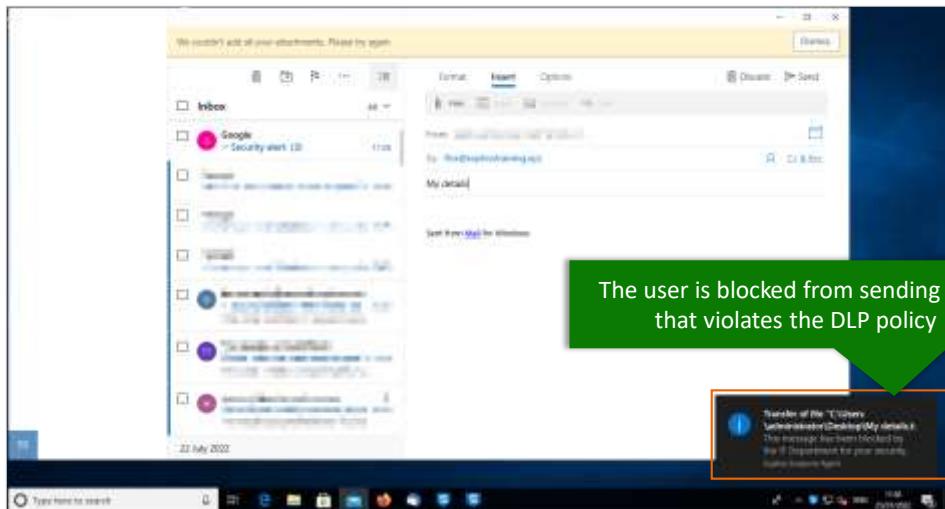
Click **Finish** to return to the DLP SETTINGS page.

Creating a Policy from a Sophos Template

The screenshot shows the Sophos Endpoint Protection interface. On the left, a sidebar menu includes 'Endpoint Protection' (selected), 'Analytics' (Dashboard, Logs & Reports), 'Manage Protection' (People, Computers), 'Cloud Work' (selected, Policies, Settings, Protect Devices), and 'Help & Tools' (Free Trials). The main content area is titled 'Endpoint Protection - View Computer Policy' under 'Data Loss Prevention - Base Policy - Data Loss Prevention'. It shows a 'DESCRIPTION' field and a 'Rules' section listing various data categories. A green callout box in the top right corner contains the text: 'Always remember to save any changes you make to policies'.

Your DLP policy is now fully configured.

Creating a Policy from a Sophos Template



DLP focuses on preventing inappropriate email attachments and file uploads. It does not scan the body of email messages

SOPHOS

When a user attempts to transfer a file that violates the configured policy, the transfer will be blocked or the user will be prompted to confirm the transfer depending on the configuration of the policy.

Please note that for performance reasons, DLP focuses on preventing inappropriate email attachments and file uploads. It does not scan the body of an email message

Configure and Test a Data Loss Prevention Policy



In this simulation you will configure a Data Loss Prevention policy and then test it.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/DLP/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/DLP/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

A user has included confidential data in an email and sent it. The email was not blocked by the DLP policy.
Why was the data not detected by the DLP policy?

The user was not included in
the policy

The user was using an
unsupported email client

The policy did not include a
scan email rule

DLP cannot scan the body of
the email

SOPHOS



Question 2 of 3

True or False: The CCLs defined by SophosLabs cannot be edited.

True

False

SOPHOS

Question 3 of 3

Match the rule type with the correct description.

Content Rule

DROP

Controls the transfer of file types or names

File Rule

DROP

Controls the transfer of types of data

Chapter Review

Data Loss Prevention (DLP) controls accidental data loss by **restricting what type of data and file types can be transferred**. The DLP policy is **not enabled by default**.

A **Content Control List** (CCL) can **describe a single type of data or a combination of data types**. **Rules** are used to **define the action taken** if a user interacts with a specific data type.

The **Data Loss Prevention policy** uses CCLs, content and file rules to **define a set of conditions that specify what data is allowed to be transferred** both internally and externally.

SOPHOS

Here are the three main things you learned in this chapter.

Data Loss prevention controls accidental data loss by restricting what type of data and file types can be transferred. The DLP policy is not enabled by default.

A Content Control List can describe a single type of data or a combination of data types. Rules are used to define the action taken if a user interacts with a specific data type.

The Data Loss Prevention policy uses CCLs, content and file rules to define a set of conditions that specify what data is allowed to be transferred both internally and externally.



Getting Started with Sophos Central Exclusions

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3545: Getting Started with Sophos Central Central Exclusions

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Exclusions

In this chapter you will learn what types of exclusions can be applied, when to apply them, and recommendations for best practice when applying exclusions.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to manage protected devices
- ✓ How to create and apply policies

DURATION **12 minutes**

SOPHOS

In this chapter you will learn what types of exclusions can be applied, when to apply them, and recommendations for best practice when applying exclusions.

Exclusions

Exclusions can be used to customize the detection behaviour of Sophos Central.

The screenshot shows the Sophos Central web interface. On the left, a sidebar menu includes 'Endpoint Protection' (selected), 'ANALYSES', 'MANAGE PROTECTION', and 'CONFIGURE' (selected). Under 'CONFIGURE', 'Policies' is highlighted. The main content area has a purple header 'GLOBAL EXCLUSIONS' with the subtext 'Apply to all protected devices and users' and 'Configured in Global Settings'. Below this is a table for 'Global Exclusions' with one entry: 'EXCLUDES' for 'Direction: Inbound Connection, Local Port: 3389' with 'ACTIVE FOR Computer Isolation (Windows)'. A green header 'POLICY EXCLUSIONS' with the subtext 'Applied to specific users, devices, servers or groups' and 'Configured in a Policy' follows. Below this is a table for 'Policy Exclusions' with one entry: 'EXCLUDES' for 'C:\myapplication\application' with 'ACTIVE FOR Real-time and scheduled'.

GLOBAL EXCLUSIONS
Apply to all protected devices and users
Configured in **Global Settings**

POLICY EXCLUSIONS
Applied to specific users, devices, servers or groups
Configured in a **Policy**

Sometimes it may be necessary to customize the operation of the protection policies and global settings by defining items for which the standard policy behaviour should be overridden. For example, you may want to exclude an application that is incorrectly detected as a threat until the issue has been resolved.

Global settings apply to all devices and users and allow the configuration of scanning and exploit mitigation exclusions, website management, and allowed applications.

To apply exclusions to specific devices, groups, or servers, use policy exclusions instead.

Exclusion Types

- Exclude items from being scanned for **threats**
 - Files and Folders
- Use exclusions to allow isolated devices to communicate with devices with restrictions
 - Windows processes
 - Websites
 - Applications
 - Previously detected malicious behaviour exploits
 - Folders and applications from ransomware protection

Excluded files and folders will still be scanned for **exploits**

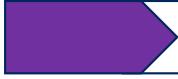
SOPHOS

There are several exclusion types that can be configured. You can exclude:

- Files or folders. Please note that excluded files and folders will still be scanned for exploits
- Windows processes
- Websites
- Applications
- Previously detected malicious behaviour exploits
- Folders or applications from ransomware protection

You can also use exclusions to allow isolated devices to communicate with other devices under restrictions. Please note that this option requires an Intercept X Advanced with XDR license.

Exclusions Use Cases

-  Vendor-recommended exclusions
-  Non-malicious applications behave in a way that is detected as malicious
-  SophosLabs verify the file/application is clean
-  Organization confirm they are happy it is safe to add the exclusion

SOPHOS

A common reason for excluding files and folders from anti-virus scanning is because vendors recommend exclusions to ensure their applications operate successfully.

Sometimes a non-malicious application behaves in a way that is detected as malicious by Sophos. Careful consideration should be given to excluding applications of this nature as they allow behaviour which is commonly considered harmful. Before adding an exclusion, the question should always be ‘why are these files doing this?’ And, ‘Is this the type of behaviour I want in my environment?’

It is important that you do not configure exclusions unless:

- The file or application has been confirmed as clean by SophosLabs
- The organization has confirmed that they are happy it is safe and can be excluded

Exclusion Investigation

CLEAN INDICATORS

- Known files that belong to a legitimate application
- Executable files that have a name relevant to the location/application they have been detected in
- A file which has been on the device for a long period of time
- During the installation of new software
- If no other anti-virus vendor is detecting the file as malicious

MALICIOUS INDICATORS

- An unknown file, possibly with a random name
- An executable file in a temp/user data location
- Detection of a file which was created at the time of the detection or shortly before
- Other recent detections on the same device
- If the file is detected by other anti-virus vendors

SOPHOS

Before adding an exclusion or allowing an application, you must ensure that the files being detected are part of a legitimate application. It is important to treat every detection as malicious and not authorize anything unless you are confident it is safe to exclude.

A few examples of clean and malicious file indicators are shown here.

Applying Exclusions

Ensure all exclusions are specific

Use policies to apply exclusions to target specific users or devices

Check all exclusions regularly

Remove any unnecessary exclusions

Exclusions may significantly reduce your protection - only use them if you understand the risks

SOPHOS

It is really important to be careful when adding any exclusions to a threat protection policy or globally as they can reduce your protection.

Here are a few guidelines for applying exclusions safely.

Firstly, make sure that any exclusions added are as specific as possible. Generalized exclusions may cover more files or folders than required. We recommend that you use policies to apply exclusions that target only specific users or devices.

Check all of the exclusions regularly to ensure that all exclusions applied are required. You may no longer need an exclusion that was applied to fix a specific issue or to comply with a vendor recommendation.

Lastly, remove any unnecessary exclusions.



Additional information in
the notes

Global Exclusions

The screenshot shows the Sophos Central interface with the 'Global Settings > Global Exclusions' path selected. A modal window titled 'Add Exclusion' is open, displaying a dropdown menu for 'EXCLUSION TYPE' with options like 'File or Folder (Windows)', 'File or Folder (Mac/MacOS)', 'File or Folder (Sophos Security VM)', 'Process (Windows)', 'Website (Windows/Mac)', 'Potentially Unwanted Application (Windows/Mac)', 'Deferred Deploy (Windows/Mac)', 'Kaspersky Protection (Windows)', 'Driver Assistant (Windows)', 'Endpoint Manager (Windows)', 'AMM3 Protection (Windows)', 'Microsoft Network Traffic Protection (DPS) (Windows)', and 'Handling packages (Windows)'.

Exclusion Examples

File or Folder (Windows):
C:\ProgramData\adobe\photoshop\

Process (Windows):
%PROGRAMFILES%\Microsoft\Office\Outlook.exe

Website:
192.168.0.0/24 google.com

Global Settings > Global Exclusions

SOPHOS

Global exclusions can be used to exclude files, websites, and applications from scanning for threats. Navigate to **Global Settings > Global Exclusions** to view existing exclusions and add new exclusions.

Global exclusions will apply to all users, devices, and servers.

[Additional Information]

For more information see the scanning exclusions here:

<https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/GlobalSettings/GlobalExclusions/index.html>



Additional information in
the notes

Setting Up Specific Exclusions

Example specific exclusion for app.exe

NOT: *.exe

USE: C:\Program Files\Software\app.exe

These folders are **not** recommended as an exclusion:

C:\Windows\

C:\ProgramData\

C:\Users\<Username>\

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\

SOPHOS

We recommend the use of specific exclusions. For example, if you needed to exclude an executable that exists in a software folder on the C drive in Program Files, an exclusion of *.exe would exclude the executable, however, it would also exclude ALL executables. This means that any malicious executable file will not be scanned or blocked. To make the exclusion specific, use the full path for the executable application.

We also recommend that you do not exclude folders where malware is most often located. For example, the Windows directory, ProgramData, Users and Startup.

[Additional Information]

An example of an exclusion. Instead of *.exe use C:\Program Files\Software\app.exe

Locations where malware is often found:

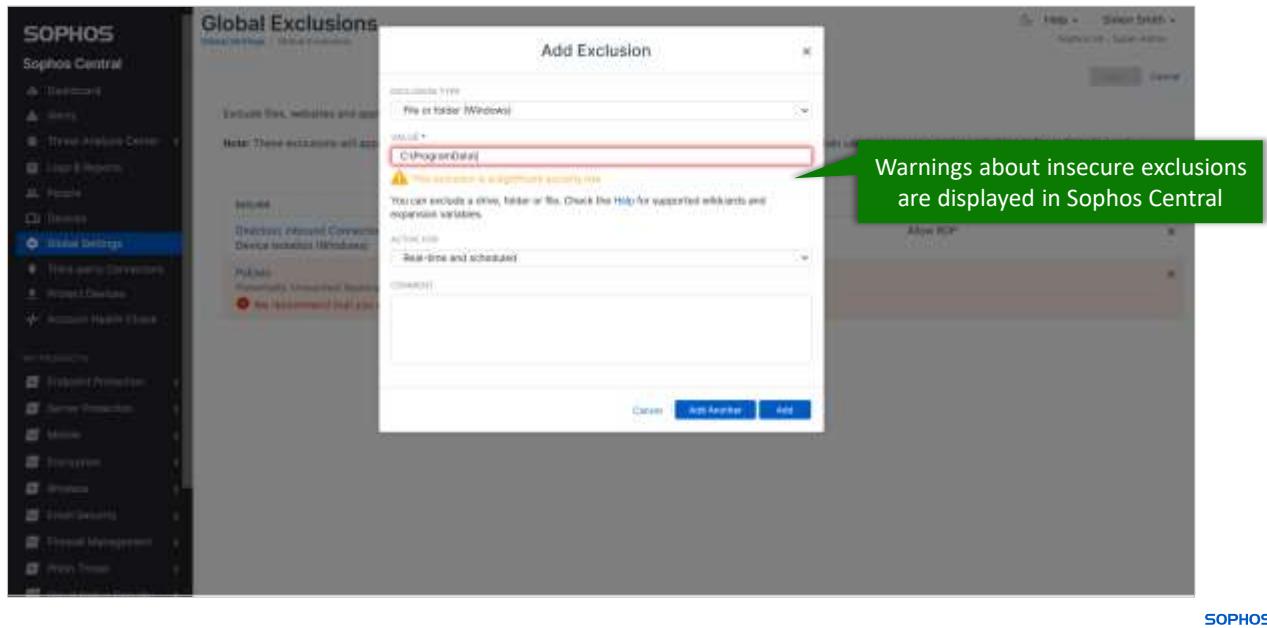
C:\Windows\

C:\ProgramData\

C:\Users\<Username>\

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\

Setting up Specific Exclusions



If you do apply an exclusion that is considered a security risk, a warning indicator will be shown. Additionally, for existing exclusions, a banner message is applied if that exclusion is not recommended by Sophos.

MacOS Scanning Exclusions

SYNTAX	ITEM(S) TO EXCLUDE
myfolder/	All files in any folder that is called myfolder, locally or on the network, and sub-folders recursively
myfolder//	All files in any folder that is called myfolder, locally on the network, but not sub-folders
myapplication	The file myapplication anywhere locally or on the network
/myfolder/myapplication	The file myapplication in a specific folder
/myfolder/	All files in the folder myfolder in a specific location and sub-folder recursively
/myfolder//	All files in the folder myfolder in a specific location but not subfolders
* .mov	All files whose filename extension is .mov anywhere locally on the network
/myfolder/* .mov	All files whose filename extension is .mov in a specific location

SOPHOS

When you add or edit an exclusion for macOS, you can type any POSIX path, whether it is a volume, folder, or file. For example, /volumes/excluded.

This table displays the rules for excluded items on macOS.



Linux Scanning Exclusions

SYNTAX	ITEM(S) TO EXCLUDE
/directory/sub-directory/file.name	Absolute path to file excludes the named file
/directory/sub-directory/	Absolute path to directory excludes everything in the named directory and below
file.name	File name excludes files with this name in any directory
directory/file.name SAV for Linux *.directory/file.name	File name excludes any path ending with the named directory and file
bar/ SAV for Linux */directory/*	Directory name excludes everything below any directory with this name
Directory/sub-directory/ SAV for Linux */directory/sub-directory/*	Relative path to a directory excludes any path containing the named directory
*.fileextension	File extension excludes any file with this extension, in any directory
/directory/*/file.name	Wildcard path excludes any file with the named file name that matches the named directory and wildcard pattern

SOPHOS

You can exclude a specific directory or file by its full path. To exclude a directory and all the directories and files below it, add a trailing slash.

[Additional Information]

Example exclusions:

/mnt/hgfs/excluded excludes the file named excluded.

/mnt/hgfs/excluded/ excludes the directory named excluded and all directories and files below it in the filesystem.

We recommend that you use this exclusion type as specifically as possible.

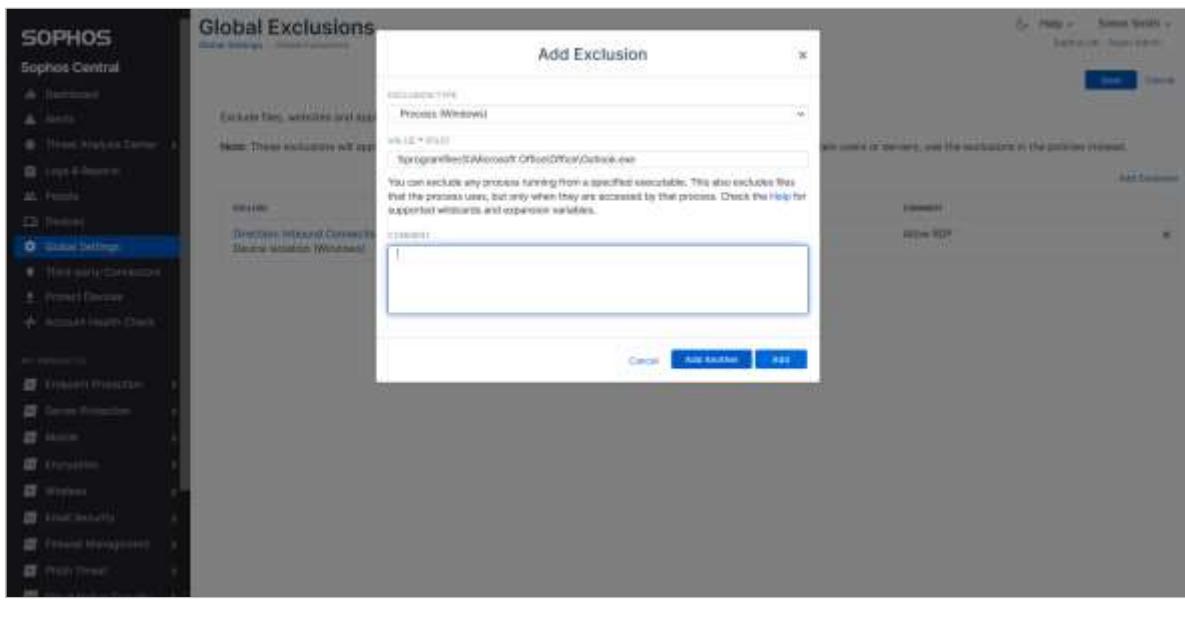
You can exclude a directory or file in any location. For example:

*/excluded excludes the file named excluded in any location.

/excluded/ excludes the directory named excluded in any location and all directories and files below it in the filesystem.

We recommend that you use this exclusion type as specifically as possible.

Process Exclusions (Windows)



SOPHOS

Excluding a process running from an application will also exclude files that the process uses when it is accessed.

When creating a process exclusion, enter the full path from the application and not just the process name shown in Task Manager.

To view all processes or other items that you may need to exclude for an application, see the application vendor's documentation.

Device Isolation Exclusions (Windows)

- Use device isolation exclusions to allow communication with devices that are isolated
- Select where isolated devices use outbound or inbound communication

Local port

Any device can use this port on isolated devices

Remote port

Isolated devices can use this port on any device

Remote address

Isolated devices can only communicate with a device with this IP



SOPHOS

You can allow isolated devices to have limited communications with other devices.

You can choose whether isolated devices will use outbound or inbound communications or both. Use the following settings to restrict communications:

Local port: Any device can use this port on isolated devices.

Remote port: Isolated devices can use this port on any device.

Remote address: isolated devices can only communicate with a device with this IP.

Device Isolation Exclusion (Windows)

Remote desktop access to an isolated device to allow troubleshooting

EXCLUDE	ACTIVE FOR	COMMENT
Direction: Outbound Connection, Remote Address: 172.16.16.20 Device isolation (Windows)		Access isolated devices to download clean up tools
Direction: Inbound Connection, Local Port: 3389 Device isolation (Windows)		Allow RDP

Access isolated devices to download clean up tools

EXCLUDE	ACTIVE FOR	COMMENT
Direction: Outbound Connection, Remote Address: 172.16.16.20 Device isolation (Windows)		Access isolated devices to download clean up tools
Direction: Inbound Connection, Local Port: 3389 Device isolation (Windows)		Allow RDP

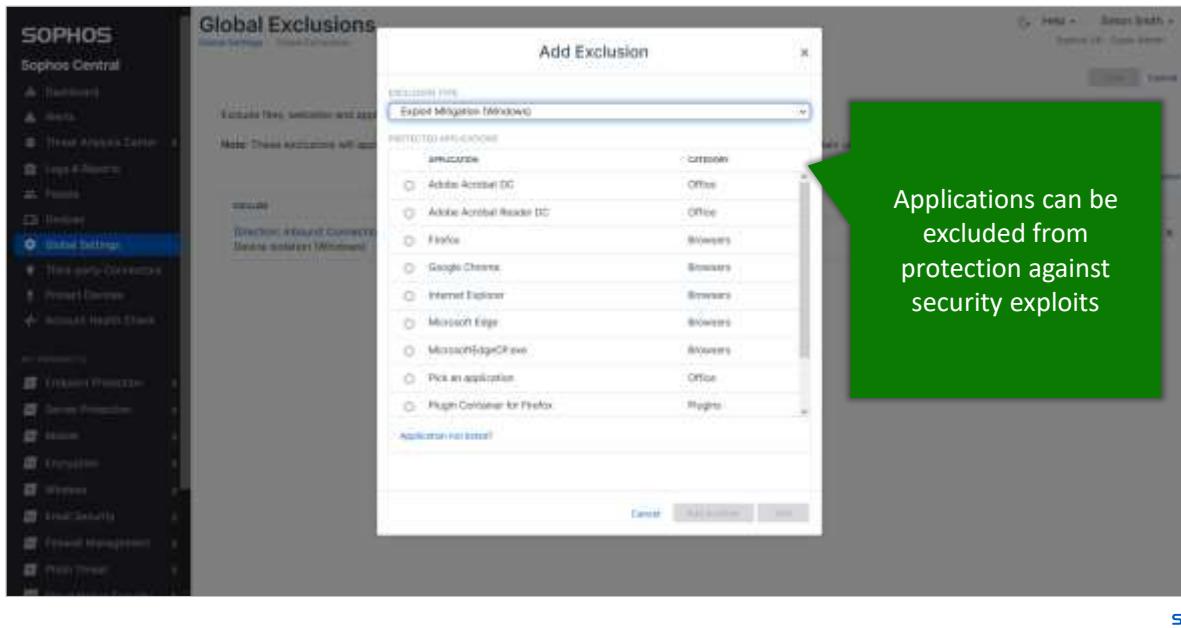
SOPHOS

Here are a couple of examples of how to configure device isolation exclusions.

Remote desktop access to an isolated device is required to allow troubleshooting, to ensure this select inbound connection and enter the port number.

Should you want to access an isolated device to download a clean up tool, select outbound connection and in the remote address, enter the address of the server.

Exploit Mitigation Exclusions



Applications can be excluded from protection against security exploits, this allows you to exclude any exploit that has already been detected. This can be useful if you want to exclude an application that has been incorrectly detected as a threat until the issue is resolved. Once you select an application from the list, you can then select to disable protection for that application.

Exploit Mitigation Exclusions

Protect the application whilst removing specific exploit checks



Applying an application exclusion will completely disable exploit mitigation protection

SOPHOS

You can select the exploit types that you want to check for and those that you do not. This allows you to protect the application whilst removing specific exploit checks.

It is important to note that if used, this will completely disable exploit mitigations for the application it is applied to. Therefore, we recommend that you exclude detected exploit methods using exclusion settings.

Please note that any applications that are excluded are excluded from exploit protection for all users and devices which could allow behaviour which is commonly considered to be bad.



Additional information in
the notes

Exploit Mitigation Exclusions

The screenshot shows the 'Add Exclusion' dialog with the 'EXCLUSION TYPE' dropdown set to 'Exploit Mitigation (Windows)'. Under 'PROTECTED APPLICATIONS', there is a list of applications categorized by type:

APPLICATION	CATEGORY
Adobe Acrobat DC	Office
Adobe Acrobat Reader DC	Office
Firefox	Browsers
Google Chrome	Browsers
Internet Explorer	Browsers
Microsoft Edge	Browsers
Microsoft EdgeCP.exe	Browsers
Pick an application	Office
Plugin Container for Firefox	Plugins

At the bottom, a text input field contains the placeholder 'Application not listed!'.

If an application is not listed, you can add it using its absolute path

The screenshot shows the 'EXCLUDE APPLICATION BY PATH' dialog with the input field containing '\$appdata\myapplication\myapp.exe'. Below the input field, a note says: 'You can exclude an application by absolute path. Check the Help for supported wildcards and expansion variables.'

SOPHOS

If an application is not listed, you can add it using its absolute path. You can use wildcards and variables when you set up scanning exclusions. We recommend that you make your wildcards as specific as possible.

Different variables are used for exploit mitigation exclusions, for example using the variable \$appdata will cover the local and roaming folders as well as the common app data folder and the folder id. For all folder locations please see the additional information in the notes.

[Additional Information]

- C:\Users\<user>\AppData\Local
- C:\Users\<user>\AppData\Roaming
- CSIDL_COMMON_APPDATA
- FOLDERID_LocalAppDataLow



Wildcards and Variables

Wildcard examples:

Expression	Description
theory\document	Excludes any file named document in a folder named theory (in any location)
*.txt	Excludes all .txt files in any locations
C:\theory\	Excludes all files and folders underneath C:\theory\ and including C:\theory\

Variable examples:

Expression	Description
%USERPROFILE%	Excludes C:\Users**\ from scanning
%appdata%	Excludes C:\Users**\AppData\Roaming\ from scanning

Wildcards and variables reduce your protection, be cautious when using them

SOPHOS

You can use wildcards and variables when setting up scanning exclusions. When you use a wildcard or a variable you should ensure that it is specific to retain the protection of the organization.

Here are a few examples of wildcards and variables that are supported when applying scanning exclusions.

[Additional Information]

For more examples, please see the help documentation here:

<https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/GlobalSettings/GlobalExclusions/MitigationExclusionsVariables/index.html#variables>



Additional information in
the notes

Server Exclusions

- Exclusions for common server roles
- Process exclusions
- Environment variables
- Server specific policies

The screenshot shows the Sophos Central interface for managing server protection. On the left, there's a sidebar with 'ANALYSIS' and 'MANAGE PROTECTION' sections. Under 'MANAGE PROTECTION', 'Servers' is selected, and 'Policies' is highlighted. The main content area is titled 'Server Protection - WinServer1'. At the top, there are tabs for 'SUMMARY', 'EVENTS', 'STATUS', 'EXCLUSIONS' (which is highlighted with a red box), 'APPLICATIONS', 'LOCKDOWN EVENTS', and 'POLICIES'. Below the tabs, it says 'These files and applications are currently excluded from scanning for threats.' There are two tabs: 'Known exclusions' (selected) and 'All exclusions'. A search bar and a 'refresh' button are also present. In the 'Real-time scanning - Options' section, there are two toggle switches: 'Automatically exclude activity by known applications' (highlighted with a red box) and 'Detect malicious behavior'. Under 'Detect malicious behavior', there are three sub-options with checkboxes: 'This setting applies to servers running the latest version of Core Agent', 'Adaptive active adversary protection' (which is checked and has a green checkmark), and 'If disabled, active adversary behaviors are reported in Detections for XDR customers'.

Server protection is designed specifically for servers. Exclusions for common server roles are automatically applied. Process exclusions and environmental variables can be added to server policies which provide a greater level of control for protected server security.

Server exclusions are comprised of both automatically applied exclusions and manually applied exclusions. Exclusions for common Windows server applications are automatically applied and are delivered as a data feed to enable Sophos to add new roles over time. All server exclusions are displayed on the EXCLUSIONS tab in the server details in Sophos Central.

In the threat protection policy, the option to automatically exclude activity by known applications is enabled by default.

[Additional Information]

You can view all known application exclusions in knowledge base article **KB-000035264**.
<https://support.sophos.com/support/s/article/KB-000035264>



Additional information in
the notes

Virtual Server Scanning Exclusions

EXCLUSION	NOTES
C:\programdata\adobe\photoshop\	Excludes the folder. You must suffix the back slash for this type of exclusion
C:\program files\program*.com	Excludes files with a .com extension in the specified folder
file.txt	Excludes files with this name in any location
File.*	Excludes all files called 'file' with any extension in all locations
*.txt	Excludes all files with a .txt extension in all locations
C:\file???.docx	Excludes C:\file12.exe but not C:\file123.exe

SOPHOS

For virtually protected servers, you can exclude drives, folders or files by file path. However, there are restrictions on specifying items without a full path and also the use of wildcards.

When you apply an exclusion without a full path, you must include the extension, for example file should be applied as file.txt. You can use wildcards when setting up scanning exclusions, as with all exclusions, it is recommended that you make these as specific as possible.

The exclusions shown here are valid for virtual server exclusions.

[Additional Information]

<https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/GlobalSettings/GlobalExclusions/VirtualServerScanningExclusions/index.html#example-wildcards>

Simulation: Device Isolation Exclusion



In this simulation you are going to create a device isolation exclusion that will allow RDP access to any protected endpoints that have been isolated

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/DeviceIsolationExclusion/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/DeviceIsolationExclusion/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of the following is considered a clean file indicator?

An executable in a temporary data location

A known file that belongs to a legitimate application

An unknown file with a random name

The file is detected by other anti-virus vendors

SOPHOS



Question 2 of 3

True or False: Exclusions should be specific and target specific users or devices.

True

False

SOPHOS



Question 3 of 3

How can you protect an application whilst excluding the application from specific exploit scanning?

Device Isolation Exclusion

Scanning Exclusion

Exploit Mitigation Exclusion

Process Exclusion

SOPHOS

Chapter Review

Exclusions can be used to **override protection policies** by **excluding specific applications, files, or folders** from being scanned.

Exclusions can be used to **allow isolated devices to communicate** with other devices under restrictions.

Exclusions should be added with **extreme caution**. Exclusions **reduce the security** of an organization.

SOPHOS

Here are the three main things you learned in this chapter.

Exclusions can be used to override protection policies by excluding specific applications, files, or folders from being scanned.

Exclusions can be used to allow isolated devices to communicate with other devices under restrictions.

Exclusions should be added with extreme caution. Exclusions reduce the security of an organization.



Getting Started with Sophos Central Server Lockdown

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3560: Getting Started with Sophos Central Server Lockdown

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Server Lockdown

In this chapter you will learn what Server Lockdown is, how to configure the Server Lockdown policy and how to enable and manage a locked down server. You will also learn how to unlock a server.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

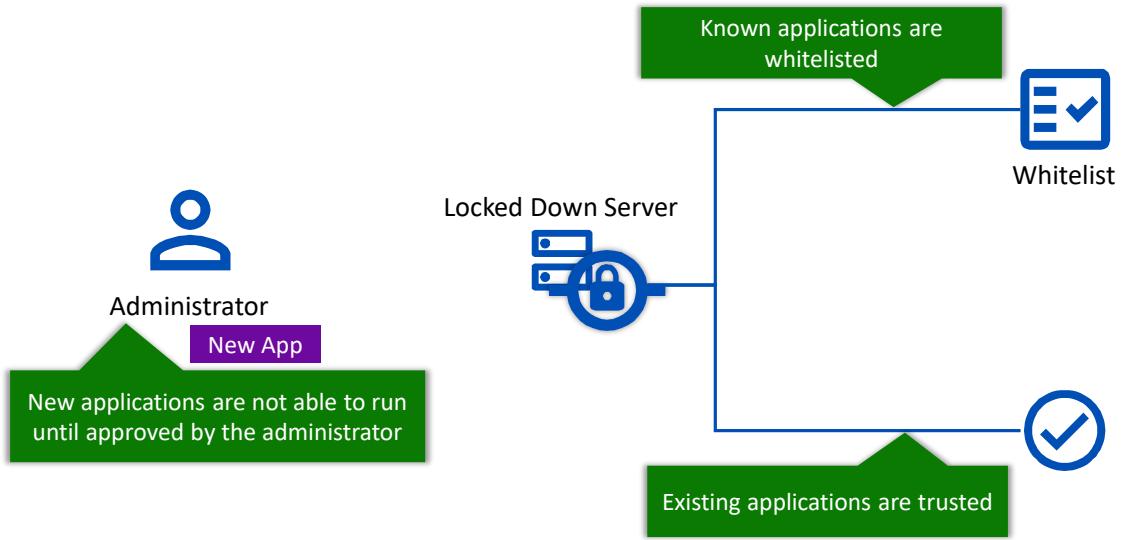
- ✓ How to protect and manage a Windows server in Sophos Central

DURATION **7 minutes**

SOPHOS

In this chapter you will learn what Server Lockdown is, how to configure the Server Lockdown policy and how to enable and manage a locked down server. You will also learn how to unlock a server.

What is Server Lockdown?



SOPHOS

Server lockdown uses technology that only allows approved applications to run on servers. Controlling what is able to run on a protected server and what modifications can be made, can make it harder for an attacker to compromise a server.

Server Lockdown uses drivers that reside in the operating system kernel that only allow trusted applications and their associated files to execute and modify files.

Server Lockdown Policy

- Change the settings on a locked down server without unlocking it
- Allow existing software to run and modify applications
- Configure the Lockdown policy before locking down a server to decrease the overall time taken to generate the whitelist

The screenshot shows the Sophos Central web interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Server Protection', 'ANALYSIS', 'COMMAND', and 'POLICIES' which is highlighted in blue. Below these are 'Antivirus', 'Update Management', and 'Windows Firewall'. The main content area has tabs for 'Web Control (1)', 'Lockdown (1)', 'Data Loss Prevention (0)', and 'Update Management (1)'. Under 'Lockdown (1)', there is a table with one row. The row contains 'Name: Root Policy - Lockdown', 'Status: Enforced', 'Server (single / group):', and 'Last modified: Aug 25, 2022'. A red box highlights the 'Root Policy - Lockdown' name. At the bottom of the main content area, it says 'Windows Firewall (1)'.

SOPHOS

The Server Lockdown policy is used to change the settings on a locked down server without unlocking it. For example, you may want to add and run new software.

Allowing files and folders permits new software to run. It also allows existing software to run and modify other applications. An example could be a folder used to restore trusted installers. Please be cautious when using this option as it ‘trusts’ the software so that any files it creates or changes are also trusted.

It is beneficial to configure the Server Lockdown policy before locking down a server because the specified files and folders will not be scanned or added to the whitelist. This decreases the overall time taken to generate the whitelist.

Server Lockdown Policy

- Files in a network share are not blocked if the folder location or file is blocked in the Lockdown policy
- Allowed and blocked lists in the Lockdown policy **ONLY** apply to local execution

The screenshot shows the 'Server Protection' interface in Sophos Central. The left sidebar has a dark theme with white text and icons. The 'Policies' option is selected and highlighted in blue. The main content area has a light background. At the top, there's a note about locking down a server and allowing specific software to run. Below it, the 'Allowed files/folders' section shows a table with one entry: 'C:\Program Files\Mozilla Firefox\firefox.exe'. An 'Add allowed file/folder' button is at the top right of this section. Below that is the 'Blocked files/folders' section, which contains a note that says 'Block software that is currently allowed to run.' A table here shows one entry: 'C:\Program Files (x86)\Notepad++\notepad++.exe'. An 'Add blocked file/folder' button is at the top right of this section. The bottom right corner of the interface has the 'SOPHOS' logo.

'Blocked files/folders' can be used to block software that is currently allowed to run or to block a specific folder 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. An example may be a share or filer location.

Please note, if you have installers in a share, they can be executed on a remote computer without being in the allowed files and folders, this is only required to allow local execution on the server. In the same way, you cannot prevent a shared installer from being run on a remote computer by adding it to the blocked files and folders.

Enabling Server Lockdown

The screenshot shows the Sophos Central interface for Server Protection. On the left sidebar under 'MANAGE PROTECTION', the 'Servers' option is selected. In the main content area, the 'SUMMARY' tab is active. A green arrow points from the 'Lock Down' button in the sidebar to the 'Lock Down' section of the summary card. Another green arrow points from the 'Begin Lockdown' button in the summary card to the 'Begin Lockdown' button in the modal dialog. The modal dialog is titled 'Lock Down' and contains instructions about creating an allow list and a warning about software installations during the process.

Server Lockdown is enabled on the **Details** page for a server by clicking **Lock Down**.

When locking down a server, the current state is taken 'as good', and any existing applications can be run normally. New applications added after lockdown will not be able to run unless allowed by a Sophos Central administrator. The process is known as whitelisting. The lockdown process scans all local drives, so any policies will need to cover these.

Please note that Server Lockdown can take some time to complete.

Enabling Server Lockdown

The screenshot shows the Sophos Central interface for managing server protection. On the left sidebar, under 'MANAGE PROTECTION', the 'Servers' option is selected. In the main content area, a server named 'WinServer1' is selected. The 'SUMMARY' tab is active. On the left, there's a sidebar with several buttons: 'Scan Now', 'Unlock' (which is highlighted with a red box), 'Diagnose', 'Reset health status', and 'Live Response'. In the main summary section, under 'Lockdown Status', it shows 'Locked' (also highlighted with a red box). Other details shown include the IPv4 Address (172.16.16.10), Operating System (Windows Server 2019 Standard), Processor Architecture (x64), and Tamper Protection (On).

Once completed, a server will display the ‘Unlock’ button in the server details.

On the **SUMMARY** tab you will see the Lockdown Status. This will change during the lockdown process, however, when completed, it will display as ‘Locked’.

Enabling Server Lockdown

The screenshot shows the Sophos Endpoint Self Help Tool interface. On the left, there's a sidebar with 'Update Status' (Last update: 01 September 2022 11:21, Update Now), 'Products' (including Update Cache 1.9.0.143, Message Relay 1.6.0.26, Server Core Agent 2022.2.18, Server Intercept X 2021.3.1.15, and Lockdown 71.2.1 (Locked down)), and 'Troubleshooting' (Open Endpoint Self Help Tool). The main area has tabs for Health State, System, Installed Components, Services, Management Communication, Update, Policy, and Server. The 'Lockdown' section is highlighted with a red box. It shows 'State' as 'Locked' and 'Date Whitelisted' as 05:40 Sep 1, 2022 (UTC+01:00). Below it is 'Sophos Update Cache' with 'Status' as 'Good' and 'Last Successful Update' as 11:08:35 Sep 1, 2022 (UTC+01:00). A 'Remediation' section with a 'Did this help you?' button is also visible. The bottom right corner says 'SOPHOS'.

The Sophos Endpoint Agent will display the Lockdown status of the server. Click **About** to view the products installed.

Opening the **Endpoint Self Help Tool** and select the **Server** tab which displays the Lockdown state and when the files were whitelisted.

Managing a Locked Down Server

The screenshot shows the Sophos Central interface for managing a locked-down server named WinServer1. The left sidebar has a dark theme with categories like ANALYZE, MANAGE PROTECTION (with Servers selected), and CONFIGURE. The main area is titled 'Server Protection - WinServer1' and shows a summary of events from August 24, 2022, to August 25, 2022. A red box highlights the 'Update Report' button in the top right corner of the event list. The event list table includes columns for EVENT (COUNT), DATE, PARENT, and TARGET, with 575 Lockdown Events listed.

EVENT (COUNT)	DATE	PARENT	TARGET
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	mpavdita.lkg
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	mpavdita.vdm
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	mpengine.dll
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	mpengine.lkg
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	MpAsBase.vdm
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	MpAvBase.vdm
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	MpAvDita.vdm
Write File Denied ()	Aug 24, 2022 2:53 PM	MsMpEng.exe	MpEngine.dll

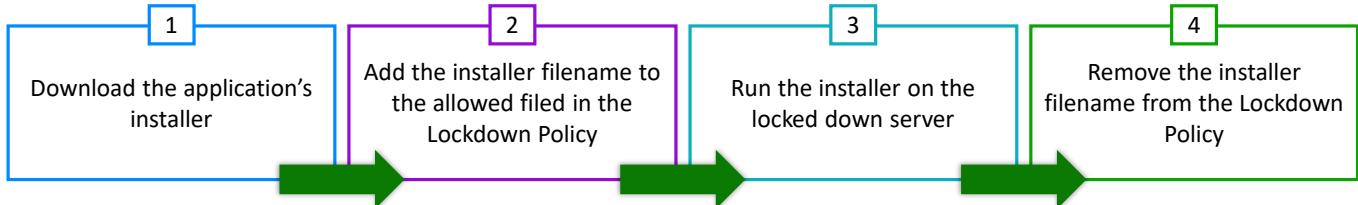
The **LOCKDOWN EVENTS** tab will appear in the server details page once lockdown has been completed. This tab displays any triggered warnings or events relating to the locked down status.

Please note that following lockdown, you will need to click **Request Report** to view the report. You will then need to click **Update Report** to view any updated lockdown events.



Additional information in
the notes

Managing a Locked Down Server



Avoid allowing applications like FileZilla.exe in the Lockdown Policy as files downloaded by the allowed application can be executed on the Locked Down server and reduce protection

SOPHOS

To add or update an application without unlocking the server, we recommend the following process:

1. Download the installer of the application you want to install on the locked down server
2. Add the application's installer file name to the Lockdown Policy in Sophos Central as an allowed file
3. Run the installer on the locked down server
4. Once the application is installed, remove the installer file from the Lockdown Policy in Sophos Central

This process will add the installed application's files to the local whitelist so that it is executed successfully.

Adding application installers or execution files in the Lockdown Policy to allow them on a protected server can have unwanted effects, and can reduce the security of the server. If you choose to add an Internet browser for example, every file that is downloaded from that browser becomes trusted, and can execute on the server.

The process detailed here prevents this from happening, allowing your servers to run the required applications without compromising the security of your servers.

[Additional Information]

For more information and other applications that should be manually configured, see knowledge base article **KB-000035445**. <https://support.sophos.com/support/s/article/KB-000035445>



Additional information in
the notes

Unlocking a Locked Down Server

The screenshot shows the Sophos Central interface for managing server protection. On the left sidebar under 'MANAGE PROTECTION', the 'Servers' option is selected. In the main content area, the 'Server Protection - SRV3' page is displayed. A vertical menu on the left side of the main content area includes options like 'Isolate', 'Scan Now', 'Unlock' (which is highlighted with a red box), 'Diagnose', and 'Reset health status'. The 'Unlock' button is located below the 'Scan Now' button. At the top right of the main area, there are tabs for 'SUMMARY', 'EVENTS', 'STATUS', 'EXCLUSIONS', 'APPLICATIONS', and 'POLICIES'. Below these tabs, the 'Recent Events' section lists several log entries. The 'Agent Summary' section provides details about the last Sophos Central activity, the last agent update, and assigned products.

To unlock a server, navigate to the Server details page in Sophos Central and click **Unlock**.

Please note that when unlocking a server unauthorized activities on that server will no longer be prevented. A confirmation message will be displayed to ensure that you mean to unlock the server.

Once unlocked, the server will return to its unlocked state and the execution of all files will be allowed. The lockdown agent on the server needs to be removed locally. The unlock process does not remove the agent. This is completed by locating the uninstall string in the registry and running an uninstall command from a command prompt.

[Additional Information]

More information about this can be found in Knowledge base article **KB-000035355**.

<https://support.sophos.com/support/s/article/KB-000035355>

Simulation: Configure and Apply Server Lockdown



In this simulation, you will enable Server Lockdown and test the lockdown features.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/ServerLockdown/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/ServerLockdown/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

When a server is Locked Down, what type of applications can be run?

None

Internet Browsers

Known/Trusted

Business

SOPHOS



Question 2 of 3

True or False: Allowed and blocked items in a Lockdown Policy only apply to locked down servers.

True

False

SOPHOS



Question 3 of 3

Put the steps in the correct order to add a new application to a Locked Down server.

Remove the installer filename from the Lockdown Policy

DROP

1

Add the installer filename to the Lockdown Policy

DROP

2

Download the application's installer

DROP

3

Run the installer on the Locked Down server

DROP

4

SOPHOS

Chapter Review

Server Lockdown uses technology that **only allows trusted applications** and their associated files to execute and modify files.

The **Server Lockdown policy is used to change the settings** on a locked down server without unlocking it.

Allowing files and folders permits new software to run. It also allows existing software to run and modify other applications.

SOPHOS

Here are the three main things you learned in this chapter.

Server lockdown uses technology that only allows trusted applications and their associated files to execute and modify files.

The Server Lockdown policy is used to change the settings on a locked down server without unlocking it.

Allowing files and folders permits new software to run. It also allows existing software to run and modify other applications.



Sophos Central Server File Integrity Monitoring

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE3570: Sophos Central Server File Integrity Monitoring

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central Server File Integrity Monitoring

In this chapter you will learn what file integrity monitoring is, how to configure it, and how it works.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to protect servers from Sophos Central
- ✓ How to manage servers in Sophos Central

DURATION **5 minutes**

SOPHOS

In this chapter you will learn what file integrity monitoring is, how to configure it, and how it works.



Additional information in
the notes

File Integrity Monitoring (FIM)

Why Monitor?

- Critical systems for additional security
- Assists in meeting compliance

What is Monitored?

- Files
- Folders
- Registry keys
- Registry values

Find out More!

- Pre-configured with default rules
- Default monitoring locations: <https://support.sophos.com/support/s/article/KB-000038115>
- FAQs: <https://support.sophos.com/support/s/article/KB-000038360>

SOPHOS

Sophos File Integrity Monitoring can assist you in either monitoring critical systems, providing additional security, or to meet PCI:DSS compliance.

When enabled, File Integrity Monitoring can monitor files, folders, registry keys and values.

The policy is pre-configured with default rules as well as providing the ability to add additional monitoring locations or exclusions.

The default monitoring locations are documented in the knowledge base and frequently asked questions can be found there also.

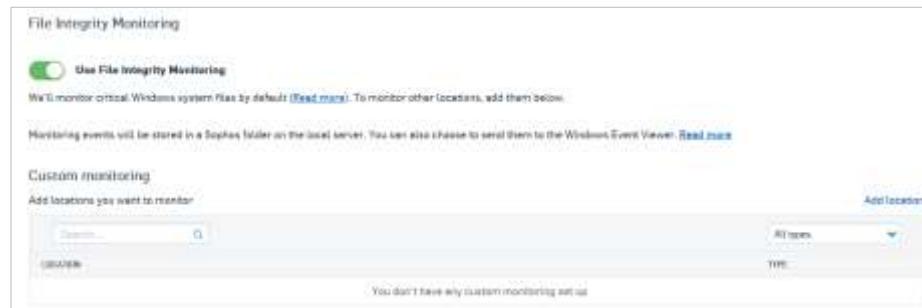
[Additional Information]

Default monitored locations **KB-000038115**: <https://support.sophos.com/support/s/article/KB-000038115>

FAQs **KB-000038360**: <https://support.sophos.com/support/s/article/KB-000038360>

File Integrity Monitoring (FIM)

- Add files, folders, registry keys and values to be monitored



- Exclude specific files, folders, registry keys and values from being monitored



SOPHOS

File Integrity Monitoring is installed by default, however, it is only applied when the File Integrity Monitoring policy is enabled.

There are two configurable policies for File Integrity Monitoring:

- Custom monitoring** allows you to add files, folders, registry keys and values to the list of monitored items. This is in addition to the critical Windows system files that are monitored by default
- Monitoring exclusions** let you exclude files, folders, registry keys and values. For example, you may decide to exclude a critical Windows system file that is monitored by default

File Integrity Monitoring (FIM)

Add location

You can add a folder, file or registry key. Check the Help for supported wildcards and system variables.

Type: **Folder**

Path: **For example: C:\some**

This will monitor files in the folder.

Monitor changes to the folder as well as the files.

Apply to sub-folders.

Please enter file types (separated by commas):
.txt, .log, .xml

You can monitor up to five different file types.

Cancel **Add location** **Next**

The registry key is monitored only, any registry values must be added separately

Add location

You can add a folder, file or registry key. Check the Help for supported wildcards and system variables.

Type: **Registry Key**

Path: **For example: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management**

Apply to subkeys.

Cancel **Next** **Finish**

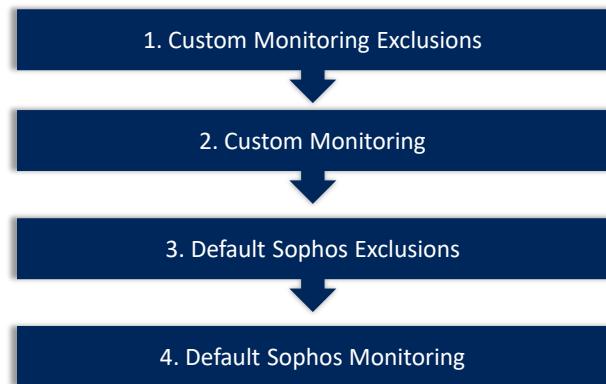
Selecting a folder will monitor the folder and files included by default

When the folder type is selected for monitoring, File Integrity Monitoring monitors the folder and the files included in the folder by default. To monitor changes made to only the files, de-select **Monitor changes to the folder as well as the files**.

When selecting a registry key for monitoring, the key is monitored but the values within it are not. You must use the registry value option to monitor any values included in a registry key.

File Integrity Monitoring (FIM)

- Rules are evaluated in order of precedence



SOPHOS

Rules are evaluated with the following order of precedence:

1. Custom monitoring exclusions
2. Custom monitoring
3. Default Sophos exclusions
4. Default Sophos monitoring



Additional information in
the notes

File Integrity Monitoring (FIM)

The screenshot shows a Windows File Explorer window. The address bar indicates the path: This PC > Windows (C) > ProgramData > Sophos > File Integrity Monitoring > Export. A single file named '2020-12-03_10-48_1_2_2_databatch.xml' is listed in the file list. The file is an XML Document, modified on 12/3/2020 at 10:48 AM, and is 1 KB in size.

- Files written every 15 minutes
- Each file may contain multiple events
- Files older than 90 days are deleted

SOPHOS

File Integrity Monitoring events are logged locally on assigned protected servers.

These files are written every fifteen minutes and each file may contain multiple events. The data files in the default location are purged when they become older than ninety days, so we recommend storing your own copy of the data to prevent deletion of any data that you may require.

[Additional Information]

Events are stored in the databatc.xml file which can be found in the C:\ProgramData\Sophos\File Integrity Monitoring\Export directory.

File Integrity Monitoring (FIM)

```
<database type="sophos.fim.databatch" timestamp="2019-04-01T11:39:32Z" schemaVersion="1.0" xmlns="http://www.sophos.com/xml/msys/SophosFim.xsd">
<item eventType="21" eventName="SetRegistryValue" eventTime="2019-04-01T11:23:21Z" isAlert="0" isCustom="0" eventCount="1"
targetName="LastLogOffEndTimePerfCounter" targetParent="\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows MT\CurrentVersion\Winlogon\" targetId=""
processId=2688" processCreateTime="2019-04-01T11:23:10Z" processImageFile="winLogon.exe" processImageFolder="C:\Windows\System32" accountSid="S-1-5-18" accountDomain="NTAUTHORITY" accountName="SYSTEM" specificData="" />
<item eventType="4" eventName="ModifyFileContent" eventTime="2019-04-01T11:32:49Z" isAlert="0" isCustom="1" eventCount="1" targetName="BGInfo.bat" targetParent="C:\BGInfo\" targetId="" processId="67196" processCreateTime="2019-04-01T11:32:41Z" processImageFile="notepad.exe" processImageFolder="C:\Windows\System32" accountSid="S-1-5-21-4003377331-1401390349-2030712665-500" accountDomain="SOPHOS" accountName="Administrator" specificData="" />
<item eventType="104" eventName="userPolicyChanged" eventTime="2019-04-01T11:37:54Z" isAlert="0" isCustom="0" eventCount="1" targetName="" targetParent="" targetId="" processId="0" processCreateTime="" processImageFile="" processImageFolder="" accountSid="" accountDomain="" accountName="" specificData="95be498b3528a73f2e990776451fd267ba6509f9725ab847c5" />
```

The file information shows:

- The modified file and its path
- When it was modified and which process
- Which user modified the file
- Whether it is a custom rule or a default rule

SOPHOS

Here is an example of one of the data files. If we look at the highlighted example, we can see that it is for a file modification.

We can see the following information:

- The file that was modified along with the file path
- When it was modified and by which process
- Which user modified the file
- And, whether it was a custom rule or a default rule



Additional information in
the notes

File Integrity Monitoring (FIM)

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various log sources, including 'Event Viewer (Local)', 'Custom Views', 'Windows Logs', 'Application and Service Logs', 'Hardware Events', 'Internet Explorer', 'Key Management Service', 'Memory', 'Sophos' (which is expanded to show 'Endpoint Self-Help' and 'File Integrity Monitoring'), and 'Events'. A sub-menu under 'Events' shows 'Sophos FIM Event Channel'. On the right, the main pane displays the 'Sophos FIM Event Channel - Number of events: 9' table. The table has columns for 'Level', 'Date and Time', 'Source', and 'Event ID : Task Category'. All entries are at the 'Information' level and occurred on 12/12/2018 at 3:39:32 AM, with the source being 'Events' and the task category being 'None'. Below the table, there are two tabs: 'General' (selected) and 'Details'. The 'Details' tab is highlighted with a green arrow. The details pane shows event properties: targetName (BGInfo), targetParent (\REGISTRY\MACHINE\SOFTWARE\WOW6432No), targetId (67864), processId (67864), processCreateTime (2018-12-12T11:26:03.720Z), and processImageFile (regedit.exe). At the bottom of the details pane, there is a link 'Event Log Online Help'.

In addition to the default event logs, you can also register a Windows Event Log channel that will enable events to be logged to the Windows Event Log. To enable the logging of events in the Windows Event Log, you must run the command shown here in an elevated command prompt.

Please note that Sophos does not purge Windows events. This is done by the Windows event log when the size of the data in the File Integrity Monitoring Event Channel exceeds the default limit of 51MB. The limit can be changed from the Windows Event Viewer or by a policy (if configured). You may want to periodically export events to another location to prevent loss of data.

[Additional Information]

The elevated command prompt to enable logging of events in the Windows Event Log is: `wevtutil im "%ProgramFiles%\Sophos\File Integrity Monitoring\SophosFimEventProvider.man"`

Enable and Configure File Integrity Monitoring



In this simulation you will enable and configure File Integrity Monitoring.

LAUNCH SIMULATION

CONTINUE

<https://training.sophos.com/ce/simulation/FIM/1/start.html>

SOPHOS

Please complete this simulation.

Click **Launch Simulation** to start. Once you have finished, click **Continue**.

[Additional Information]

<https://training.sophos.com/ce/simulation/FIM/1/start.html>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which of the following can be monitored when FIM is enabled?

Files

Applications

Registry Values

Processes

SOPHOS



Question 2 of 3

What is the function of File Integrity Monitoring?

To allow approved applications to run on servers

To monitor critical systems for additional security

To send an email alert to admins when any file is modified

To monitor the Sophos installation files on the server

SOPHOS



Question 3 of 3

In which directory are the File Integrity Monitoring events logged?

C:\Program Files (x86)\Sophos\File Integrity Monitoring\Export

C:\Program Files(x86)\File Integrity Monitoring

C:\ProgramData\Sophos\File Integrity Monitoring\Export

C:\ProgramData\File Integrity Monitoring

SOPHOS

Chapter Review

Sophos File Integrity Monitoring can assist you in monitoring critical systems, providing additional security, or to meet PCI:DSS compliance.

File Integrity Monitoring can monitor files, folders, registry keys and values.

The policy is pre-configured with default rules as well as providing the ability to add additional monitoring locations or exclusions.

SOPHOS

Here are the three main things you learned in this chapter.

Sophos File Integrity Monitoring can assist you in monitoring critical systems, providing additional security, or to meet PCI:DSS compliance.

File Integrity Monitoring can monitor files, folders, registry keys and values.

The policy is pre-configured with default rules as well as providing the ability to add additional monitoring locations or exclusions.



Getting Started with Sophos Central Logs and Reports

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4005: Getting Started with Sophos Central Logs and Reports

December 2022

4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Logs and Reports

In this chapter you will learn how to run, customize, and save reports.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Access and navigate Sophos Central
- ✓ Protect and manage devices with Sophos Central

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how to run, customize, and save reports.

Overview

The screenshot shows the Sophos Central interface with the 'Logs & Reports' section selected in the left-hand navigation menu. The main area displays a table of report templates and a section for logs.

Logs & Reports

View logs and reports to help analyze and improve your security.

Template Name	Legacy?	Source	Created By	Schedule Frequency	Report Format	Generated Reports
Week Malware Report	✓	Events		Weekly	CSV	N/A
Bandwidth - UK	✓	Firewall		Weekly	PDF	13

Total Templates: 2

Logs

General Logs

- Events**: Shows all security events, such as malware detections, on your devices and let you filter them to generate reports.
- Audit Logs**: Record of all activities and changes made to the system.

Email Security Logs

- Message History**: Shows log of all mail processed by the system.

Cloud Optix

- Audit Logs**

Sophos Central provides an extensive range of logs and reports.

All logs and reports can be viewed by navigating to **Logs & Reports** in the left-hand menu of the Sophos Central dashboard.

Overview

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various sections: Dashboard, Alerts, Threat Analysis Center, Logs & Reports (which is selected and highlighted in blue), People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, and Mobile. The main content area is titled 'Logs' and contains several sections: 'General Logs' (Events and Audit Logs), 'Endpoint & Server Protection Logs' (Data Loss Prevention and Live Response session audit), 'Reports' (Users and Endpoint & Server Protection), and 'Cloud Optix' (Email Security Logs and Audit Logs). Each section provides a brief description of its function.

SOPHOS

Sophos Central

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports**
- People
- Devices
- Global Settings
- Third-party Connectors
- Protect Devices
- Account Health Check

MY PRODUCTS

- Endpoint Protection
- Server Protection
- Mobile

Logs

General Logs

- Events**
Shows all security events, such as malware detections, on your devices and let you filter them to generate reports.
- Audit Logs**
Record of all activities and changes made to the system.

Endpoint & Server Protection Logs

- Data Loss Prevention**
Show all activity triggered by data loss prevention rules.
- Live Response session audit**
Shows all activity in each Live Response session.

Reports

Users

- Users**
Shows how many users are active, inactive or unprotected, as well as details of those users.

Endpoint & Server Protection

- Hero Reports**

Email Security Logs

- Message History**
Shows log of all mail processed by the system.

Cloud Optix

- Audit Logs**
Record of all activities and changes made to Cloud Optix, including policy changes and alert suppressions.

The logs and reports available depend on the products you have licensed.

Product Specific Logs and Reports

The image displays three side-by-side screenshots of the Sophos Central interface, each showing a different product's specific logs and reports page.

- Sophos Endpoint Protection - Logs & Reports:** This dashboard shows logs and reports for Endpoint Protection. It includes sections for "Logs" (Endpoint Protection Logs, Data Loss Prevention), "Reports" (Users, Endpoint Protection, Computers, Malware and PUAs blocked), and a sidebar with ANALYZE (Dashboard, Logs & Reports selected), MANAGE PROTECTION (People, Computers), and more.
- Sophos Server Protection - Logs & Reports:** This dashboard shows logs and reports for Server Protection. It includes sections for "Logs" (Server Protection Logs, Data Loss Prevention) and "Reports" (Servers, Policies, Settings, Protect Devices). The sidebar is identical to the Endpoint Protection dashboard.
- Sophos Central Footer:** The bottom right corner of the interface features the "SOPHOS" logo.

If you prefer to view only the logs and reports that are available for a specific product, navigate to the product specific dashboard.

In the **Logs & Reports** page, you will find the reports and the logs that are relevant for that product only.

User, Computer and Server Reports

The screenshot shows the Sophos Central interface for Endpoint Protection. The left sidebar has a dark theme with white text. It includes sections for ANALYZE (Dashboard, Logs & Reports, which is selected), MANAGE PROTECTION (People, Computers), CONSOLE (Policies, Settings, Protect Devices), and MORE PRODUCTS (Free Trials). The main content area is titled "Endpoint Protection - User Report". At the top, there are summary statistics: 99 Active users, 6 Online users, 0 Inactive 2+ Weeks users, 31 Inactive 2+ Months users, and 62 No Devices. Below this is a table with columns: NAME, EMAIL, ONLINE, DEVICES, LOGINS, GROUPS, and HEALTH. The table lists several user accounts with their associated devices and login history. A message at the bottom says "Displaying 99 out of 99".

NAME	EMAIL	ONLINE	DEVICES	LOGINS	GROUPS	HEALTH
TRAININGDEMO\administrator	TRAININGDEMO\administrator	5 minutes ago	WinClient5, WinClient3, WinClient4, WinClient1, WinClient2	TRAININGDEMO\administrator	TRAININGDEMO\administrator	●
SOPHOS\Administrator	SOPHOS\Administrator	16 hours ago	Training-W10	SOPHOS\Administrator	SOPHOS\Administrator	●
WINDOWS-XRD\Administrat...	WINDOWS-XRD\Administrat...	16 hours ago	Windows-XRD	WINDOWS-XRD\Administr...	WINDOWS-XRD\Administr...	●
SOPHOS\helpdesk	SOPHOS\helpdesk	6 days ago		SOPHOS\helpdesk		●
MN-5035A11489B4\Rebec...	MN-5035A11489B4\Rebec...	6 days ago		MN-5035A11489B4\Re...		●

The reports for users, endpoints and servers all look similar.

They contain a summary view at the top of the page. Clicking on the numbers in the summary view will apply a filter to the report for the selected category.

The detailed information varies depending on the report; however, the reports will typically show details like associated devices, the health status, login information and management information.

You can use all this information to monitor protected devices and users and spot any inconsistencies.

Events Report

Events Report

Reports Events Report

Help Simon Smith Sophos UK - Super Admin

Choose period: Last 7 days

Update

Show all security types ▾ Search by User Group ▾ Search by Computer or Server Group ▾

Checked items are included in the event results:

- Type (193)
- Runtime Detections (10)
- Application Control (18)
- Malware (15)

Aug 17, 2022 Aug 18, 2022 Aug 19, 2022 Aug 21, 2022 Aug 23, 2022

ID	DATE	EVENT	USER	USER GROUPS
1	Aug 18, 2022 8:34:52 PM	Malware marked as resolved	SOPHOS\Administrator	Training-W10
2	Aug 18, 2022 8:34:52 PM	Malware marked as resolved	SOPHOS\Administrator	Training-W10
3	Aug 18, 2022 8:34:52 PM	Malware marked as resolved	SOPHOS\Administrator	Training-W10

Displaying 15 out of 193

The events report provides information on all events. You can search for events and filter the date range allowing you to narrow down your search. Once you change any of the filters, click **Update** to update the report.

In the event list next to the graphical representation of events, you can filter the event types that are displayed. This filter is useful if you only want to focus on a particular event type, for example policy violations, or malware detections.

These filters can be further expanded for each event type so that you can report on the specific actions taken, for example, malware that has been detected, cleaned up, not cleaned up or locally cleared.

Events Report

The screenshot shows the Sophos Central interface with the 'Events Report' selected. The left sidebar includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports' (which is selected), 'People', 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Under 'My Products', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, and Firewall Management. The main area has a title 'Events Report' with sub-links 'Reports' and 'Events Report'. It features a search bar, a date range selector ('Choose period: Last 7 days'), and filter buttons for 'Show all severity types', 'Search by User Group', and 'Search by Computer or Device Group'. A legend indicates checked items: Type (193), Malware (15) (selected), Potentially Unwanted Application (PUA) (200), Policy Violations (4) (selected), and Web Control (53). A bar chart shows event counts from Aug 17 to Aug 23. Below the chart is a table of event details:

TIME	DATE	EVENT	USER	USER GROUP	DEVICE
▲	Aug 23, 2022 9:06:58 AM	Controlled application blocked: Microsoft Power...	TRAINING0EMQ\administrator		WinClient
▲	Aug 23, 2022 3:15:02 PM	Controlled application blocked: Microsoft Power...	SOPHOS\administrator		Training VM
▲	Aug 22, 2022 11:24:01 AM	Controlled application blocked: Microsoft Power...	TRAINING0EMQ\administrator		WinClient

Displaying 37 out of 193

On the far right, there are 'Save as Custom Report' and 'Export' buttons, with the 'Export' button highlighted with a red box. A dropdown menu for 'Export' lists options: 'CSV of current view', 'PDF of current view', 'CSV of past 90 days', and 'PDF of past 90 days'.

In this example, we have filtered the report to show only malware and policy violation events.

The events report can be exported to either a CSV or a PDF. You can select to export the details of the report for the past 90 days, or to use the current time filter you have configured.

Exporting events details can assist with the offline manipulation or presentation of the data.

Events Report

A	B	C	D	E	F	G
Severity	When	Event	User	User Groups	Device	Device Groups
Medium	2022-08-23T09:06:58+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient2	Sales Operations AUS
Medium	2022-08-22T15:13:02+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	SOPHOS\Administrator		Training-W10	Reading Office
Medium	2022-08-22T11:24:01+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient5	
Medium	2022-08-22T11:09:23+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient3	
Medium	2022-08-22T11:07:47+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient1	Sales Operations AUS
Medium	2022-08-22T11:04:31+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient2	Sales Operations AUS
Medium	2022-08-22T11:03:43+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient4	
Medium	2022-08-20T13:51:17+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	SOPHOS\Administrator		Training-W10	Reading Office
Medium	2022-08-19T09:08:19+01:00	Controlled application blocked: Microsoft PowerShell (System tool)	TRAININGDEMO\administrator		WinClient6	
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office
Low	2022-08-18T18:34:52+01:00	Malware marked as resolved	SOPHOS\Administrator		Training-W10	Reading Office

SOPHOS

You can save the report to suit your individual requirements once it has been exported.

Customised Reports

The screenshot shows the Sophos Central interface with the 'Events Report' selected. The left sidebar includes links for Dashboard, Alerts, Threat Analysis Center, Log & Reports (which is highlighted), People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Under 'My Products', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, and Firewall Management. The main content area is titled 'Events Report' and shows a bar chart for the period 'Last 7 days'. The chart has two bars: one at Aug 17, 2022, with a value of 34, and another at Aug 23, 2022, with a value of 8. Below the chart is a list of events with columns for ID, Date, Event, User, and User Groups. The events listed are all of type 'Malware' (15) and occurred on Aug 22 and Aug 23, 2022. At the bottom, it says 'Displaying 37 out of 193'.

You can customize the events report and then save it. Once saved, it will retain all the filters applied.

To save a report, click **Save as Custom Report**.

Name the report and select how you want to distribute the report. Please note that if you are including personally identifiable information in the report, we recommend that you select to send a link to the report rather than attach the report to an email.

Schedule the frequency of when the report is sent. Please note that any schedule created will automatically stop after 6 months.

Saved Reports

The screenshot shows the Sophos Central interface with the 'Logs & Reports' section selected. At the top, there's a search bar and navigation links for Help, Simon Smith, and Business UK - Super Admin. Below the header, a green callout box points to the 'View the report format' link in the table header. The table lists saved reports with columns for Template Name, Legacy?, Source, Created By, Schedule Frequency, Report Format, and Generated Reports. One row is highlighted with an orange box around the 'Legacy?' column, which contains the value 'Bandwidth - UK'. The table shows 13 total templates. Below the table, there are sections for General Logs, Email Security Logs, Audit Logs, Cloud Optix, Endpoint & Server Protection Logs, Data Loss Prevention, and Live Response session audit.

Template Name	Legacy?	Source	Created By	Schedule Frequency	Report Format	Generated Reports
Bandwidth - UK	Legacy?	Firewall		Weekly	PDF	13

Logs

General Logs

- Events**
Shows all security events, such as malware detections, on your devices and let you filter them to generate reports.
- Audit Logs**
Record of all activities and changes made to the system.

Endpoint & Server Protection Logs

- Data Loss Prevention**
Show all activity triggered by data loss prevention rules.
- Live Response session audit**

Email Security Logs

- Message History**
Shows log of all mail processed by the system.

Cloud Optix

- Audit Logs**
Record of all activities and changes made to Cloud Optix, including policy changes and alert suppressions.

Once you have saved a report, it is easily run from the **Logs & Reports** page. A list of all saved reports are displayed at the top of the **Logs & Reports** page. You can view who created them, their format and their scheduled frequency.

There are two types of report formats, legacy and newer. You can determine if a report is using the legacy format by viewing the legacy column.

Scheduled Reports

Legacy Reports

- Each administrator can configure up to 25 scheduled reports
- Scheduled reports expire after 6 months
- Maximum of 10,000 events per report or log
- Only the administrator who created the report can view them

SOPHOS

Legacy reports use an older format and have some restrictions.

- Each administrator can configure up to twenty five scheduled reports
- Scheduled reports expire after six months. You can edit the scheduled report and save it anew to reset this timer
- There is a maximum of ten thousand events per report or log
- Only the administrator who created the report can view them

Scheduled Reports

Newer Reports

- Each administrator can configure up to 100 scheduled reports
- Any administrator who has access can view the reports
- Reports are sent in the language of the Sophos Central Admin Account you have configured

SOPHOS

Newer reports do not have the same restrictions as the legacy format.

- Each administrator can configure a maximum of one hundred scheduled reports. This means you can have up to one hundred reports for all of the features that use this report format
- Any administrator who has access can view the reports
- Reports are sent in the language of the Sophos Central Admin account you have configured

DLP Events

The screenshot shows the Sophos Central interface with the 'DLP Events' section selected. On the left, there's a sidebar with 'SOPHOS' branding and links for Dashboard, Alerts, Threat Analysis Center, Log & Reports (which is highlighted), People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for 'MY PRODUCTS' (Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management) and 'RECENT ACTIVITY'. The main content area is titled 'Data Loss Prevention Events Log' and shows a table of events. At the top of this table are filters for 'Event name' (with a search bar and dropdown for 'Choose period' showing 'Last 90 days'), 'Hide Filters', and an 'Update' button. There are two filter panels: 'Filter by rule name' (with checkboxes for 'Rules (3)', 'Plain text files (1)', 'Plain Text Files (1)', and 'Private and Confidential (1)') and 'Filter by file type' (with checkboxes for 'File types (1)' and 'Plain text (3)'). The table has columns for DATE AND TIME, USER, DEVICE, RULE NAME, RULE ACTION, FILE NAME, and DESTINATION TYPE. It lists three events: one where a plain text file was allowed, one where a private and confidential file was blocked, and one where a plain text file was blocked. A note at the bottom says 'Displaying 3 Events.'

Date and Time	User	Device	Rule Name	Rule Action	File Name	Destination Type
Jul 27, 2022 11:32:38 AM	TRAININGDEMO\admi...	WinClient1	Plain text files	User allowed	My details (2).txt	application
Jul 27, 2022 11:31:39 AM	TRAININGDEMO\admi...	WinClient1	Private and Confidential	Blocked	My details.txt	application
Jul 26, 2022 11:30:27 AM	TRAININGDEMO\admi...	WinClient1	Plain Text Files	Blocked	My details.txt	application

The Data Loss Prevention (DLP) Events Log displays all events triggered by data loss prevention rules for devices.

The log allows you to search for specific events of a user, device or rule name over a specific time period.

The log displays the data and time of the event along with the user, the device, the rule name and file action. It will also include the name of the file that caused the event.

As with all reports and logs, you can export this report, and like the event log you can save customized reports for re-use.

Please note that a device can send a maximum of 50 data control events per hour to Sophos Central. All events are logged locally on the device.

Audit Logs

The screenshot shows the Sophos Central interface with the 'Audit Log' report selected. The top navigation bar includes 'Help', 'Simon Smith - Sophos UN - Super Admin', and a 'Logout' button. The left sidebar has sections for 'Sophos Central' (Dashboard, Alerts, Threat Analysis Center, Log & Reports), 'People', 'Devices', 'Global Settings', 'Third-party Connectors', 'Protect Devices', and 'Account Health Check'. Under 'My Products', there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, and Firewall Management. The main content area is titled 'Audit Log' with tabs for 'Reports' and 'Audit Log'. It features a search bar, date range filters ('From: Aug 1, 2022' to 'To: Aug 23, 2022'), and an 'Update' button. A note says 'Specify date range within past 90 days'. The table lists audit events:

Date	Modified By	Item Type	Modified
Aug 23, 2022 3:39:10 PM	[REDACTED]@sophos...	Users And Groups	[REDACTED]@sophostraining.xyz
Aug 23, 2022 3:37:58 PM	[REDACTED]@sophos...	Data Lake	Computer Settings
Aug 23, 2022 3:37:58 PM	[REDACTED]@sophos...	Data Lake	Computer Settings
Aug 23, 2022 3:31:01 PM	[REDACTED]@sophos...	Data Lake	Computer Settings
Aug 23, 2022 3:31:01 PM	[REDACTED]@sophos...	Data Lake	Computer Settings
Aug 23, 2022 3:04:39 PM	ssmith@sophostraining...	Events	Report type: EVENT, name: Week Malware Report
Aug 23, 2022 2:11:06 PM	ssmith@sophostraining...	Authentication	ssmith@sophostraining.xyz
Aug 23, 2022 2:11:06 PM	ssmith@sophostraining...	Authentication	2nd Work Mobile
Aug 23, 2022 2:10:43 PM	ssmith@sophostraining...	Authentication	ssmith@sophostraining.xyz
Aug 23, 2022 2:10:43 PM	ssmith@sophostraining...	Authentication	ssmith@sophostraining.xyz
Aug 23, 2022 2:10:41 PM	ssmith@sophostraining...	Authentication	ssmith@sophostraining.xyz

You can review and export a record of all activities that are monitored by Sophos Central using the audit log report.

All activities for the past seven days are shown in the audit log by default, however, you can view all activities for up to 90 days and export the report.

For accurate audit logging, ensure that admin accounts are not shared.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!

Question 1 of 3

Which report allows you to filter the event type?

Audit Log

Events Report

Computer Report

User Report

Question 2 of 3

Select the file formats a log or report can be exported to?

HTML

CSV

PDF

DOC

?

Question 3 of 3

How long in months will scheduled reports expire?
(Enter a numerical value)

SOPHOS

Chapter Review

The available logs and reports will **depend on your licensed products**.

The events report **details all events** across all protected devices.

Reports can be **customized and saved** to be run at regular intervals.

SOPHOS

Here are the three main things you learned in this chapter.

The available logs and reports will depend on your licensed products.

The events report details all events across all protected devices.

Reports can be customized and saved to be run at regular intervals.



Getting Started with Sophos Central Health Checks

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4010: Getting Started with Sophos Central Health Checks

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Health Checks

In this chapter you will learn how to check the health of your protected devices. You will learn which tools are available in Sophos Central to help maintain security health.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

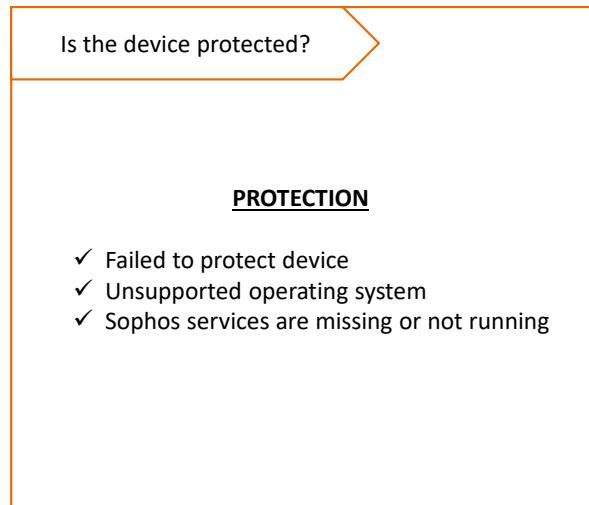
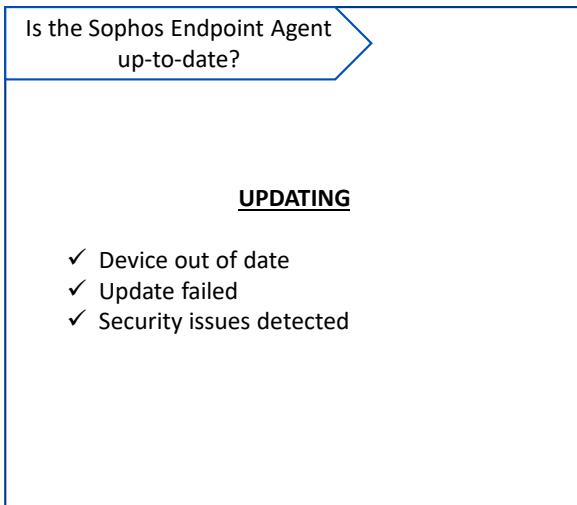
- ✓ How to access and navigate Sophos Central
- ✓ How to manage and protect devices with Sophos Central
- ✓ How to view logs and reports

DURATION **11 minutes**

SOPHOS

In this chapter you will learn how to check the health of your protected devices. You will learn which tools are available in Sophos Central to help maintain security health.

Protection Health Check



SOPHOS

We recommend that you review the protection and health of all protected devices as regularly as possible.

Ensure that all protected devices are up-to-date and are reporting into Sophos Central. If you do have devices that are not reporting back, ensure you know the reason why.

To review the protection of your devices, evaluate both the update and protection status of all devices.

- Are they able to update successfully?
- Are there any devices that are out-of-date?
- Is the update failing on any devices?
- Have any security issues been detected?

The devices report allows you to review the protection of your devices in one place, you can filter the report by health status allowing you to focus on those with a bad health status in the first instance.

Check your device protection to ensure that:

- An installation has not failed
- Sophos services are running
- There are no errors returned
- A device is not running on an unsupported operating system
- Central management has not been overridden on a device
- The security heartbeat is not missing or failed

These issues will be shown as alerts in Sophos Central if they require manual intervention to resolve.

Protection Health Check



How often?

- As part of a detection investigation
- When remediating events and alerts
- As frequently as possible

SOPHOS

So, how often should you be running health checks?

We recommend that if you are investigating a detection, you should be checking on the overall health of all protected devices.

Additionally, when you are remediating events and alerts. Health checks should be carried out as frequently as possible to ensure security.

Recommended Health Check Steps

Ensure that there are **no exclusions for exploits**

Global Settings > System Settings > Exploit Mitigation Exclusions

Check your **Global exclusions**. Specifically, exclusions for paths such as C:\Windows\Temp

Check your **endpoint and server threat protection policies**. Are there any local policy exclusions that have been applied to directories such as \\AppData\\Local\\Temp

Check the **Malware and PUAs blocked report** for patterns, particularly for re-detected malware

SOPHOS

It is worth working through the following steps regularly to ensure security.

Ensure that no exploit exclusions have been turned on in Sophos Central. If an exclusion has been applied, an exploit will not be detected and is able to exploit your network.

Check your global exclusions, particularly exclusions to paths such as C:\\Windows\\Temp or other common directories. If an attacker has access to common directories, it makes it easier to move through your network.

Check the threat protection policies for local exclusions that may have been applied to resolve an intermittent issue and not removed.

Check the Malware and PUAs blocked report in Sophos Central. This report is useful in determining patterns, particularly if malware is being re-detected across your network.

Device List

Easily see if Tamper Protection is enabled for protected computers and servers

Computer Name	Protection	Encryption	Last user	Last action	Group	Tamper protection
DB-1	✓ Intercept X Advanced with XDR	+	rebeccacook	Nov 8, 2022 3:17 PM		On
macOS Monterey 12.6	✓ Intercept X Advanced with XDR	+	Sophos	Nov 7, 2022 5:15 PM	Office Workers	Off
Windows 10 Pro	✓ Intercept X Advanced with XDR	+	Training	Nov 6, 2022 6:04 PM	Reading Office	Off
Windows 10 Enterprise	✓ Intercept X Advanced with XDR	+	TrainingAdmin	Nov 4, 2022 4:57 PM		Off
Windows 10 Pro	✓ Intercept X Advanced with XDR	+	TrainingAdmin	Nov 4, 2022 4:58 PM		On
Windows 10 Pro	✓ Intercept X Advanced with XDR	+	enable	Nov 4, 2022 4:58 PM		On
Windows 10 Pro	✓ Intercept X Advanced with XDR	+	Sophos	Nov 4, 2022 4:17 PM	Sales Operations	On
Windows 10 Pro	✓ Intercept X Advanced with XDR	+	administrator	Nov 4, 2022 4:07 PM		Off
Windows 10 Enterprise	✓ Intercept X Advanced with XDR	+	stan	Oct 18, 2022 5:46 PM		On

To assist with health checks, there are a number of built in features that will alert you to any issues.

For example, on the **Devices** page, a ‘Tamper protection’ column is included that indicates if Tamper Protection is enabled or disabled for protected devices.

Device List

The screenshot shows the Sophos Central interface with the 'Devices' section selected. On the left, there's a sidebar with various product categories like Support Protection, Server Protection, and Endpoint Protection. The main area is titled 'Computers' and shows a list of 11 devices. A dropdown menu is open over the first device, listing three filter options: 'Show all computers', 'Computers with a medium or bad status', and 'Computers with a bad status'. A green callout box to the right of the dropdown says 'Filter the device page to display on devices that need attention'. The table columns include Device Name, Protection Type, Last User, Last Action, Group, and Tamper protection.

Device Name	Protection Type	Last User	Last Action	Group	Tamper protection
DS-3	Intercept X Advanced with XDR	rebeccacook	Nov 8, 2022 3:17 PM		On
macOS Monitor	Intercept X Advanced with XDR	Sophos	Nov 7, 2022 5:15 PM	Office Workers	Off
Windows 10 Pro	Intercept X Advanced with XDR	Sophos	Nov 6, 2022 6:04 PM	Reading Office	Off
Windows 10 Enterprise	Intercept X Advanced with XDR	Training	Nov 4, 2022 4:57 PM		On
Windows 10 Pro	Intercept X Advanced with XDR	TrainingAdmin	Nov 4, 2022 4:58 PM		On
Windows 10 Pro	Intercept X Advanced with XDR	enable	Nov 4, 2022 4:58 PM		On
Windows 10 Pro	Intercept X Advanced with XDR	Sophos	Nov 4, 2022 4:57 PM	Sales Operations	On
Windows 10 Pro	Intercept X Advanced with XDR	administrator	Nov 4, 2022 4:57 PM		Off
Windows 10 Enterprise	Intercept X Advanced with XDR	stan	Oct 18, 2022 5:46 PM		On

The protected computer and server pages can be filtered to show only those devices with a medium or bad status, only a bad status, and those devices that have Tamper Protection disabled.

This allows you to filter the device page to show only those devices that require attention.

Device List

The screenshot shows the Sophos Central interface under the 'Computers' tab. A context menu is open over a selected device, specifically a Windows 10 Pro computer. The menu item 'Turn on tamper protection' is highlighted with a red box and an arrow pointing to it. The menu also includes options like 'Reset health status' and 'Delete'. The main table lists various devices with columns for Protection, Encryption, Last user, Last action, Group, and Tamper protection status.

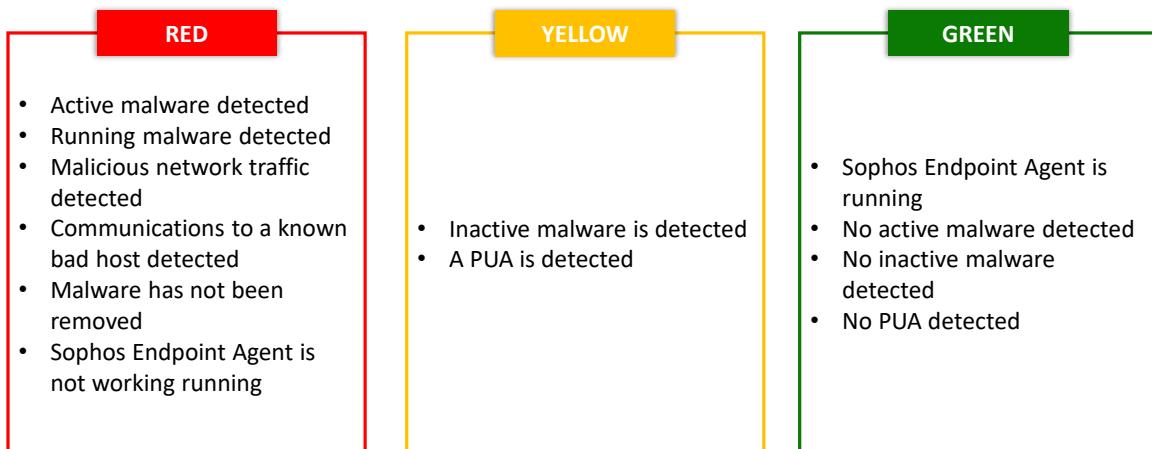
OS	Protection	Encryption	Last user	Last action	Group	Tamper protection
macOS Monterey	Intercept X Advanced with XDR	enable	Sophos	Nov 8, 2022 3:17 PM	Office Workers	On
Windows 10 Pro	Intercept X Advanced with XDR	Sophos	Nov 4, 2022 4:17 PM	Reading Office	Off	
Windows 10 Enterprise	Intercept X Advanced with XDR	administrator	Oct 12, 2022 5:46 PM	Sales Operations	Off	
Windows 10 Pro	Intercept X Advanced with XDR	stan	Oct 12, 2022 5:46 PM	Marketing	On	

Selecting a device from the list will show additional options that help manage and remediate devices.

For remediation, this means you can easily turn on Tamper Protection if it is turned off and reset the health status of a device.



Device Health Status



SOPHOS

The health status of protected devices is important as it can indicate that a device has been compromised.

If a device is showing with a red status, it can indicate that active or running malware has been detected, that malicious network traffic has been detected or communications with a known bad host. It can also indicate that malware has not been removed automatically, or that the Sophos Endpoint Agent is not running.

If a device is showing with a yellow status, it can indicate that inactive malware has been detected or that a PUA has been detected.

A device with a green status is considered healthy. The Sophos Endpoint Agent is running with no errors, there is no active or inactive malware detected, and no PUAs have been detected

[Additional Information]

For further information regarding the health status of devices please see knowledge base article **KB-000035572**. <https://support.sophos.com/support/s/article/KB-000035572>

Device Health Status

The screenshot shows the Sophos Central interface for managing device health. On the left, there's a sidebar with 'SOPHOS' branding and various navigation links like 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', and 'Devices'. The 'Devices' link is highlighted. The main area is titled 'Computers' with a sub-section 'View device usage from computers'. At the top, there are tabs for 'Computers' (selected), 'Servers', 'Mobile Devices', and 'Unmanaged devices'. Below the tabs are buttons for 'Manage Endpoint Software', 'Turn on temporary protection', 'Recover Recovery Key', 'Reset health status' (which is highlighted with a red box and has an orange arrow pointing to it), and 'Delete'. There are also dropdowns for 'All Computers', 'Show all computers', 'Any protection type', and 'Recently'. A table lists 10 selected devices, each with a small icon, a name, and a protection status (e.g., Intercept X Advanced with XDR). The table footer says '10 / 10 computers / 2 selected'. To the right of the table is a modal window titled 'Reset health' with the following content:

- Reset health status on the 3 selected devices
- This resets the health status of these devices and clears current alerts for these devices in Sophos Central. It also prompts the devices to dismiss any malware issues locally.
- The reset does not affect protection.
- If the device has underlying issues, it might return to its current health status.
- This reset only applies to up-to-date Windows and Linux devices. Devices running old software or other operating systems ignore it.

At the bottom of the modal are 'Cancel' and 'Reset' buttons.

You can reset the security health status of selected devices to green or ‘healthy’.

It is important to note that resetting the health status of a device does not clean up threats or fix software issues. A health status reset will clear the alerts for a device in Sophos Central and in the Sophos Endpoint Agent.

A health reset should be done if you want to clear old issues and focus on a current issue or future issues. Devices that are issue-free stay ‘healthy’ after the reset, so any current or future protection or malware issues will be more obvious.

To reset the health status, select the devices from the device list and click **Reset health status**. This doesn't affect protection, if a device has an issue that requires action, the status of the device will return to yellow or red to indicate a bad health status.

Please note that the option to reset the health status is not available for macOS devices.

Malware Health Check

The screenshot shows the Sophos Central interface with the 'Logs & Reports' menu selected. A green callout box highlights the 'Select:' section, which contains three checked items: 'Runtime Detections' and 'Malware'. A blue arrow points from this section to the main report area. The report title is 'Events Report' with a subtitle 'Reports - 6 events Report'. It includes filters for 'Search by Computer or user in threat' and 'Choose period: Last 90 days'. Below these are sections for 'Show all severity types', 'Search by User Group', and 'Search by Computer or Server Group'. A bar chart shows event counts over time, with a peak around August 31st. The main table lists four malware detection events from October 18th, 2022, at 10:48 AM, each involving the file 'EICAR-AV-Test'. A blue callout box on the right side of the report area states: 'What does it show? All detection events including cleaned-up malware'.

To check the malware health of your estate, you can filter the **Events Report** to display only runtime detections and malware events, including malware that has been cleaned up automatically.

For example, if you have a compromised device that is trying to contact other devices on the network. You may see several malware events shown in this report which could indicate that there is something on the device that needs manual investigation to remediate.

Optionally you can select to include potentially unwanted applications in the report. This can be useful, as attackers can make use of applications to exploit a device.

Device Health Status

The health status of any protected device is displayed in Sophos Central on the device page. On the **Events** tab, you can view the events that have taken place on the device. In this example, malware and malicious behaviour was detected and cleaned up on this device.

Account Health Check – Protection Installed

The screenshot shows the Sophos Central interface with the 'Account Health Check' page selected. The left sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Connectors, Protect Devices, and Account Health Check (which is highlighted). Below that is a 'MY PRODUCTS' section with links for Endpoint Protection, Server Protection, Mobile, Encryption, and Wireless. The main content area is titled 'Account Health Check' and includes a message about checking for issues to fix. It features a 'Protection installed' section with two cards: 'Endpoint protection' (12 of 12 endpoints have all your licensed protection installed) and 'Server protection' (18 of 18 servers have all your licensed protection installed). Below this are sections for Tamper protection, Policies, and Exclusions.

The **Account Health Check** page is split into sections that display any settings used that could mean your security is vulnerable.

Let's have a look at the currently available sections. Firstly, the 'Protection installed' section which checks whether all of the licensed protection software is installed on all protected devices. If Account Health Check warns that devices do not have all the licensed protection software installed, you can select to fix the issue automatically or manually.

Account Health Check – Tamper Protection

The screenshot shows the Sophos Central interface with the 'Account Health Check' section selected. The main content area is titled 'Tamper protection'. It displays three status cards:

- Endpoint tamper protection:** Shows 5 of 12 endpoints have tamper protection turned off. A 'Tell me how to fix' button is present.
- Server tamper protection:** Shows 4 of 18 servers have tamper protection turned off. A 'Tell me how to fix' button is present.
- Global tamper protection:** Shows Tamper protection is turned on for your computers and servers. This card has a green checkmark icon and a descriptive message.

A green callout bubble points to the 'Global tamper protection' card with the text: "Ensure Tamper Protection is enabled globally. Check each device to understand why Tamper Protection is disabled".

Left sidebar (My Products):

- Endpoint Protection
- Server Protection
- Mobile
- Encryption
- Wireless

Bottom navigation bar:

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports
- People
- Devices
- Global Settings
- Third-party Connectors
- Protect Devices
- Account Health Check (selected)

The ‘Tamper Protection’ section indicates if any endpoints or servers have Tamper Protection turned off. The health check will also check the global setting for Tamper Protection.

If the global setting is disabled, it needs to be enabled before you can enable Tamper Protection for individual devices. We recommend checking those devices that have Tamper Protection disabled to understand why as without this protection, devices are more vulnerable to attack.

Account Health Check – Tamper Protection

The screenshot shows the Sophos Central interface. On the left sidebar, under 'MY PRODUCTS', 'Endpoint Protection' is selected. The main content area has two sections: 'Endpoint tamper protection' (status: 5 of 12 endpoints have tamper protection turned off) and 'Global tamper protection' (status: Tamper protection is turned on for your computers and servers). A red box highlights the 'Tell me how to fix' button in the Endpoint tamper protection section. An orange arrow points from this button to a detailed guide on the right titled 'Fix endpoint tamper protection'. The guide includes a warning about account health checks, steps to identify affected computers, and a screenshot of the 'Account Health Check' page with a yellow box around the 'Scan now' button.

Clicking on the ‘Tell me how to fix’ button will re-direct you to the help documentation where you can find instructions on how to resolve the issue that has been identified.

Account Health Check – Policies

The screenshot shows the Sophos Central interface with the 'Account Health Check' page selected. The left sidebar lists 'Sophos Central' and 'My Products' sections. The main content area is titled 'Account Health Check' and includes a message about checking for issues to fix. Below this are three sections: 'Protection installed', 'Tamper protection', and 'Policies'. The 'Policies' section is expanded, showing two items: 'Endpoint Threat Protection policy settings' (with a red warning icon) and 'Server Threat Protection policy settings' (with a green checkmark icon). Each item has a sub-section indicating the number of policies checked against recommended settings. A 'Tell me how to fix' button is visible at the bottom of the policies section.

The ‘Policies’ section checks your configured endpoint and server policies. A red warning is displayed in the policies section of the account health check if a policy setting differs from Sophos’ recommended settings. The recommended settings offer the best security. If you must change settings to fix issues, change as few as you can and apply them to as few devices as you can.

A ‘Tell me how to fix’ button displayed will re-direct you to the help page which provides instructions on how to resolve the issue identified.

Account Health Check – Exclusions

The screenshot shows the Sophos Central interface with the 'Account Health Check' selected in the sidebar. The main content area is titled 'Policies' and displays three categories of exclusions:

- Endpoint Policy Exclusions:** 1 of 3 endpoint policies have exclusions causing one or more significant security risks. A 'Tell me how to fix' button is present.
- Global Exclusions:** 1 global exclusion is causing one or more significant security risks. A 'Tell me how to fix' button is present.
- IT Group Exceptions:** This policy has 1 exclusions causing significant security risks. A 'PsExec' button is present.

The ‘Exclusions’ health check will review all policy and global exclusions configured. Should an exclusion be identified as a security risk it will be highlighted here. You will also see a banner message in the policy and against the exclusion entry in global exclusions.

Whilst we do not prevent you adding exclusions that pose a serious security risk, we do highlight the risk when you add the exclusion, when you view the exclusion either in a policy or globally, and in the health check. We encourage you to review all exclusions regularly to ensure that they are relevant and only applied to those users that require them.

Please note that additional health checks may be added in future versions of Sophos Central.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

What happens when the health status of a device is reset?

All threats are cleaned up

A full system scan is initiated on the device

All alerts are cleared and the health status is set to green/healthy

Any software issues are resolved

SOPHOS



Question 2 of 3

True or False: You can reset the health status for Windows endpoints only.

True

False

SOPHOS



Question 3 of 3

Match the expected device health status to the symptoms.

YELLOW

DROP

No malware has been detected

RED

DROP

Inactive malware has been detected

GREEN

DROP

Active malware has been detected

SOPHOS

Chapter Review

To review the protection of your devices, **evaluate both the update and protection status** of all devices.

Health checks should be carried out as frequently as possible, including following detection investigations and remediating events and alerts.

Resetting the health status of a device **clears alerts for the device**.
It **does not** clean up threats or fix software issues.

SOPHOS

Here are the three main things you learned in this chapter.

To review the protection of your devices, evaluate both the update and protection status of all devices.

Health checks should be carried out as frequently as possible, including following detection investigations, and remediating events and alerts.

Resetting the health status of a device clears alerts for the device in Sophos Central and locally. It does not clean up threats or fix software issues.



Getting Started with Sophos Central Alerts and Events

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4020: Getting Started with Sophos Central Alerts and Events

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Alerts and Events

In this chapter you will learn how to view and manage Sophos Central events and alerts, and how to configure email alerts for administrators.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Access and navigate Sophos Central
- ✓ Protect and manage devices with Sophos Central

DURATION

13 minutes

SOPHOS

In this chapter you will learn how to view and manage Sophos Central events and alerts, and how to configure email alerts for administrators.

Alerts and Events



Events are logged for **ALL detections** including clean up



Alerts are **ONLY** created when **ACTION IS REQUIRED**

SOPHOS

The Sophos Endpoint Agent will detect and clean up malicious and suspicious items. The threat protection features will protect your network from multiple various attacks.

Sophos Central allows you to view exactly what has happened across the network. It does this by logging all events and creating alerts so that administrators are alerted to any behaviour that is not safe. Events are logged for ALL detection events, including clean up events.

It is important to understand that to prevent the dashboard being flooded with information, alerts are only shown when an action is required. What the subsequent actions are, will depend on the alert.



Event Types

Informational	Medium	High
<ul style="list-style-type: none">• No action required• Examples:<ul style="list-style-type: none">• Malware cleaned up• Updated succeeded	<ul style="list-style-type: none">• Action required• Examples:<ul style="list-style-type: none">• Detections that are automatically remediated• Policy non-compliance• Reboot required	<ul style="list-style-type: none">• Action required• Examples:<ul style="list-style-type: none">• Detection that requires manual intervention• API token expiry• Real-time protection disabled

SOPHOS

There are three event types in Sophos Central.

Informational events are logged for reference and require no action. For example, when a detection has been cleaned up or a device has updated successfully.

Medium severity events are logged when action is required. For example, when a device is out of compliance or requires a reboot. Malware detections that are automatically remediated are reported as medium events, however, these events are only displayed until the detection has been cleaned up.

High severity events are logged when action is required and will remain in the event lists until they are remediated or acknowledged by a Sophos Central administrator. This can include detections that require manual intervention or further investigation, API tokens expiring, or disablement of real-time protection.

Please note that not all medium and high events will generate an alert for the event. For example, when a reboot is required, an alert is only triggered if the reboot is not performed within two weeks of the event.

[Additional Information]

For further information about alerts please see knowledge base article **KB-000038134**:
<https://support.sophos.com/support/s/article/KB-000038134>

Events

The screenshot shows the Sophos Endpoint Protection interface for a computer named 'Training-W10'. The left sidebar has a 'Computers' section selected. The main area is titled 'Endpoint Protection - Training-W10' and shows the 'Events' tab is active. A summary bar indicates '0 events' from Aug 2, 2022, to Oct 31, 2022, with a note about 'Outbreaks since Aug 2, 2022'. Below is a table of events:

Severity	Date	Description	Action
Outbreak detected	Oct 31, 2022 12:18 PM	Outbreak detected	Details
Informational	Oct 31, 2022 12:18 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Medium	Oct 31, 2022 12:17 PM	Malware detected: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:17 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:18 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:18 PM	Malware detected: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:15 PM	Malware detected: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:15 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:14 PM	Malware detected: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:14 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:13 PM	Malware cleaned up: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details
Informational	Oct 31, 2022 12:13 PM	Malware detected: 'EICAR-AV-Test' at 'C:\Users\Training\Downloads\ieicar.txt.com'	Details

387 Events

The **Events** tab for a computer or server lists all events, and the icon next to the event shows the severity. In this example the severity of the first three lines are:

- High as the volume of events indicates an outbreak
- Informational confirming the malware was cleaned up
- And medium, the malware detection

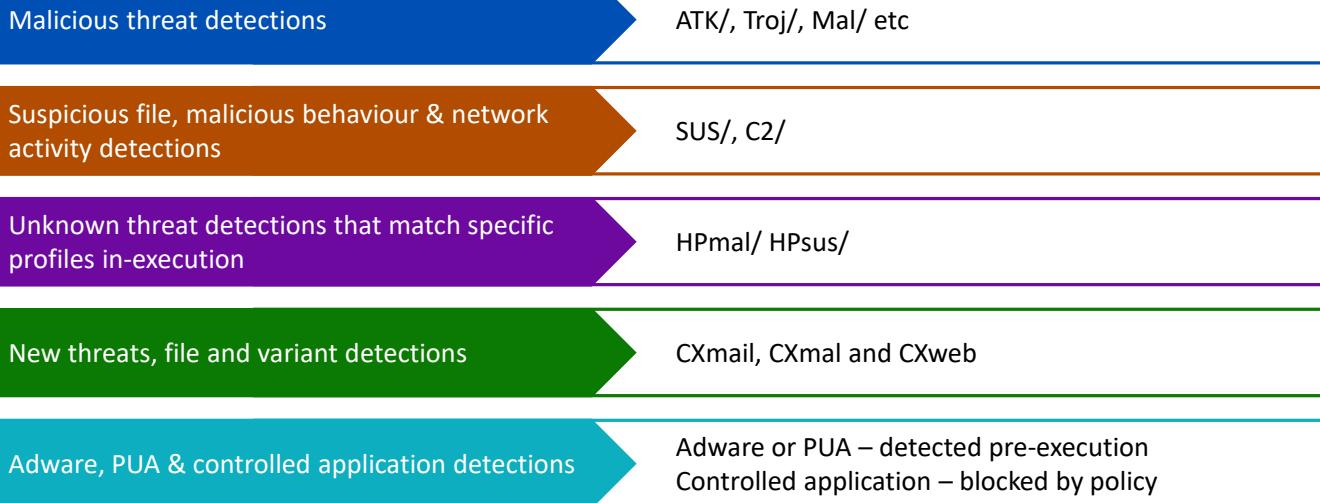
Event Details

The screenshot shows the Sophos Endpoint Protection interface. On the left, there's a sidebar with navigation links like 'Dashboard', 'Logs & Reports', 'Profile', and 'Computers' (which is currently selected). The main area displays a list of detected items. One item is highlighted with a red border, and its 'Details' link has also been clicked, opening a detailed view. This dialog box contains information such as the detection name ('EICAR-AV-Test'), SHA-256 hash ('SHA-256: 775e0211abf64893e54d471988f7bb9d1663fc820ec2fe2a2c4538aaef6337fd8'), and the file path ('Path: C:\Users\Training\Downloads\testcalc.txt.com'). It also includes sections for allowing the application ('Allow this application') and adding comments ('Comments'). A 'Details' link at the bottom right of the dialog box is highlighted with a red box.

Clicking on the **Details** link for the malware detection event provides more information, and the option to allow the application. This action should be taken with great caution and only if you are certain that the detected item is safe to allow.



Detection Types



SOPHOS

All detection events will display the detection type. It is useful to understand the type of detections you may see in order to know how best to remediate the threat. Let's take a quick look at the main types of detections.

Malicious threats will typically be detected by the on-access scanner using definitions.

Suspicious detections are based on properties of the scanned file which determine if it is malicious. Malicious behaviour detections are triggered when an application performs actions that are classed as malicious. C2 detections are returned if malicious network traffic has been detected.

Unknown threats are detections that match specific combinations of behaviours when running that indicate malicious intent. Unknown threats will be displayed as HPmal or HPsus detections.

CXmail detections are email born threats, CXweb detections are malicious files detected before a download takes place, and CXmal detections are threats that are detected in-execution.

Adware and PUA detections are detections of applications that may be legitimate, however, they can pose a risk. Controlled application detections are legitimate applications that are being blocked by the application control policy.

[Additional Information]

Comparison of Sophos's malicious file detection technologies **KB-000034084**.

<https://support.sophos.com/support/s/article/KB-000034084>

Most Recent Alerts

The screenshot shows the Sophos Central Dashboard. On the left is a sidebar with navigation links like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Online Settings, Third-party Connectors, Protect Devices, and Account Health Check. Below that is a section for 'My Products' with icons for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, and Firewall Management.

The main dashboard area has a title 'Sophos Central Dashboard' with a subtitle 'See a summary of your existing protection'. It features four large status indicators: '4 Total Alerts' (blue), '3 High Alerts' (red), '0 Medium Alerts' (yellow), and '1 Low Alerts' (green). Below these are sections for 'Most Recent Alerts' (listing four entries with dates and descriptions like 'Outbreak detected' and 'Real-time protection disabled') and 'Devices and users: summary' (showing endpoint activity status with 1 Active and 0 Inactive for Month).

On the right side, there are two boxes: 'Web control' (0 Web Threats Blocked) and 'Policy Violations Blocked' (54 Policy Violations Blocked). Top right corner shows user info: Stephen UK - Senior Admin and Help, Training, and Support links.

The **Dashboard** lists the most recent alerts, showing events that require attention.

Alerts

The screenshot shows the Sophos Central interface with the 'Alerts' tab selected. At the top, there are four summary cards: 'Total Alerts' (4), 'High Alerts' (3), 'Medium Alerts' (0), and 'Low Alerts' (1). Below these are filtering options ('Filter By: All products', 'All categories') and a 'Group' toggle. A table lists four alerts with columns for Description, Count, and Actions. Each alert has an 'Actions' button with two options: 'Mark As Resolved' and 'Reinstall Endpoint Protection'. The last three rows of the table are highlighted with a red border.

Description	Count	Actions
Cabinet detected	1	Mark As Resolved
Firewall connection to Sophos Central has been restored	1	Mark As Acknowledged
Real-time protection disabled	1	Mark As Acknowledged Reinstall Endpoint Protection
Real-time protection disabled	1	Mark As Acknowledged Reinstall Endpoint Protection

The **Alerts** page provides more details about each alert, which can be accessed by clicking the arrow next to it.

It also shows the **Actions** that can be taken for the alerts listed.

Actions

Actions available for alerts, depending on the alert type

- **Mark As Acknowledged** removes an alert from the list but does not remove threat details from the quarantine manager
- **Mark As Resolved** clears the alert from the list in Sophos Central and clears the threat details from the quarantine manager
- **Clean Up** removes the detected item
- **Reinstall Endpoint Protection** re-directs to the ‘Protect Devices’ page
- **Contact Support for additional help**
- **Authorize PUA** allows a Potentially Unwanted Application to run on all computers

SOPHOS

The following actions are available for alerts, depending on the alert type and the type of device the alert applies to.

- **Mark As Acknowledged** removes an alert from the list but does not remove threat details from the quarantine manager
- **Mark As Resolved** clears the alert from the list in Sophos Central and clears the threat details from the quarantine manager on the computer or server. Please note that the actions ‘Mark As Acknowledged’, and ‘Mark as Resolved’ do not resolve the threats, they simple resolve and acknowledge the alert
- **Clean Up** removes the detected item
- **Re-install Endpoint Protection** re-directs you to the Protect Devices page, for download of the Sophos agent software
- **Contact Support for additional help.** This action becomes available, for example when malware cleanup fails
- **Authorize PUA** allows a Potentially Unwanted Application to run on all computers



Additional information in
the notes

Alert Details

<input type="checkbox"/>	! Outbreak detected	Oct 31, 2022 12:16 PM	TRAINING-W10\Training	Training-W10	^
	<p>Description: Outbreak detected</p> <p>More information: We made more than 100 detections in 24 hours. We won't report further detections in the events list but we'll still block malware and PUIAs on the computer.</p> <p>What you need to do: Investigate the cause of the outbreak. When you believe you've resolved the situation, go to the alert and mark it as resolved.</p>	<p>Endpoint Type: Computer</p> <p>OS: Windows</p> <p>User: TRAINING-W10\Training</p> <p>Device: Training-W10</p>		<p>Actions:</p> <p>Mark As Resolved</p>	

<input type="checkbox"/>	! Real time protection disabled	Oct 31, 2022 2:20 PM	n/a	DC	^
	<p>Description: Real time protection disabled</p> <p>More information: We have tried to enforce the Sophos Central policy and enable real-time protection. If the computer is online but not accepting the policy, the Sophos endpoint software may not be working.</p> <p>What you need to do: Reinstall the Sophos endpoint software or investigate further in the logs on the endpoint.</p>	<p>Endpoint Type: Server</p> <p>OS: Windows</p> <p>User: n/a</p> <p>Device: DC</p>		<p>Actions:</p> <p>Reinstall Endpoint Protection</p> <p>Mark As Acknowledged</p>	

SOPHOS

Here we can see the details for two alerts.

An outbreak alert is automatically reported if a device experiences 100 detections in 24 hours.

The second alert shows that real-time protection has been disabled for a computer for more than 2.5 hours.

A description of all threat protection alerts, of high and medium severity, is included in the Sophos Central Admin Help.

[Additional Information]

<https://docs.sophos.com/central/Customer/help/en-us/ManageYourProducts/Alerts/AlertsMalware/index.html>

Alerts

The screenshot shows the Sophos Central interface with the 'Alerts' section selected. At the top, there are four summary cards: 'Total Alerts' (6), 'High Alerts' (4), 'Medium Alerts' (2), and 'Low Alerts' (0). Below these are filter options ('Filter By: All products', 'All categories') and a 'Ungroup' button (which is highlighted with a red box). The main list displays three alerts with checkboxes and actions: 'You must renew your API Token' (Count: 3, Action: 'Mark As Acknowledged'), 'Manual PUA cleanup required: "PsKill"' (Count: 2, Action: 'Mark As Resolved'), and 'Malware not cleaned up: EICAR-AV-Test' (Count: 1, Action: 'Mark As Resolved').

Description	Count	Action
You must renew your API Token	3	Mark As Acknowledged
Manual PUA cleanup required: "PsKill"	2	Mark As Resolved
Malware not cleaned up: EICAR-AV-Test	1	Mark As Resolved

Alerts can be filtered by product and alert category.

All alerts for a specific threat or event are grouped together under a single entry in the list which makes alerts easier to manage. You can select to ungroup the alerts if required.

The 'Count' column shows the number of alerts for each group entry. To view all alerts in a group, click the arrow on the right to expand the group section.

Default Email Alerts



Emails are sent for medium and high-level events that require action



Emails are sent to all administrators



Emails are **not** sent if an alert of the same type has been sent in the previous 24 hours

SOPHOS

Whilst administrators can view alerts when they log into Sophos Central, they may not always have Sophos Central open. Email alerts can be configured to notify administrators about specific alerts by product, severity or category.

By default, email alerts are sent for medium or high-level events that require action, and are sent to all administrator users. Email alerts are not sent if an alert for the same type of event has been sent within the previous 24 hours, this is to prevent notification flooding should an outbreak occur.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various navigation items like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected and highlighted in blue), Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are Endpoint Protection and Encryption sections. At the bottom of the sidebar, there are links for Malware Sample Submission and Sophos News. The main content area has several sections: 'See which items you've blocked and add or remove items.', 'Manage Update Caches and Message Relays', 'Enable your devices to get updates from a cache on the network and to communicate with Sophos Central through message relays.', 'Bandwidth Usage', 'Limit the bandwidth that Windows endpoints and servers use for downloading updates.', 'Configure email alerts' (which is highlighted with a red box), 'Manage email alerts for admins.', 'Encryption Recovery Key Search' (with a sub-note about getting a device encryption recovery key by entering a volume or recovery identifier), 'Admin Isolated Devices' (with a note about seeing which devices are isolated and removing them from isolation), and 'Forensic Snapshots'. To the right, there are sections for 'Manage M365 domain settings and view status', 'Post delivery protection', 'Manage post delivery automatic message removal', 'Data Loss Prevention' (with 'Rules' and 'Content Control Lists' sub-sections), 'Sophos Central Self Service' (with 'User Access' sub-section), and 'Zero Trust Network Access' (with a link to 'General Zero Trust Network Access settings'). A prominent dark blue bar at the bottom states 'Only Super Admin users can configure email alerts'.

Only users with the Super Administrator role can change the default email alert settings. To view the settings, navigate to **Global Settings > Configure email alerts**.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left, a sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected and highlighted in blue), Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are links for Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area is titled 'Configure email alerts' under 'Global Settings / Configure email alerts'. It has tabs for Administrators, Distribution Lists, Frequency, Custom rules, and Exceptions. The 'Administrators' tab is active. A sub-section titled 'Administrators' displays a list of users with their names, email addresses, and roles. To the right of each user is a 'Receiving alerts' column with a toggle switch. The first two users have 'No' selected, while the last two have 'Yes' selected. An orange box highlights this column.

Name	Email address	Role	Receiving alerts
Anne	anne@trainingdemo.xyz	Super Admin	No
Global Training	ztna-central@trainingdemo.xyz	Super Admin	Yes
Jako	jako@trainingdemo.xyz	Admin	No
Robert	robert@trainingdemo.xyz	Super Admin	Yes

The first step of configuring email alerts is to define which administrators should receive alerts. You can set who will receive email alerts from Sophos Central and who will not.

Simply toggle the receiving alerts button to yes or no to configure who receives alerts and who doesn't.

Configure Email Alerts

The screenshot shows the Sophos Central interface. The left sidebar is titled 'SOPHOS' and includes sections for 'Sophos Central', 'MY PRODUCTS', and 'Encryption'. Under 'Global Settings', the 'Email' tab is selected. The main content area is titled 'Configure email alerts' and shows the 'Distribution lists' tab selected. It displays a table with one row, showing an email address and its description. A blue button labeled 'Add email address' is visible. A dark blue banner at the bottom states: 'Distribution lists are **not available** for Sophos Central trial/evaluation accounts'.

Email address *	Description
globaltraining@...	global training shared inbox

You can add and manage distribution lists, allowing you to add the email addresses of your distribution lists, ticketing system, or people you want to notify about alerts who do not have Sophos Central Admin access.

Please note that the distribution list feature is not available for Sophos Central trial accounts.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left sidebar, under 'Global Settings', the 'Global Settings' option is selected. The main content area is titled 'Configure email alerts' and shows the 'Frequency' tab selected. It includes sections for 'Notification frequency' and 'Set by severity'. A dropdown menu for 'High alert' is open, showing options: 'Immediately', 'Hourly', 'Daily', and 'Never'. A 'Save' button is visible in the top right corner.

The frequency of when email alerts are sent can be configured by either severity, product, or category.

Selecting to send email alerts by severity allows you to configure how often an alert is sent based on its severity. You can select from immediately, hourly, daily, or never for high, medium, and informational alerts.

It is good practice to configure high alerts to be emailed immediately so that administrators are able to respond to events quickly. Similarly, you may decide that informational alerts do not need an email notification and set these to never send an alert.

Configure Email Alerts

The screenshot shows the Sophos Central interface with the 'Global Settings' tab selected. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, etc. The main area is titled 'Configure Email Alerts' and contains a section for 'Set by product'. It lists several products with dropdown menus for 'Send alert' frequency. A dropdown menu for 'Firewall' is open, showing options: Immediately, Hourly, Daily, and Never. A 'Restore sophos default settings' button is also visible.

Product	Send alert
Cloud Switch	Immediately
Email Gateway	Immediately
Encryption	Immediately
Endpoint	Immediately
Firewall	Immediately Hourly Daily Never
Mobile	Immediately
Phish Threat	Immediately
Server	Immediately
Sophos Central	Immediately
Web Gateway	Immediately
Wireless	Immediately
Zero Trust Network Access	Immediately

Setting the alerts by product allows you to control how often alerts are sent for each licensed product.

Configure Email Alerts

The screenshot shows the Sophos Central interface with the 'Global Settings' tab selected in the sidebar. The main area displays a table of alert categories and their corresponding send alert frequency options. A dropdown menu for 'Cloud Switch Events' is open, showing options: Immediately, Hourly, Daily, and Never. A note at the top says 'Set by category' and 'Set the frequency depending on the category of alert'. A button to 'Reset Sophos default settings' is also visible.

Category	Products Affected	Send alert
Active Directory Synchronization	Sophos Central	Immediately
App Reputation	Endpoint, Server	Immediately
Cloud Switch Events	Cloud Switch	Immediately Hourly Daily Never
Connectivity	Firewall	Immediately
Device Encryption	Encryption	Immediately
Forensic Snapshot	Endpoint, Server	Immediately
General	Sophos Central	Immediately
Malware	Endpoint, Server	Immediately
Managed Threat Response	Endpoint, Server	Immediately
Mobile Control	Endpoint, Secure Mobile	Immediately

You can only select one notification frequency type, **severity, product or category**

Alerts set by category splits alerts into the event categories. You can then configure how often alerts are received per alert category. For example, you can configure malware alerts to be sent immediately, whilst general Sophos Central alerts are sent daily or hourly.

Remember, you can only select one notification frequency type, by severity, product or category.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is selected and highlighted in blue). Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area is titled "Configure email alerts" and shows the "Custom rules" tab selected. It displays a message stating, "You can set custom email alerts rules that override your default settings for administrators or distribution lists." Below this, it says, "You don't currently have any custom rules" and features a blue "Create rule" button. At the top right of the main content area, there are links for Help, UK Training, and the user account (Sophos UK - Super Admin).

Custom rules allow you to specify alert notification settings for specific administrators or distribution groups. This is useful if you have a particular distribution group that you only want to receive malware alerts, or a help desk user that you only want to receive protection alerts for specific products.

To get started, click **Create rule**

Select the user role you want to create the custom rule for and then select the specific administrators with that role that you want to configure the rule for. Any distribution emails you have configured will also be displayed here.

Configure Email Alerts

The screenshot shows the Sophos Central interface with the 'Global Settings' option selected in the sidebar. The main content area is titled 'Alert Types' with the sub-instruction 'Choose the alert types that the rule will include.' Below this, there are three sections: 'Set by severity', 'Set by product', and 'Set by category'. In the 'Set by severity' section, three checkboxes are checked: 'High alert' (Daily), 'Medium alert' (Daily), and 'Info alert' (Never). The 'Set by product' and 'Set by category' sections also have checkboxes checked, though their details are less visible.

Once you have selected the administrators the rule will apply to, you will configure the type of alerts you want them to receive.

In this example, we are creating a custom rule for the help desk user. All severity alert types are selected, only server and endpoint products are selected and only those alert categories that relate to protection account creation and management of users and devices.

Configure Email Alerts

The screenshot shows the Sophos Central interface under 'Global Settings' in the left sidebar. The 'Email Alerts' section is selected. A banner at the top states: 'Using a custom rule will override any email alerts being sent to the recipients included in the custom rule'. Below this, a note says: 'You can set custom email alerts rules that override your default settings for administrators or distribution lists.' A blue button '+ Create new rule' is visible. The main area displays a single custom rule named 'Help Desk User Rules' with the following details:

Description:	Help Desk users responsible for administration tasks for protection issues.
Role:	HelpDesk
Administrators:	All
Distribution lists:	-
Notification methods:	Severity: All Product: Encryption, Endpoint, Server, Sophos Central Category: Active Directory Synchronization, Device Encryption, Forensic Snapshot, General, Malware, Managed Threat Response, Product Updates, Protection Issues, User Activity Verification, Virtualisation, Xgemail

A summary of all custom rules is displayed. The list is expandable to view the custom rule details. You can select to pause, edit, or delete any custom rules created.

Please note that using a custom rule will override any email alerts being sent to recipients included in the custom rule.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left, a dark sidebar lists various sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is selected). Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area has a title 'Configure email alerts' and a subtitle 'Global Settings / Configure email alerts'. It features a navigation bar with tabs: Administrators, Distribution Lists, Frequency, Custom rules, and Exceptions (which is highlighted). A section titled 'Exceptions' contains a note: 'The list below shows exceptions you have set up. You set them at the Alerts page to change the frequency of email alerts for certain alert types. You can edit them here.' Below this are three listed exceptions: 'Your APNs certificate was renewed' (Endpoint, Server, Mobile), 'Manual PUA cleanup required' (Endpoint, Server), and 'Malware not cleaned up' (Endpoint, Server). Each exception has a 'Send alert' dropdown menu open, showing options: Immediately, Hourly, Daily, and Never. The 'Immediately' option is highlighted.

Notification exceptions are configured on the **Alerts** page.

An email alert option is displayed for alerts that allows you to change the frequency of that alert. Once you have changed the alert frequency, that alert type will appear on the **Exceptions** tab in **Configure email alerts**.

You can then change the frequency of those exceptions on the **Exceptions** tab using the drop down menu.

Configure Email Alerts

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various menu items like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected and highlighted in blue), Protect Devices, and Account Health Check. Under 'MY PRODUCTS', there are Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area is titled 'Global Settings' and contains several sections: Bandwidth Usage, HTTPS Updating, a highlighted 'Configure email alerts' section (with a padlock icon), Encryption Recovery Key Search, Admin Isolated Devices, Forensic Snapshots, and Malware Sample Submission. To the right, there are sections for Mobile (Data Lake uploads), Data Loss Prevention (Rules, Content Control Lists), and Sophos Central Self Service (User Access).

and to communicate with Sophos Central through message relays.

Bandwidth Usage
Limit the bandwidth that Windows endpoints and servers use for downloading updates.

HTTPS Updating
Manage whether updating is performed using the secure HTTPS protocol.

Configure email alerts
Manage email alerts for admins.

Encryption Recovery Key Search
Get a device encryption recovery key by entering a volume or recovery identifier.

Admin Isolated Devices
See which devices you've isolated and remove them from isolation.

Forensic Snapshots
Configure forensic snapshots, which get data to help you investigate potential threats.

Malware Sample Submission

Mobile
Data Lake uploads
Control uploads to the Data Lake

Data Loss Prevention
Rules
Create rules to reuse across multiple policies.

Content Control Lists
Create content control lists to reuse across multiple policies.

Sophos Central Self Service
User Access
Manage users' access to Sophos Central Self Service.

It is important to note that email alerts can be configured globally by a Sophos Partner. In Sophos Central, you will see the padlock icon next to the **Configure email alerts** option in Global Settings.

If you select **Configure Email Alerts**, you will see a banner message explaining that the settings are controlled by your Sophos partner.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!

Question 1 of 3

By default, email alerts are sent for which severity of alert?

High severity only

High and medium severity

All alerts

No alerts, the required
severity must be chosen



Question 2 of 3

True or False: Events are logged for all detections, including clean up.

True

False

SOPHOS

Question 3 of 3

How many detections must occur in a 24 hour period for an outbreak alert to be reported?

Chapter Review

Events are logged for **ALL** detection events, including clean up events. **Alerts are only shown when action is required.**

When you mark an alert as **acknowledged** or **resolved**, the alert is removed from the alert list. This **does not remove the detected threat** from the device.

By default, **email alerts** are sent for **medium or high-level events that require actions**, and they are sent to **all users with the administrator role**.

SOPHOS

Here are the three main things you learned in this chapter.

Events are logged for **ALL** detection events, including clean up events. Alerts are only shown when action is required.

When you mark an alert as acknowledged or resolved, the alert is removed from the alert list. This does not remove the detected threat from the device.

By default, email alerts are sent for medium or high-level events that require actions, and they are sent to all users with the administrator role.



Getting Started with Sophos Central Threat Remediation

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4025: Getting Started with Sophos Central Threat Remediation

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central Threat Remediation

In this chapter you will learn how to view and manage threats, including those that are not automatically cleaned up.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to protect and manage devices with Sophos Central
- ✓ How to view alerts and events in Sophos Central

DURATION **11 minutes**

SOPHOS

In this chapter you will learn how to view and manage threats, including those that are not automatically cleaned up.

Considerations



Consider how a protected device might become infected.

SOPHOS

Let's take a moment to consider how a protected device might become infected.

Why Might Devices Become Infected?

Unprotected device(s) on a network

No anti-malware software installed

Unprotected devices can provide a point of access for attacks to gain network access

Running out of date anti-malware software

Devices that are not protected against the latest threats are vulnerable to attacks

Anti-malware features are not enabled

All protection features should be enabled, without them, the device is vulnerable

Missing app and/or OS updates and patches

Out of date or unpatched apps and OS's make a device weak and vulnerable to exploitation

SOPHOS

One attack vector is an unprotected device or devices on a network. Unprotected could be considered as any of the following states.

A device that has no anti-malware software installed. An unprotected device can provide a point of access for an attacker to gain access to a network and then access more of that network to get what they want.

A device that is running out of date anti-malware software. Devices that are not protected against the latest threats can be vulnerable to attacks.

Devices that, whilst protected, do not have all of the recommended security features enabled. All protection features should be enabled, without them, the device is vulnerable.

Devices that are missing application or operating system updates and patches. Out of date and unpatched applications and operating systems make a device weak as the software is vulnerable to exploitation.

Why Might Devices Become Infected?

Inappropriate Exclusions

Malware can leverage legitimate applications and processes to evade detection

Excluding tools can create opportunities for malicious exploitation

Allowing a known PUA on all devices for example, could allow an attack to exploit that application

SOPHOS

Inappropriate exclusions can leave your network open to attack. Malware will also try to leverage legitimate applications and processes as much as possible to evade detection.

Creating exclusions for tools that you find useful or necessary can create an opportunity for malicious exploitation.

Why Might Devices Become Infected?

Zero-Day Threats

Attacks are constantly developing new attack techniques

Attackers will use malware that aims to bypass anti-malware software

SOPHOS

Sophos Central includes several techniques to detect and block zero-day threats, however, attackers do not generally release malware they know is going to be detected and blocked.

They will release malware they believe will bypass anti-malware software and are therefore constantly developing new techniques that a detection has not been created for.

Automatic Clean Up

The EVENTS tab details both the detection and clean up events

SEV	TYPE	DATE	EVENT
⚠		Nov 2, 2022 8:35 PM	Malware detected: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1_HighScore.zip\HighScore.exe'
●		Nov 2, 2022 8:35 PM	Malware cleaned up: 'EICAR-AV-Test' at 'http://www.sophoshost.com/eicar/index.html'
●		Nov 2, 2022 8:35 PM	Malicious connection detected: 'EICAR-AV-Test' at 'http://www.sophoshost.com/eicar/index.html' [Technical Support reference: 275a]
●		Nov 2, 2022 8:34 PM	Malware cleaned up: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1_HighScore.zip\HighScore.exe'
⚠		Nov 2, 2022 8:34 PM	Malware detected: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1_HighScore.zip\HighScore.exe'
●		Nov 2, 2022 9:59 AM	Update succeeded
●		Oct 31, 2022 2:10 PM	Real time protection re-enabled
●		Oct 31, 2022 2:09 PM	Peripheral allowed: Mats Virtual CDROM ATA Device
●		Oct 31, 2022 2:09 PM	Peripheral allowed: Floppy disk drive
●		Oct 31, 2022 2:09 PM	Central management has been resumed
●		Oct 31, 2022 10:10 AM	Real time protection disabled

SOPHOS

For a large majority of detections, the Sophos Endpoint Agent will automatically clean up any detected malicious files, folders, processes, or applications.

Detection Types

Anti-Exploit

Jun 1, 2018 11:02 AM

'HeapSpray' exploit prevented in Windows Wordpad Application

CryptoGuard

Jun 1, 2018 11:03 AM

CryptoGuard detected ransomware in C:\Users\judehawke\Desktop\SophosTesterv3214\SophosTester.exe

Application Lockdown

Jun 1, 2018 1:35 PM

'Lockdown' exploit prevented in Internet Explorer

Safe Browsing

Jun 1, 2018 11:17 AM

Safe Browsing detected browser Google Chrome has been compromised

SOPHOS

The types of alerts you may see in Sophos Central will depend on the threat detected. These example detections would be automatically cleaned up where possible. For any threat that is not automatically cleaned up, you will see an alert for it in Sophos Central.

Detection Types

ML/PE-A

Malicious Portable Executable

KB-000036922

ML/PUA

Potentially Unwanted Application

KB-000034357



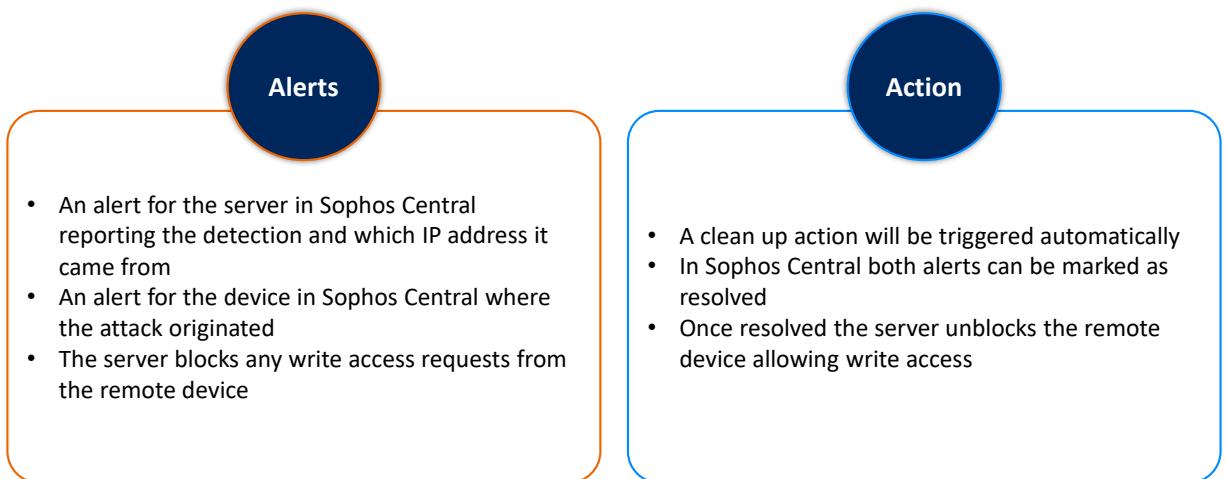
Examples of portable executables:

- .exe
- .sys
- .dll
- .scr

SOPHOS

The Sophos Endpoint Agent will detect malicious files and can generate either a ML/PE-A detection for files categorized as malicious or an ML/PUA detection for files categorised as PUAs.

Remotely Run Ransomware



SOPHOS

Runtime protection includes protection from remotely run ransomware. Detections are triggered when ransomware is remote to a device but attacks files that are stored on the device, such as files stored on a shared drive.

If such an attack is detected, a clean up action will be triggered automatically and any files that may have been encrypted are restored.

Malicious Traffic Detections

C2/Generic-B: Not blocked and not cleaned up

Specify date range within past 90 days		
SEV	TYPE	DATE
		Jun 17, 2021 11:35 AM
		Jun 17, 2021 11:32 AM
!		Jun 17, 2021 11:29 AM
		Jun 17, 2021 11:22 AM

Malicious connection detection locally cleared: 'C2/Generic-B' at 'C:\Windows\System32\wscript.exe'
Update succeeded
Malicious connection detected: 'C2/Generic-B' at 'C:\Windows\System32\wscript.exe' (Technical Support reference: 277413403)
Reboot to complete update; computer stays protected in the meantime

C2/Generic-A and C2/Generic-C: Blocked but not cleaned up

Specify date range within past 90 days		
SEV	TYPE	DATE
!		Jun 8, 2021 3:34 PM
		Jun 8, 2021 3:34 PM
		Jun 8, 2021 12:28 PM

Sophos Firewall detected malicious connections: 'C2/Generic-C' at 'C:\program files (x86)\Google\Chrome\application\chrome.exe'
Access was blocked to "sophostest.com/calitheme/index.html" because of "C2/Generic-A".
Update succeeded

SOPHOS

A C2 detection indicates malicious traffic has been detected. There are three C2 detection variants.

C2/Generic-B is the most serious. This detection means that malicious traffic was detected but not blocked and that the threat has not been cleaned up. This type of detection requires investigation as active malware is on the device. The malware is not blocked, as the malicious traffic is detected at the point of connection and so has already happened.

C2/Generic-A and C detections are returned when the malicious traffic detected has been blocked. C2/Generic-A detections are generally only seen on Sophos Firewalls, unless the URL is being accessed by an Internet browser process. C2/Generic-C detections are usually only seen on devices that are using Sophos Security Heartbeat with a Sophos Firewall.

Exploit Detections

What happens when an exploit is detected?

- The exploit is stopped
- The user is notified
- A threat graph is generated
- The threat is automatically cleaned up

What action needs to be taken?

- Investigate using the threat graph
- Determine if a user downloaded or authorized a vulnerable application
- Ensure that the operating system and applications are up-to-date
- Provide user training

SOPHOS

If an exploit is detected, it will be stopped. The user of the device is notified and a threat graph is created. These detections are automatically cleaned up.

Following an exploit detection, an administrator should investigate using the threat graph which provides the details of where the threat originated, how it spread, which processes were involved, and which files were effected. An administrator should determine if a user downloaded or authorized a vulnerable application that allowed the exploit. Additionally, an administrator should ensure that the operating system and applications are up to date and that all patches are installed on the device. Finally, the administrator should educate users on safe browsing techniques and review user policies in Sophos Central.

As a result of an investigation, an administrator may decide to block downloads from specific websites and Internet browsers, or to restrict user access to applications.

Web Browser Detections

What happens when a web browser threat is detected?

- Sophos Endpoint Agent warns the user to close the browser
- A threat graph is generated
- The threat is automatically cleaned up

What action needs to be taken?

- Use the threat graph to identify the IP address and URL connection associated with the attack
- Determine if the IP address or URL should be blocked

SOPHOS

If a web browser threat is detected, the threat is automatically cleaned up and the user is warned to close the Internet browser. A threat graph is automatically created in Sophos Central.

Following this type of detection, an administrator can use the threat graph to identify the IP address and URL connection associated with the attack. They should determine if the IP address or URL should be blocked. The user should also be advised to check any accounts if they entered credentials and to change any passwords if they were entered on the website.

Malware Detections

What happens when malware is detected?

- Malware is detected and automatically cleaned up
- The malware and associated files are quarantined
- The user is notified
- A threat graph is generated

What action needs to be taken?

- No further action is required
- The threat has been detected and cleaned up
- All associated files have been removed from the device
- If the item was incorrectly detected as malware, it can be restored

SOPHOS

If malware is detected on a device, it will be automatically cleaned up. The malicious items and all associated files are quarantined. The user is notified and a threat graph is generated in Sophos Central.

In this case, there is no action required as the threat has been detected and removed from the device. If the item was incorrectly detected, it can be restored.

Manual Clean Up

The screenshot shows the Sophos Central Dashboard with the following details:

- Sophos Central Dashboard:** Shows a total of 6 alerts (6 Total Alerts, 4 High Alerts, 2 Medium Alerts, 0 Low Alerts).
- Most Recent Alerts:** A list of five recent alerts, including one for an EICAR test detection.
- EICAR-AV-Test Detail View:** Shows the alert description: "EICAR-AV-Test detected file named 'EICAR-TEST.AVI' in folder 'C:\Windows\Temp'. The file was identified as malicious by multiple engines." It also lists affected operating systems (Windows 10 Pro, Windows 11 Pro) and provides links to summary, file information, and knowledge base articles.
- Callout Box:** A green callout box points to the knowledge base article link in the alert detail view, with the text: "View the detection information and view knowledge base articles about the detection type".

For those detections where manual intervention is required, an alert will be triggered and displayed in Sophos Central.

If you select the alert description from the most recent alerts list on the dashboard, you will be redirected to the knowledge base which lists articles related to that detection.

In this example, it is an EICAR test detection.

Manual Clean Up

The screenshot displays the Sophos Central Dashboard. On the left, the navigation menu includes options like Dashboard, Alerts, Threat Analysis Center, Log & Reports, People, Devices, Global Settings, Protect Devices, Account Health Check, and MY PRODUCTS (Endpoint Protection, Server Protection, Mobile). The main area shows a summary of alerts: 6 Total Alerts, 4 High Alerts, 2 Medium Alerts, and 0 Low Alerts. Below this is a list of 'Most Recent Alerts' with details such as date, time, alert type, and affected device. A green callout box points to the device name 'linux-av' in the list. On the right, there's a detailed view of the device 'linux-av' under the 'Events' tab, showing recent events like manual cleanup requests and update successes.

Sophos Central Dashboard

See a snapshot of your security protection.

Help - UK Training -
Sophos UK - Super Admin

6 Total Alerts
4 High Alerts
2 Medium Alerts
0 Low Alerts

Most Recent Alerts

Date	Time	Description	Device	Action
Nov 27, 2022	1:01 AM	Your API token Active Directory will expire in 5 days	WINCLIENT1\S...	Show full details
Nov 17, 2022	1:01 AM	Your API token Active Directory will expire in 15 days	WINCLIENT1\S...	Show full details
Nov 10, 2022	10:57 ...	Manual PUA cleanup required: 'PakIIR' at 'C:\Users\So...	WINCLIENT1\S...	Show full details
Nov 10, 2022	10:57 ...	Manual PUA cleanup required: 'PsKIR' at 'C:\Users\So...	WINCLIENT1\S...	Show full details
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at 'home/c...	n/a	linux-av
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at 'home/c...	n/a	Show full details

Sophos UK - Super Admin

SUMMARY EVENTS STATUS POLICIES

Recent Events

Date	Time	Description
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at '/home/central/cache/mozilla/firefox/4ppn4qzg.default'
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at '/home/central/cache/mozilla/firefox/4ppn4qzg.default'
Nov 3, 2022	10:38 AM	Update succeeded
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at '/home/central/cache/mozilla/firefox/4ppn4qzg.default'
Nov 3, 2022	10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at '/home/central/cache/mozilla/firefox/4ppn4qzg.default'

Sophos UK - Super Admin

View the device the detection was found on

If you select the device name, you will be re-directed to the device page where you can review the status of the device and view the detection on the **Events** tab.

Manual Clean Up

The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes 'Dashboard', 'Alerts' (which is selected), 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices', 'Global Settings', 'Protect Devices', 'Account Health Check', and sections for 'MY PRODUCTS' like 'Endpoint Protection', 'Server Protection', 'Mobile', 'Encryption', 'Wireless', and 'Email Security'. The main content area displays a summary of alerts: 6 Total Alerts, 4 High Alerts (highlighted in red), 2 Medium Alerts (highlighted in yellow), and 0 Low Alerts. Below this, a specific alert is detailed: 'Detection description and information' (highlighted in blue), 'Device and user information' (highlighted in green), and 'Actions' (highlighted in orange). The alert itself is titled 'Manual cleanup required: EICAR-AV-Test' and occurred on Nov 3, 2022 at 10:38 AM. It provides a 'Description' of the threat found in a specific file path, a 'More Information' link, and a 'What you need to do' section with a link to a knowledge base article. Device details include Endpoint Type: Server, OS: Posix, User: n/a, and Device: 344-01. Action buttons include 'Mark As Resolved' and 'Learn More'.

Clicking **Show full details** displays the **Alerts** page. Expanding the alert details displays the information about the detection. A description of the detection and any further information available. Links and information are provided to assist with cleaning up the detection.

Information about where the detection was found, the device type, the operating system, and the device name and user that was logged in at the time the detection was triggered are displayed.

The available actions for the detection are also displayed here. Available actions could be to resolve the alert.

Depending on the detection, you can also select to mark the alert as acknowledged, view the threat graph, or amend the frequency of email alerts for the detection type.

Manual Clean Up



Marking an alert as resolved **does not clean up** the threat

SOPHOS

If you select to mark an alert as resolved by selecting **Mark as resolved** you will be clearing the alert from Sophos Central.

This action **DOES NOT** clean up the detected threat. It **ONLY** clears the alert from Sophos Central.

Sophos Protection for Linux



SOPHOS

There is no automatic clean up for servers protected by Sophos Protection for Linux. When there is a detection, access to the file is blocked in place and manual clean up is required.

Sophos Protection for Linux

The screenshot shows the Sophos Central web interface. On the left is a sidebar with links like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices (which is selected), Global Settings, Protect Devices, and Account Health Check. The main area is titled 'linux-av' and shows a summary of recent events. The 'Events' tab is active, displaying a list of five recent events:

Date	Action	Description
Nov 3, 2022 10:38 AM	Manual cleanup required	'EICAR-AV-Test' at '/home/central/.cache/mozilla/firefox/4ppn4cqzg.default'
Nov 3, 2022 10:38 AM	Manual cleanup required	'EICAR-AV-Test' at '/home/central/.cache/mozilla/firefox/4ppn4cqzg.default'
Nov 3, 2022 10:38 AM	Update succeeded	
Nov 3, 2022 10:38 AM	Manual cleanup required	'EICAR-AV-Test' at '/home/central/.cache/mozilla/firefox/4ppn4cqzg.default'
Nov 3, 2022 10:32 AM	Manual cleanup required	'EICAR-AV-Test' at '/home/central/.cache/mozilla/firefox/4ppn4cqzg.default'

The **Events** tab for the server will display the detection event.

For Sophos Anti-Virus for Linux (Legacy) protected servers, there is a clean up option available to run locally.

Linux Clean Up



Additional information in
the notes

The screenshot shows the Sophos Central Dashboard. On the left is a sidebar with navigation links: Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Protect Devices, Account Health Check, MY PRODUCTS, Endpoint Protection, Server Protection, Mobile, and Encryption. The main area is titled "Sophos Central Dashboard" with the sub-instruction "See a snapshot of your security protection". It displays four alert counts: 6 Total Alerts (blue), 4 High Alerts (red), 2 Medium Alerts (yellow), and 0 Low Alerts (green). Below this is a section titled "Most Recent Alerts" with five entries. The fifth entry, dated Nov 3, 2022 10:38 AM, has its entire row highlighted with an orange border. This row contains the alert text "Manual cleanup required: 'EICAR-AV-Test' at '/home/c...'".

Date	Alert Text	Host	User	Action
Nov 27, 2022 10:01 AM	Your API token Active Directory will expire in 5 days			Show full details
Nov 17, 2022 1:01 AM	Your API token Active Directory will expire in 15 days			Show full details
Nov 10, 2022 10:57 ...	Manual PUA cleanup required: 'PsKill' at 'C:\Users\Se...'	WINCLIENT1\S...	WinClient1	Show full details
Nov 10, 2022 10:57 ...	Manual PUA cleanup required: 'PsKill' at 'C:\Users\Se...'	WINCLIENT1\S...	WinClient1	Show full details
Nov 3, 2022 10:38 AM	Manual cleanup required: 'EICAR-AV-Test' at '/home/c...'	n/a	linux-av	Show full details

On the Sophos Central Dashboard, you will see the alert text, **Manual cleanup required**. This indicates that clean up of the detected file must be carried out manually using a native removal command.

Once you have cleaned up the detection on a Linux protected server, you will need to mark the alert as resolved in Sophos Central to remove the alert.

[Additional Information]

For more information on how to manage a Sophos Protection for Linux (SPL) protected server, please see our on-demand technical training course.

Linux Clean Up

Run a second scan to confirm the clean up was successful

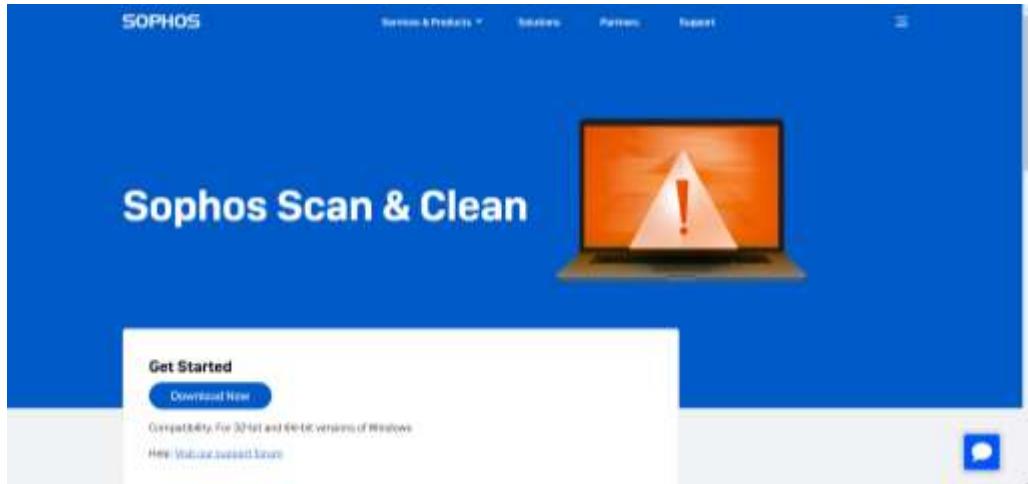
SOPHOS

Manual clean up for Sophos Anti-virus for Linux (Legacy) is achieved by using the savscan command. In this example, we are passing it to the location to scan the whole server. We include the argument –remove so that during the scanning process, any detected files will be cleaned up.

Here we can see that we are prompted to remove the detected files. By using the `-nc` argument you can disable confirmation prompts so detected items are automatically removed.

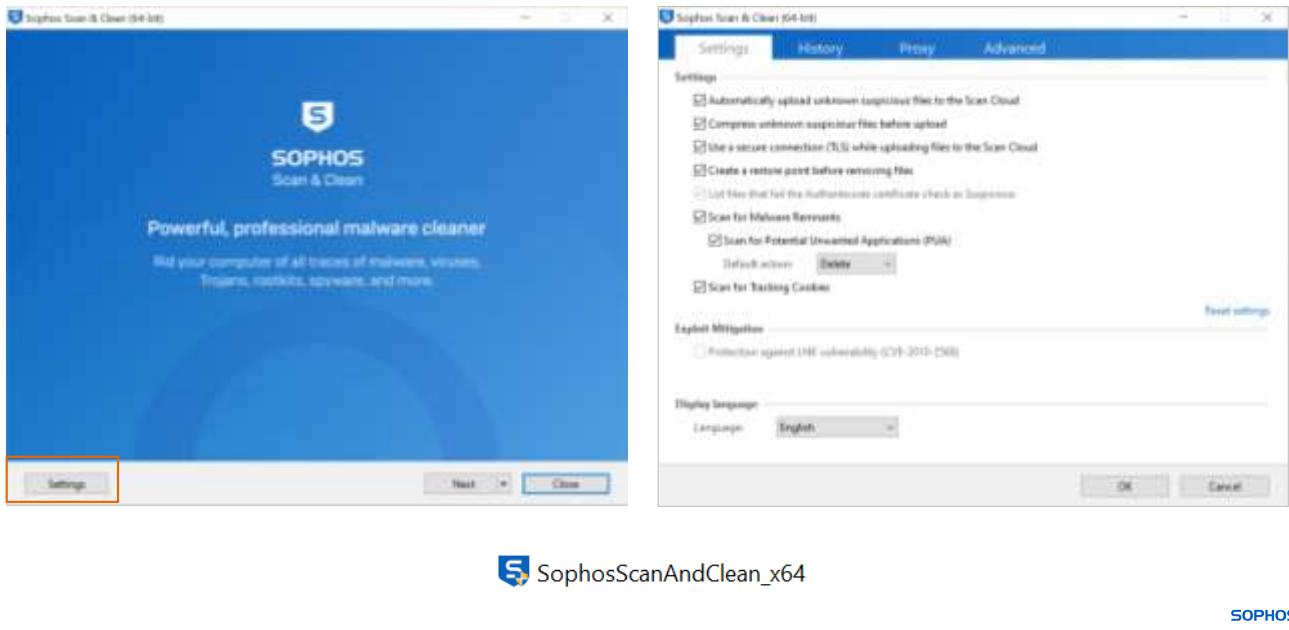
It is important to run a second scan to confirm that all items have been cleaned up successfully.

Sophos Scan & Clean



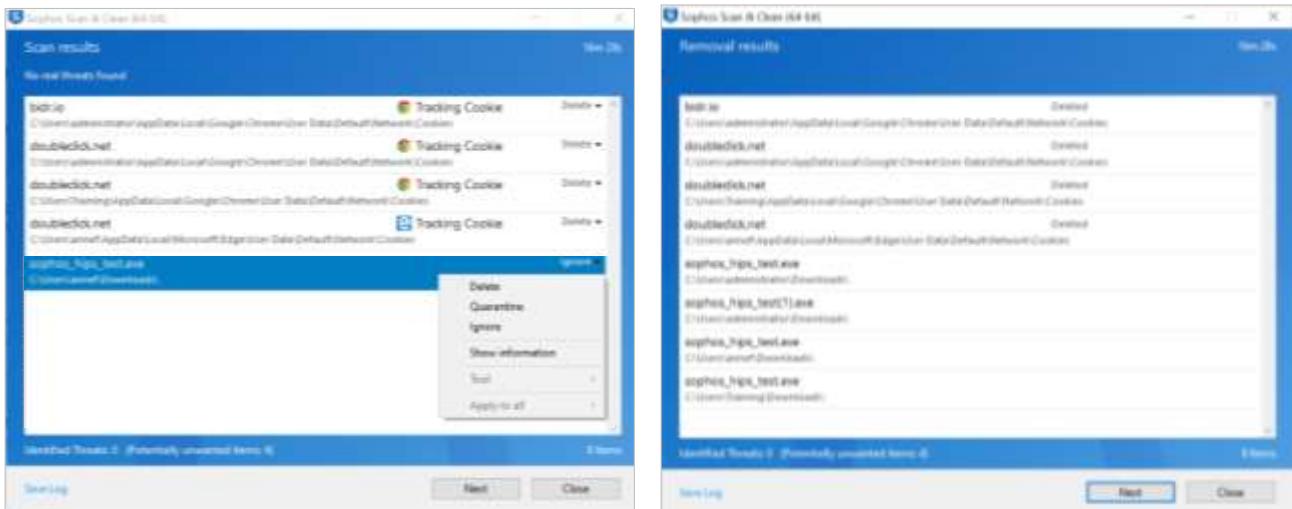
Sophos Scan & Clean is a free second-opinion virus removal scanner that is capable of both detecting and removing threats and other malware. It works alongside existing anti-virus solutions and is supported on Windows 7 and later, with 32 and 64-bit versions.

Sophos Scan & Clean



Once downloaded, the program can be launched. You can select to customize the operation settings if required.

Sophos Scan & Clean



SOPHOS

Any files or threats found are displayed with a suggested action to be taken. The action can be modified using the drop-down list. Any items that are marked for deletion will be automatically deleted when the scan is finished.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

Which Sophos tool provides a second opinion virus scanner?

Virus Removal Tool

Bootable AV

Sophos Scan & Clean

SOPHOS



Question 2 of 3

True or False: Marking an alert as resolved does not clean up the threat.

True

False

SOPHOS



Question 3 of 3

Which of the following statements about Sophos Protection for Linux is true?

A cleanup option is provided
in Central

Sophos Scan & Clean
provides manual cleanup

Cleanup must be carried out
manually

SOPHOS

Chapter Review

Marking an alert as resolved **does not clean up** the threat.

There is **no automatic clean up** for servers protected by **Sophos Protection for Linux**. When there is a detection, access to the file is blocked in place and **manual clean up is required**.

Sophos Scan & Clean is a free **anti-virus removal tool** that works alongside existing anti-virus solutions and is supported on Windows 7 and later, with 32 and 64-bit versions.

SOPHOS

Here are the three main things you learned in this chapter.

Marking an alert as resolved does not clean up the threat.

There is no automatic clean up for servers protected by Sophos Protection for Linux. When there is a detection, access to the file is blocked in place and manual clean up is required.

Sophos Scan & Clean is a free virus removal tool that works alongside existing anti-virus solutions and is supported on Windows 7 and later, with 32 and 64-bit versions.



Getting Started with Sophos Central SafeStore

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4030: Getting Started with Sophos Central SafeStore

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central SafeStore

In this chapter you will learn how Sophos Central quarantines detected files and restores them if required.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

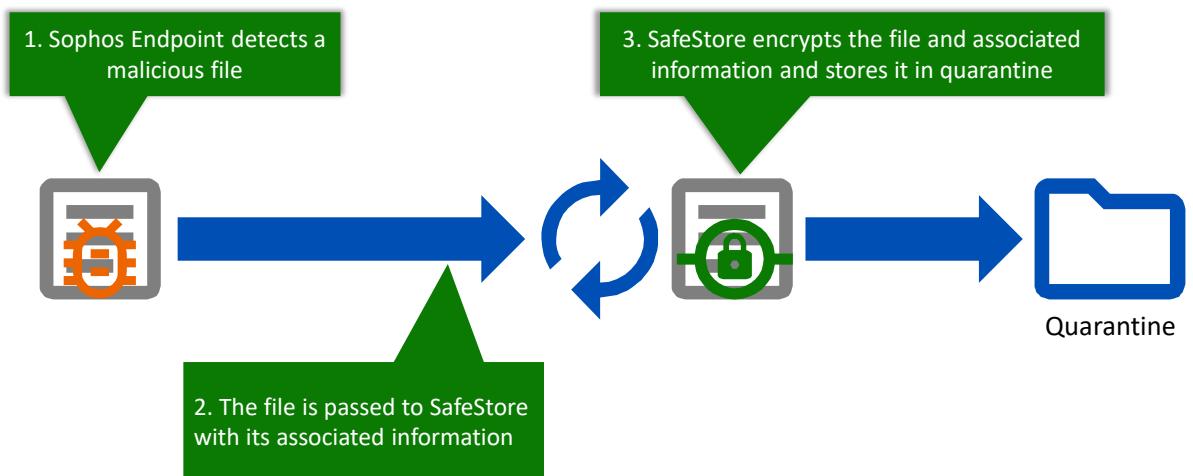
- ✓ How Sophos Central detects threats
- ✓ How threats are cleaned up automatically
- ✓ How to allow applications that have been detected as a PUA

DURATION **10 minutes**

SOPHOS

In this chapter you will learn how Sophos Central quarantines detected files and restores them if required.

SafeStore Overview



SOPHOS

When Sophos cleans up a file it is passed to SafeStore with its associated information. SafeStore encrypts the file and associated information and stores it in the quarantine.

The associated file information can include registry keys, permissions and service information, to ensure that if it needs to be restored it can be left in a fully functioning state.

Please note that if a file is disinfected and the malicious code is removed from the file, the remaining file is clean and is not sent to SafeStore.



Additional information in
the notes

SafeStore File Release

Why might you need to release a file from SafeStore?

Unwanted detection

e.g., PUA

- Investigate file/application for legitimacy
- Create an exclusion to release the file/application from SafeStore

False positive

e.g., custom internal application

- Consult **KB-000037167** to ensure FP status
- Apply an exclusion to release the file from SafeStore

SOPHOS

There are several reasons you may choose to release a file that has been quarantined. Two possible reasons for releasing a file from SafeStore are:

- If a file or a PUA has been detected and cleaned up and you want to continue using it
- If a file has been quarantined due to a false positive detection

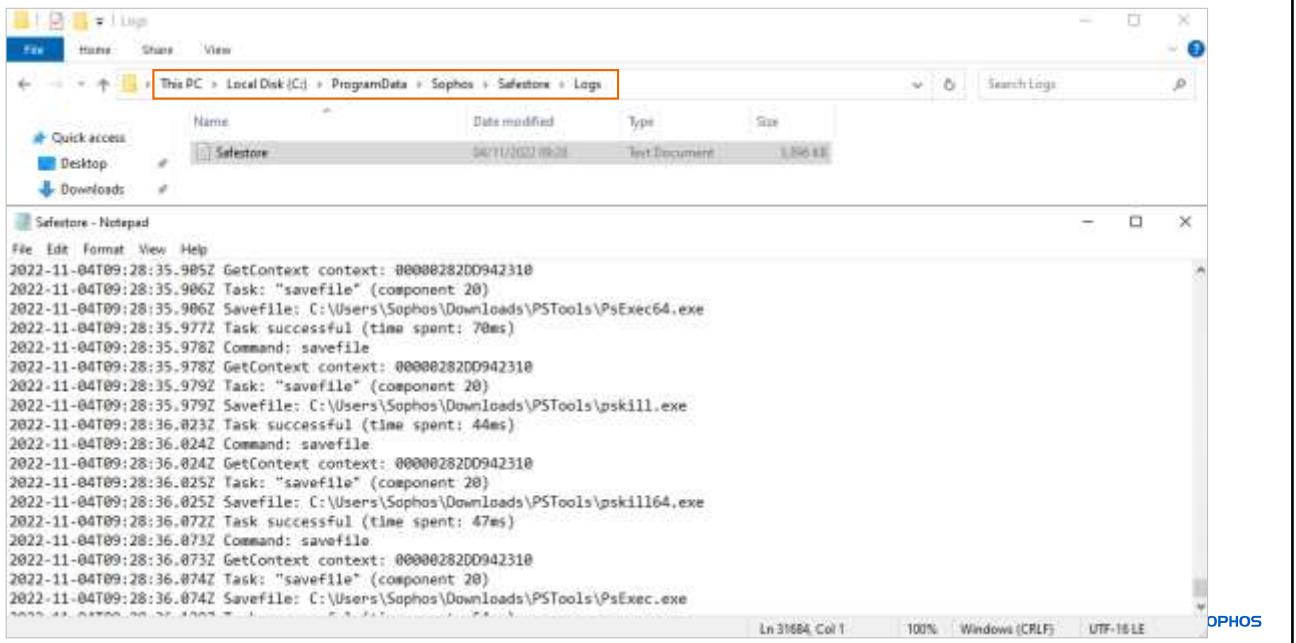
If you want to use a file or an application that has been cleaned up, it is recommended that you create an exclusion in the local threat protection policy for the file or application. Please note that any exclusions should be carefully considered before being implemented as they reduce your security. Once the exclusion has been applied to a device through a policy, the files related to the detection are released from the SafeStore.

If you suspect a file is a false positive detection, we recommend that you investigate it before releasing the file. If files are detected due to a false positive, and Sophos later releases an update that resolves the detection, that file will be restored. This is because the contents of SafeStore are rechecked whenever there is an update.

[Additional Information]

To ensure a file is a false positive please see knowledge base article **KB-000037167**.
<https://support.sophos.com/support/s/article/KB-000037167>

SafeStore Logs



```
SafeStore - Notepad
File Edit Format View Help
2022-11-04T09:28:35.985Z GetContext context: 00000282DD942310
2022-11-04T09:28:35.986Z Task: "savefile" (component: 20)
2022-11-04T09:28:35.986Z Savefile: C:\Users\Sophos\Downloads\PSTools\PsExec64.exe
2022-11-04T09:28:35.977Z Task successful (time spent: 70ms)
2022-11-04T09:28:35.978Z Command: savefile
2022-11-04T09:28:35.978Z GetContext context: 00000282DD942310
2022-11-04T09:28:35.979Z Task: "savefile" (component: 20)
2022-11-04T09:28:35.979Z Savefile: C:\Users\Sophos\Downloads\PSTools\pskill.exe
2022-11-04T09:28:36.023Z Task successful (time spent: 44ms)
2022-11-04T09:28:36.024Z Command: savefile
2022-11-04T09:28:36.024Z GetContext context: 00000282DD942310
2022-11-04T09:28:36.025Z Task: "savefile" (component: 20)
2022-11-04T09:28:36.025Z Savefile: C:\Users\Sophos\Downloads\PSTools\pskill64.exe
2022-11-04T09:28:36.072Z Task successful (time spent: 47ms)
2022-11-04T09:28:36.073Z Command: savefile
2022-11-04T09:28:36.073Z GetContext context: 00000282DD942310
2022-11-04T09:28:36.074Z Task: "savefile" (component: 20)
2022-11-04T09:28:36.074Z Savefile: C:\Users\Sophos\Downloads\PSTools\PsExec.exe
```

Ln 31684 Col 1 100% Windows (CRLF) UTF-16 LE

SOPHOS

The SafeStore quarantine is stored in the SafeStore directory.

If we look at the log file, we can see a ‘savefile’ action for detected files. In this example, the Microsoft PS Tools suite was downloaded which triggered multiple detections.

[Additional Information]

SafeStore log directory: C:\ProgramData\Sophos\SafeStore\Logs

SafeStore Events

The clean up action is logged meaning the associated files are in the SafeStore

DEV	TYPE	DATE	EVENT
WinClient1	Info	Nov 4, 2022 11:25 AM	'https://config.edge.skypw.com/config/v1/EdgeUpdate/1.3.169.31' blocked due to category 'Streaming K...
Windows 10	Info	Nov 4, 2022 9:28 AM	PUA cleaned up: 'PsKill' at 'C:\Users\Sophos\Downloads\pstools\pskill64.exe'
172.16.1.70	Info	Nov 4, 2022 9:28 AM	PUA cleaned up: 'PsKill' at 'C:\Users\Sophos\Downloads\pstools\pskill.exe'
Last User: Sophos	Info	Nov 4, 2022 9:28 AM	PUA cleaned up: 'PsExec' at 'C:\Users\Sophos\Downloads\pstools\psexec64.exe'
Internet	Info	Nov 4, 2022 9:28 AM	PUA cleaned up: 'PsExec' at 'C:\Users\Sophos\Downloads\pstools\psexec.exe'
WinClient1	Warning	Nov 4, 2022 9:28 AM	PUA detected: 'PsExec' at 'C:\Users\Sophos\Downloads\pstools\psexec64.exe'
Windows 10	Warning	Nov 4, 2022 9:28 AM	PUA detected: 'PsExec' at 'C:\Users\Sophos\Downloads\pstools\psexec.exe'
172.16.1.70	Warning	Nov 4, 2022 9:28 AM	PUA detected: 'PsKill' at 'C:\Users\Sophos\Downloads\pstools\pskill64.exe'
Last User: Sophos	Warning	Nov 4, 2022 9:28 AM	PUA detected: 'PsKill' at 'C:\Users\Sophos\Downloads\pstools\pskill.exe'
Internet	Warning	Nov 4, 2022 9:12 AM	'https://download.sysinternals.com/files/PSTools.zip' blocked due to category 'Hacking'

The detection is logged

The **Events** tab on a device record will detail all events happening on a device, including detections of unwanted files or applications and false positives.

In the events list you will see two lines per detection. The first line is the detection event, and the second line is the clean up event. When a file is cleaned up both it, and its associated files are encrypted in the SafeStore.

SafeStore Events

The screenshot shows the Sophos Central interface with the 'Devices' tab selected. A device named 'WinClient1' is selected. The 'Events' tab is active, displaying a list of 171 events from August 8, 2022, to November 7, 2022. The events list includes various PUA detections and blocked files, such as 'PsKill' and 'PsExec'. A specific event from November 7, 2022, at 9:12 AM is highlighted with a red box, showing the URL 'https://download.sysinternals.com/files/PSTools.zip' was blocked due to category 'Hacking'. The 'Details' link for this event is also highlighted.

Date	Event Description	Details Link
Aug 8, 2022	'https://config.edge.skype.com/config/v1/EdgeUpdate/1.3.169.31' blocked due to category 'Streaming Media'	
Nov 7, 2022	1, 2022 9:12 AM 'https://download.sysinternals.com/files/PSTools.zip' blocked due to category 'Hacking'	Details

To release a file from the SafeStore, locate the detection event in the **Events** tab of the device where it has been detected.

Scroll to the right to view the **Details** link.

SafeStore File Recovery



- SHA 256
 - Allow the file by the SHA 256 which will allow any file with the same SHA 256
- File Path
 - Allow the file by the specific file path will whitelist any file with the same name in that specific location
- Certificate
 - Allow the file by the certificate whitelists all files signed by the digital signature

SOPHOS

The event details include the detection name, certificate, SHA 256 hash, and the path the file was detected in. If you suspect the detection is a false positive, you can use this information to check if other vendors are categorizing the file as malicious or legitimate.

You can choose to allow the application in three ways, either using the SHA 256, the file path or the certificate.

If you select to release a file using the file path it will whitelist any file with the same name in that specific location, this helps when legitimate files are detected again after they have been updated, even if the SHA 256 has changed. If you select to release a file using the certificate it will whitelist every file signed by this digital signature, which can be useful to ensure legitimate applications that are signing their files do not get detected. However, if you have reason to believe the certificate might have been compromised then it is safer to use the SHA 256 instead.

Please note that allowing an application by any of the above methods will result in the SHA 256, file path or certificate being whitelisted for your entire environment. This means if you have multiple devices that detect the same file, it will be restored on all of them.

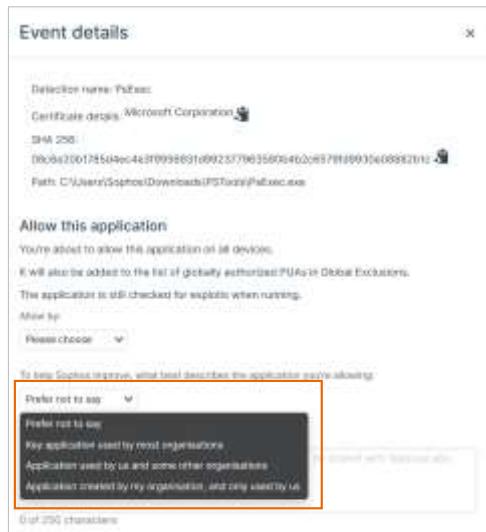
SafeStore File Recovery

When allowing detected applications, classify the application type:

- Key application used by most organizations
- Application used by your organization and other organizations
- Application created by your organization, and only used by you

Once a detected application is allowed it will be released from SafeStore on all devices where it has been detected.

The detected application is added to the allowed applications list in Global Settings.



Sophos **does not recommend** allowing detected applications UNLESS you are sure they are safe

SOPHOS

Once you have selected how to allow the detected file or application, select the option to log why the file has been released. It is important to understand that Sophos does not recommend allowing any detected applications unless you are sure they are safe.

When you allow a detected application, you can also classify what type of application it is:

- Key application used by most organizations
- Application used by us and some other organizations
- Application created by my organization, and only used by us
- Or you can choose not to say

Once an application is allowed it will be released from SafeStore on all devices where it was detected. Once a detected application has been allowed, it will be added to the allowed applications list in **Global Settings**.

Policy Exclusions



SafeStore is scanned when a policy is updated



Excluded files/applications are restored
If a location is excluded **ALL** detected items are restored

Locations **NOT** recommended for whitelisting

- ✗ C:\
- ✗ C:\TEMP\
- ✗ C:\users\[username]\
- ✗ C:\users\[username]\downloads\
- ✗ C:\users\[username]\documents\
- ✗ C:\users\[username]\documents\my received files\

Whitelisting location could restore convicted malicious items across your network

SOPHOS

When a policy is updated and the endpoint receives the update, the SafeStore is scanned. If a new exclusion has been added, then the files and items that relate to that exclusion will be restored.

Extreme caution should be taken when excluding items. Excluding locations will return any previously convicted applications to that location, including associated files and registry entries. If this happens, you could accidentally restore convicted malicious items across your network.

[Additional Information]

We recommend that the following locations are never whitelisted as they are the most common attack locations:

- C:\
- C:\TEMP\
- C:\users\[username]\
- C:\users\[username]\Downloads\
- C:\users\[username]\Documents\
- C:\users\[username]\Documents\My Received Files\

Allowing Detection Items

WARNING: Only allow items that are legitimate

Application

In the event details select
Allow this application

- Select either:
- Certificate
 - SHA-256
 - Path

Exploit

In the event details select
Don't detect this again

Select either:

- Allow by detection ID (most secure)
- Allow by mitigation
- Allow by application

Ransomware

In the event details select
Don't detect this again

Select:

- Allow by detection ID

SOPHOS

Think carefully before you add any exclusions as this significantly reduces your protection. Exclusions can be added from the event details created by a detection for applications, exploits and ransomware. The detection and exclusion of applications have already been covered.

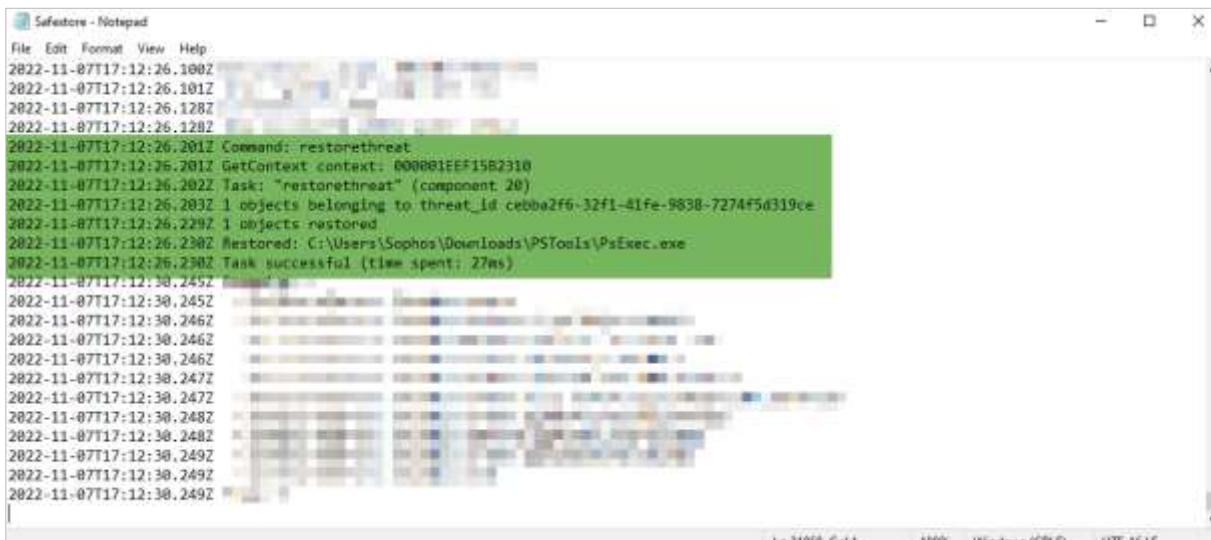
To allow an exploit, select the event details and then select ‘Don’t detect this again’. You can select either to:

- ‘Allow by detection ID’ prevents the specific detection. This is the most secure way of excluding a detected exploit. Items excluded using this method go into the **Global Exclusions** list
- ‘Allow by mitigation’ stops the device from checking a specific exploit on the affected application. For example, if a ‘Safe Browsing’ detection was triggered in Microsoft Edge, using this option will mean the endpoint no longer checks for the Safe Browsing exploit type in Edge
- ‘Exclude by application’ prevents any checks for exploits in the application. For example, if a code cave exploit was triggered in Excel and you choose this method to exclude Excel, Excel will cease to be protected from ANY exploits in the future, not just the code cave exploit. Applications excluded via this method go into the **Exploit Mitigation Exclusion** list in case you need to go back and remove the respective exclusion

It is recommended to exclude the detection ID first as this provides a better target. If the same detection happens again use the ‘Mitigation’ method, then if required exclude the application on the next occurrence.

To allow ransomware, **which is not recommended**, you can select to exclude this detection ID from checking. This will prevent the detection.

SafeStore File Recovery



```
SafeStore - Notepad
File Edit Format View Help
2022-11-07T17:12:26.100Z
2022-11-07T17:12:26.101Z
2022-11-07T17:12:26.128Z
2022-11-07T17:12:26.128Z
2022-11-07T17:12:26.201Z Command: restorethreat
2022-11-07T17:12:26.201Z GetContext context: 000001EFF15B2310
2022-11-07T17:12:26.202Z Task: "restonethreat" (component 20)
2022-11-07T17:12:26.203Z 1 objects belonging to threat_id cebba2f6-32f1-41fe-9838-7274f5d319ce
2022-11-07T17:12:26.229Z 1 objects restored
2022-11-07T17:12:26.230Z Restored: C:\Users\Sophos\Downloads\PSTools\PsExec.exe
2022-11-07T17:12:26.230Z Task successful (time spent: 27ms)
2022-11-07T17:12:30.245Z
2022-11-07T17:12:30.246Z
2022-11-07T17:12:30.246Z
2022-11-07T17:12:30.246Z
2022-11-07T17:12:30.247Z
2022-11-07T17:12:30.247Z
2022-11-07T17:12:30.248Z
2022-11-07T17:12:30.248Z
2022-11-07T17:12:30.249Z
2022-11-07T17:12:30.249Z
2022-11-07T17:12:30.249Z
```

Files can only be restored to their original location

SOPHOS

In the SafeStore log file you can see the ‘restonethreat’ command being run and the detected application being restored.

It is important to note that files can only be restored to their original location. If that location no longer exists, the restore operation will fail.

SafeStore Limitations

Note:

- An item can be a file or associated configuration
- When the limits are reached, the oldest items are removed
- Some data loss is possible

100
MB

SafeStore will not retain files larger than 100 GB

200
GB

SafeStore will use no more than 200 GB disk space

2000
Items

SafeStore will retain no more than 2000 items

SOPHOS

SafeStore has some limitations to prevent it from consuming too much disk space. These are:

- 100 MB file size limit per file. It is very uncommon for larger files to be detected as malware
- 200 GB limit on how much space SafeStore will use
- 2000 item limit on the number of items SafeStore will keep

Please note that an item can be a file or associated configuration such as registry keys. When the maximum number of files limit is reached, the oldest item will be removed from SafeStore. Due to these limitations some data loss is possible.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

When an item is released from the SafeStore, where is it restored to?

The location it was detected in

The temporary directory

The users downloads folder

The users documents folder

SOPHOS



Question 2 of 2

True or False: Sophos Central SafeStore encrypts all quarantined items.

True

False

SOPHOS

Chapter Review

When Sophos cleans up a file it is passed to SafeStore with its associated information. **SafeStore encrypts the file and associated information and stores it in the quarantine.**

Possible reasons for removing an item from the SafeStore;
Detected PUAs, incorrectly detected files or a false positive detection.

All **exclusions need to be thoroughly investigated before being applied** in Sophos Central. Any exclusion reduces your security.

SOPHOS

Here are the three main things you learned in this chapter.

When Sophos cleans up a file it is passed to SafeStore with its associated information. SafeStore encrypts the file and associated information and stores it in the quarantine.

You may want to release files from the SafeStore if they are incorrectly detected or a false positive detection.

All exclusions need to be thoroughly investigated before being applied in Sophos Central. Any exclusion reduces your security.



An Introduction to Sophos Central XDR

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection
CE4505: An Introduction to Sophos Central XDR

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

An Introduction to Sophos XDR

In this chapter you will learn what Sophos Central XDR is, and the primary XDR features available.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access Sophos Central
- ✓ How to protect and manage devices
- ✓ How to remediate threats manually
- ✓ How to view and acknowledge alerts and events in Sophos Central

DURATION 8 minutes

SOPHOS

In this chapter you will learn what Sophos Central XDR is, and the XDR features available.

What is Sophos Central XDR?

X D R

eXtended Detection and Response

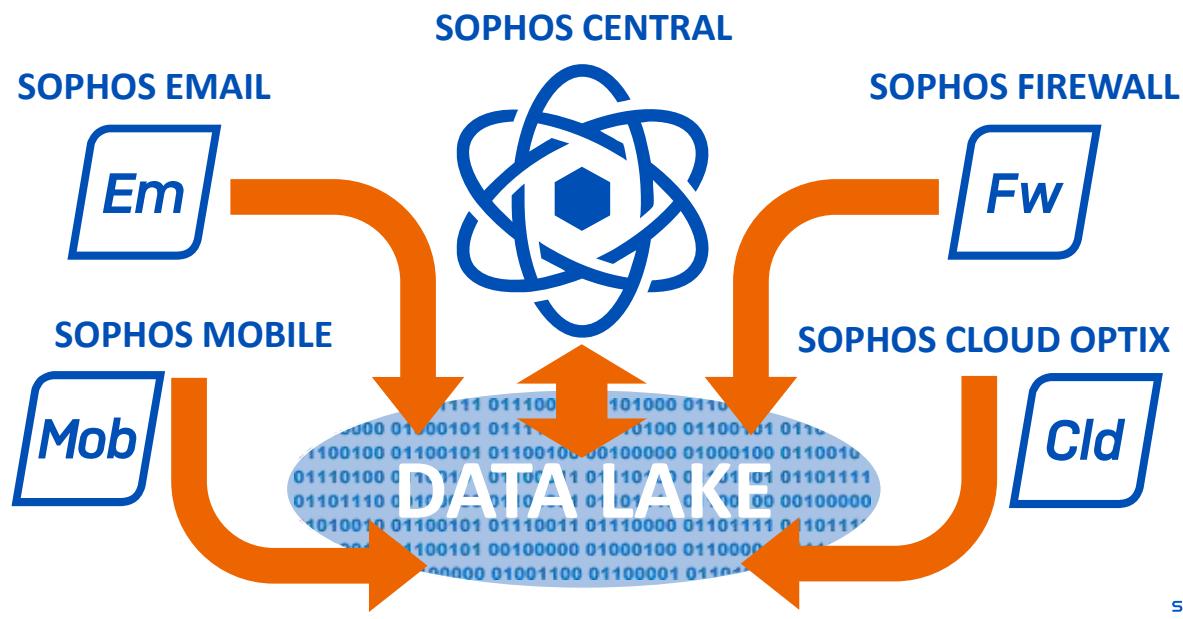
“Provides the tools that allow an administrator to have full visibility of what is happening across their estate.”

SOPHOS

Sophos Central XDR or Extended Detection and Response, provides the tools for administrators to have full visibility of what is happening across their estate.

Sophos Central XDR also leverages data from a Data Lake that allows you to perform cross product threat hunting investigations. This provides information from native endpoint, server, firewall, cloud, email, mobile, and Microsoft Office 365 integrations.

What is a Data Lake?



The Sophos Central Data Lake is a pool of information collected from protected computers and servers, Sophos Firewall, Sophos Email, Sophos Mobile, and Cloud Optix.

Sophos managed queries are run on protected devices at intervals to extract targeted information necessary for threat hunting investigation. Please note that not all the data collected from devices is stored in the Data Lake.

Data from Sophos Firewalls that have Central Firewall Reporting, and from Sophos Email with integrated Office 365 search and destroy enabled, are also included in the Data Lake, allowing you to perform cross product investigations.

Threat Analysis Center Dashboard

The screenshot displays the Sophos Threat Analysis Center Dashboard. On the left, a sidebar lists navigation options: Sophos Central XDR, Threat Analysis Center, Threat Maps, Log Monitor, Discover, Investigations, and Preferences. The main dashboard area is titled "Threat Analysis Center - Dashboard".

Recent Investigations: A table showing 10 recent investigations. Each row includes a status icon, ID, assigned to, ownership, age, last modified, total duration, and summary.

Priority	ID	Assigned to	Owner	Age	Last modified	Total duration	Summary
High	2022-08-21-001	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-002	Not Started	Sophos	4 day	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-003	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-004	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-005	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-006	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-007	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-008	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488
High	2022-08-21-009	Not Started	Sophos	4 days	Aug 21, 2022	11:58:02 AM	Initial Detection: 0001-MTR0-000000-11488

Recent detections: A heatmap showing the number of detections per hour and device type.

Most recent threat graph: A section showing threat graphs for various devices.

Recent live discover queries: A table showing recent live discover queries.

Recently scheduled queries: A table showing recently scheduled queries.

Using Sophos Central XDR, an administrator can view event and incident detections, determine the best response to a threat, and isolate devices on a network.

The **Dashboard** in the Threat Analysis Center displays recent investigations, detections, threat graphs, recent live discover queries, and recently scheduled queries.

Threat Graphs

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a sidebar lists navigation options: Threat Analysis Center, DETECTION AND REMEDIATION (Dashboard, Threat Graphs, Live Discover, Detections, Investigations, Integrations, Preferences), and a plus sign icon. The main area is titled "Threat Analysis Center - ML/PE-A". At the top right are links for Help, UK Training, and Sophos UK Support. Below the title is a horizontal timeline with icons: READING3 (IP address 192.168.1.168), Root Cause (Windows Explorer), Beacon (highscore.exe), Detected (Nov 2, 2022 8:35 PM), and Cleared. A summary table provides details: Detection name: ML/PE-A; Root cause: explorer.exe; Possible data involved: 3 business files; Where: On READING3; When: Detected on Nov 2, 2022 8:35 PM. To the right, suggested next steps include setting a status for the threat graph, isolating the device, scanning the device, and running a Live Discover query. A priority dropdown is set to Medium and a status dropdown is set to New. Below the summary is a "Graph record" tab, which is currently selected. It shows a network diagram with nodes: Windows Explorer and highscore.exe. An edge between them is labeled "ATTACH". Below the graph are filters: Processes (checked), Other files (unchecked), Business files (checked), Network connections (checked), and Registry keys (checked). A "Show direct path" button is available. To the right, there's a note about "Other file : highscore.exe" and a link to "Clean and block". A tooltip says "What does this bot do? Reproduced at time graph was created. Uncertain reputation.".

Threat Graphs show the event chain, details of the artifacts (processes, files, and keys) affected, and a diagram showing how the threat developed. This example displays a ML/PE-A detection triggered by opening a file called highscore.exe in Windows file explorer.

Live Discover

The screenshot shows the Sophos Threat Analysis Center interface. The left sidebar has a dark theme with white text and icons. It includes sections for 'DETECTION AND REMOVAL' (Dashboard, Threat Brains, Live Discover, Detections, Investigations, Integrations, Preferences), 'LIVE DISCOVER' (selected), and 'ATTACK & DEFENSE' (Cloud Optix, Compliance, Device). The main content area is titled 'Threat Analysis Center - Live Discover' and shows 'Overview / Threat Analysis Center Dashboard / Live Discover'. It features a 'Designer Mode' toggle, a query count of '18 Categories, 374 Queries', and three tabs: 'All Queries' (selected), 'Endpoint Queries', and 'Data Lake Queries'. Below these are sections for 'Queries that get data from devices or from the Data Lake' (Endpoint queries vs. Data Lake queries) and a search bar. The main grid displays various query categories with icons and counts: 'All queries [374] (All available queries)', 'Recent queries [20] (Queries run Recently)', 'Abnormal [0] (Unexpected activity or network connections)', 'ATT&CK ATTACK [26] (Queries based on attack tactics and techniques)', 'Cloud Optix [0] (Public cloud activity logs)', 'Compliance [44] (Compliance with security standards)', and 'Device [1] (Device OS performance)'. Each category has a small description below it.

The **Live Discover** tab is where you run queries against protected devices. You can use Live Discover queries to search devices for signs of threats that haven't been detected by other Sophos features. For example, unusual changes to the registry, failed authentications, or running processes that are rarely run.

You can also check the compliance and security health of each device. For example, you can search for out-of-date software or browsers with insecure settings.

Detections

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a dark sidebar lists navigation options: Dashboard, Threat Graphs, Live Discover, **Detections** (which is selected), Investigations, Integrations, and Preferences. The main content area is titled "Detections" and includes a breadcrumb trail: Overview > Threat Analysis Center Dashboard > Detections. At the top right are links for Help, UK Training, and the current user (Sophos UK - Super Admin). Below the title is a toolbar with buttons for Show filters, Export, and time ranges: Last 1 Hour, Last 24 Hours, Last 7 Days, Last 30 Days, and Custom range. A "Search" input field is also present. The main table displays five detection entries:

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Integrations	Rule	Investigations
Medium	2	Threat	Nov 24, 2022 5:28:19 PM	Execution	WinS...	5	EQL-WIN-EX...	
Medium	1	Vulnerability	Nov 24, 2022 5:28:06 PM		WinS...	5	COMPLIANCE...	
Medium	1	Vulnerability	Nov 24, 2022 5:22:14 PM		WinS...	5	COMPLIANCE...	
Medium	1	Threat	Nov 24, 2022 5:13:29 PM	Defense ...	WinS...	5	WIN-MITRE...	
Medium	1	Threat	Nov 24, 2022 5:13:29 PM	Defense ...	WinS...	5	WIN-MITRE...	

At the bottom right of the table, it says "Last updated: Dec 1, 2022, 7:15 PM".

The **Detections** page displays activities that you might need to investigate. Detections identify activity on your devices that's unusual or suspicious but hasn't been blocked. They're different from events where we detect and block activity that we already know to be malicious.

We generate detections based on data that devices upload to the Sophos Data Lake. We check that data against threat classification rules. When there's a match, we show a detection.

Investigations

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation links like Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is selected and highlighted in blue), Integrations, and Preferences. The main area is titled "Investigations" and displays a table of current investigations. The table has the following columns: Priority (with High, Medium, and Low options), Investigation ID (e.g., 2022-11-23-001, 2022-11-14-001, 2022-11-10-001, Training Example, Training Example), Status (Not Started, In Progress), Assigned to (Unassigned, Administra...), Created by (Sop...), Age (8 days, 17 days, 21 days, 23 days, 23 days), Devices (1, 5, 1, 1, 2), Integrations (1, 1, 1, 1, 1), Detections (2, 8, 3, 1, 5), Last modified (Nov 23, 2022, Nov 14, 2022, Nov 10, 2022, Nov 8, 2022, Nov 8, 2022), Last detection (Nov 23, 2022 3:17:31 PM, Nov 14, 2022 10:54:50 AM, Nov 10, 2022 11:25:33 AM, Nov 8, 2022 5:43:35 PM, Nov 8, 2022 5:38:19 PM), and Summary (Initial Detection: WIN-MITRE-Behavioral..., Initial Detection: WIN-MITRE-Behavioral..., Initial Detection: WIN-MITRE-Behavioral..., Created for demonstration, Initial Detection: WIN-MITRE-Behavioral...). At the bottom right of the table, it says "Last updated: Dec 1, 2022, 1:16 PM".

Priority	Investigation	Status	Assigned to	Created by	Age	Devices	Integrations	Detections	Last modified	Last detection	Summary
High	2022-11-23-001	Not Started	Unassigned	Sop...	8 days	1	1	2	Nov 23, 2022 8 days ago	Nov 23, 2022 3:17:31 PM	Initial Detection: WIN-MITRE-Behavioral...
High	2022-11-14-001	Not Started	Unassigned	Sop...	17 days	5	1	8	Nov 14, 2022 17 days ago	Nov 14, 2022 10:54:50 AM	Initial Detection: WIN-MITRE-Behavioral...
High	2022-11-10-001	Not Started	Unassigned	Sop...	21 days	1	1	3	Nov 10, 2022 21 days ago	Nov 10, 2022 11:25:33 AM	Initial Detection: WIN-MITRE-Behavioral...
Medium	Training Example	In Progress	Administr...	UK Train...	23 days	1	1	1	Nov 8, 2022 23 days ago	Nov 7, 2022 5:43:35 PM	Created for demonstration
Medium	Training Example	In Progress	Administr...	UK Train...	23 days	2	1	5	Nov 8, 2022 23 days ago	Nov 7, 2022 5:38:19 PM	Initial Detection: Last updated: Dec 1, 2022, 1:16 PM

On the **Investigations** tab, suspicious events reported by detections are grouped together to help you carry out forensic investigation tasks.

Investigations are created automatically when a high-risk activity is detected.

Integrations

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a dark sidebar lists navigation options: Threat Analysis Center, DETECTION AND REMEDIATION (Dashboard, Threat Briefs, Live Discover, Detections, Investigations), and the active Integrations tab. The main content area has a light blue header bar with the title 'Integrations' and a note about temporary data processing in the United States. Below this is a help message about best practices for multiple sub-estates. A navigation bar at the top right includes 'Help', 'UK Training', 'Sophos UK - Super Admin', and a search bar. The main content area displays a table titled 'Configured Integrations (1)'. It shows one entry: 'Microsoft - Office 365 Management Activity API'. This entry includes a red Microsoft logo icon, status indicators for 'Purchased' (green checkmark), 'Configured' (green checkmark), 'API' (blue), and 'Sophos XDR' (blue). A detailed description of the integration follows: 'Office 365 Management Activity includes information about user, admin, system, and policy actions and events from Office 365 and...'. Below the description are three status metrics: 'Last Synced' (Feb 1, 2022), 'Total Integrations' (1), and 'Health Status' (Green Online).

The **Integrations** tab is where you can integrate a third party product or service with Sophos Central. For example, you can add Sophos Cloud Optix anomaly alerts to Sophos Central.

When a third party product or service is integrated with Sophos Central, it can send data to the Sophos Data Lake. This allows you to query data using Live Discover for Sophos Central protected devices as well as third party products and services.

Please note that only users with the Admin or Super Admin role can view and configure integrations.

Preferences

The screenshot shows the Sophos Threat Analysis Center preferences interface. The left sidebar has a dark theme with various navigation options like Dashboard, Threat Briefs, Live Discover, Investigations, and Preferences (which is selected). The main area title is "Threat Analysis Center - Preferences". Below it are tabs for "Enrichments", "Scheduled queries" (which is active), and "Email notifications". The "Scheduled queries" tab displays a table of scheduled queries. The table has columns for Query name, Frequency, Admin name, Devices queried, Schedule status, Last edited, and Actions. There are three entries: "Pending Windows updates Data Lake 2022-11-02" (Weekly, UK Training, All devices queried, Enabled, Nov 2, 2022 11:42 AM), "Pending Windows updates" (--, UK Training, All devices queried, Disabled, Jun 30, 2021 11:18 AM), and "User Authentication" (Weekly, UK Training, All devices queried, Enabled, Jun 25, 2021 3:50 PM). A search bar is at the top of the table.

Query name	Frequency	Admin name	Devices queried	Schedule status	Last edited	Actions
Pending Windows updates Data Lake 2022-11-02	Weekly	UK Training	All devices queried	Enabled	Nov 2, 2022 11:42 AM	
Pending Windows updates	--	UK Training	All devices queried	Disabled	Jun 30, 2021 11:18 AM	
User Authentication	Weekly	UK Training	All devices queried	Enabled	Jun 25, 2021 3:50 PM	

The **Preferences** tab is where you can view enrichments, scheduled queries, and email notifications for investigations.

Live Discover lets you select data items in your query results and use them as the basis for further actions, including enrichments. Enrichments open third party websites to look up information about a potential threat you've found. We provide predefined enrichments and you can also add your own.

If you scheduled a query in Live Discover, it will be listed in the **Scheduled queries** tab.

You can select which administrators to send email notifications to when an investigation is changed. By default, an email is sent when a new investigation is created and when an administrator is assigned to an investigation.

Live Response

The screenshot shows the Sophos Central XDR interface. On the left, the navigation menu includes sections like Sophos Central, Devices, Dashboards, Alerts, Threat Analysis Center, Log & Reports, People, Devices (which is selected and highlighted in blue), Global Settings, Protect Devices, and Account Health Check. Under MY PRODUCTS, there are links for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, Firewall Management, and Phish Threat. The main content area is titled 'WinClient2' and shows a summary of recent events. At the top of the summary section, there are tabs for SUMMARY, EVENTS, STATUS, and POLICIES. The SUMMARY tab is selected. Below the tabs, there's a 'Recent Events' section with a 'View More' link. A large orange box highlights the 'Live Response' section. An arrow points from the 'Live Response' button in the sidebar to the main window. The main window has a title 'Live Response - WinClient2'. It displays a terminal session with the Windows command prompt. The terminal output shows 'Windows [Version 10.0.19041.222] Copyright (c) Microsoft Corporation. All rights reserved.' and the path 'C:\Windows\system32'. There are also status indicators for Device Encryption and Assets.

Live Response is an extended response feature that is included with Sophos Central XDR. Live Response allows administrators to remotely connect to a protected device to carry out support and investigative tasks.

Live Response is available on each individual device page.

Sophos XDR Sensor

Threat Detection Capabilities

- On-device behavior and cloud-based detections
- Does not include detection of exploits, the use of machine learning or AMSI protection

Threat Investigation Capabilities

- On-demand Live Discover queries
- Scheduled Live Discover queries

SOPHOS

Sophos Central XDR includes a Sophos XDR sensor which is designed for organizations who want to benefit from Sophos' detection, investigation, and response capabilities without having the Sophos Endpoint Agent installed.

The Sophos XDR Sensor operates in a detection and response-only mode, which means it does not provide automated protection or prevention actions. The organization must continue to rely on any existing third-party protection tools but will benefit from the capabilities included with the Sophos XDR Sensor.

These capabilities include on-device behaviour, cloud-based detections, and Live Discover.

Sophos XDR Sensor

The screenshot shows the Sophos Central interface under the 'Protect Devices' section. On the left sidebar, 'Protect Devices' is selected. The main content area has a heading 'How do I use the installers for endpoints and servers?'. It includes sections for 'Endpoint Protection' (with links to Windows and macOS installers), 'Unified Endpoint Management and Sophos Intercept X for Mobile' (with a note about device management and mobile threat defense), and 'XDR Sensor Installers' (which is highlighted with a red box). The 'XDR Sensor Installers' section notes that it sends detection data to the Sophos Data Lake and provides links to download Windows and macOS installers.

Sophos XDR Sensor installation is only supported on Windows 10 x64 or later, and macOS Big Sur 11 or later. The installer is pre-configured to only install the XDR Sensor and does not run the competitor removal tool.

Sophos XDR sensor should only be installed on devices that do not have the Sophos Endpoint Agent installed.

Sophos XDR Sensor

The screenshot shows the Sophos Central interface for managing endpoint protection. The left sidebar has 'Endpoint Protection' selected under 'ANALYST'. The main area is titled 'Endpoint Protection - Computers' and shows a list of managed computers. The first computer, 'Windows-XHD', is highlighted with an orange border. The columns in the table are: Name, IP, OS, Protection, Encryption, and Last User. The 'Protection' column for Windows-XHD displays 'XDR Sensor - Intercept X Advanced with XDR'.

Name	IP	OS	Protection	Encryption	Last User
Windows-XHD	192.168.1.184	Windows 10 Enterprise	XDR Sensor - Intercept X Advanced with XDR		Administrator
Training-W10	192.168.1.185	Windows 10 Enterprise	Intercept X Advanced with XDR		Administrator
WinClient1	172.16.16.70	Windows 10 Pro	Intercept X Advanced with XDR		administrator
WinClient2	172.16.16.80	Windows 10 Pro	Intercept X Advanced with XDR		administrator
WinClient4	172.16.16.100	Windows 10 Pro	Intercept X Advanced with XDR		administrator
WinClient3	172.16.16.80	Windows 10 Pro	Intercept X Advanced with XDR		administrator
WinClient5	172.16.16.110	Windows 10 Pro	Intercept X Advanced with XDR		administrator

Following installation, the device will be listed in Sophos Central. In the ‘Protection’ column, the license will display as XDR Sensor.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Which of these Sophos products can contribute information to the Data Lake?

Sophos Email

Sophos Wireless

Sophos Mobile

Sophos Phish Threat

Sophos Cloud Optix

Sophos Firewall

SOPHOS



Question 2 of 2

What feature allows administrators to remotely connect to a protected device?

Investigations

Live Discover

Live Response

Endpoint Self Help

SOPHOS

Chapter Review

XDR is an abbreviation for Extended Detection and Response.

Sophos Central XDR includes threat graphs, Live Discover, detections, investigations, integrations and Live Response.

Sophos Central XDR uses a Data Lake which is a pool of information collected from protected devices.

SOPHOS

Here are the three main things you learned in this chapter.

XDR is an abbreviation for Extended Detection and Response.

Sophos Central XDR includes threat graphs, Live Discover, detections, investigations, integrations, and Live Response.

Sophos Central XDR uses a Data Lake which is a pool of information collected from protected devices.



Sophos Central XDR Licensing

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4510: Sophos Central XDR Licensing

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central XDR Licensing

In this chapter you will learn how Sophos Central XDR is licensed.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to apply Sophos Central licenses
- ✓ What Sophos Central XDR is and the core features of Sophos Central XDR

DURATION **3 minutes**

SOPHOS

In this chapter you will learn how Sophos Central XDR is licensed.



Additional information in
the notes

Sophos Central XDR Licensing

Sophos Central XDR is included in the following licenses:



Intercept X Advanced with XDR



Intercept X Advanced for Server with XDR



Intercept X Advanced with MTR Standard



Intercept X Advanced for Server with MTR Standard



Intercept X Advanced with MTR Advanced



Intercept X Advanced for Server with MTR Advanced

SOPHOS

Sophos Central XDR is included in the licenses displayed here.

Click **Continue** when you are ready to proceed.

[Additional Information]

You can find a full list of features included in each license here: <https://www.sophos.com/en-us/mediabinary/PDFs/factsheets/sophos-intercept-x-license-guide.pdf>

Sophos XDR Licensing

USER COUNT

The highest value of A or B

A = Number of user licenses for XDR/MTR/Email Advanced/Mobile

B = Number of users protected by Sophos Firewall (if used)



SERVER COUNT

The number of Server XDR/MTR licenses



Number of required XDR Licenses

SOPHOS

To make use of the XDR features, you need to ensure you have the appropriate quantity of subscriptions, plus the number of Sophos XDR licenses equal to the sum of the users in the estate.

To calculate the number of XDR licenses you first need to count how many user licenses you have. This is either the total number of licenses that cover XDR, MTR, Email Advanced, and Sophos Mobile or the total number of users protected by Sophos Firewall, if it is being used. Whichever number is greater is the number you use.

You then add the server count, which is the number of Server XDR and MTR licenses. Add the server count to the user count to give you the number of required XDR licenses.

Licensing Examples

Scenario One



100 Endpoints



10 Servers

SOPHOS

Let's look at some licensing scenarios.

In the first scenario, we have a new customer with 100 endpoints and 10 servers. How many XDR licenses are required?

Licensing Examples

Scenario One

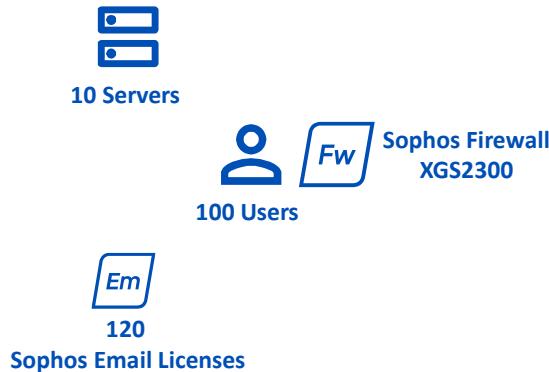


SOPHOS

In this scenario, 110 XDR licenses are required.

Licensing Examples

Scenario Two



SOPHOS

In the second scenario, we have a new customer with 10 servers, a Sophos Firewall with 100 users behind the firewall, and 120 Sophos Email Licenses.

How many XDR licenses are required?

Licensing Examples

Scenario Two



SOPHOS

In this scenario, 130 XDR licenses are required. This is because there are 10 servers plus 120 email licenses. The number of email licenses is more than the total users.

Licensing Examples

Scenario Three



Sophos Firewall
XGS2300

SOPHOS

In our last scenario, an existing Sophos customer has a Sophos Firewall with 100 users behind the firewall and 100 endpoints.

How many XDR licenses are required?

Licensing Examples

Scenario Three



100 Endpoints



100 Users



Sophos Firewall
XGS2300



100 XDR licenses are required

SOPHOS

In this scenario 100 XDR licenses are required.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 1

You have **150** users behind a Sophos Firewall, and you have **150** endpoints and **15** servers.
Enter the number of XDR licenses that are required.

SOPHOS

Chapter Review

To benefit from all the **XDR features**, you must have the **appropriate licenses applied**.

XDR Licensing is based on the **total number of users** plus the **total numbers of servers** licensed.

SOPHOS

Here are the two main things you learned in this chapter.

To benefit from all the XDR features, you must have the appropriate licenses applied.

XDR licensing is based on the total number of users, either the total number of users covering endpoint, server, email, and mobile, or the total number of users protected by a Sophos Firewall if it is being used. The greater number of users is used and added to the total number of servers licensed.



Getting Started with Sophos Central XDR Data Lake

Sophos Central Endpoint and Server Protection

Version: 4.0v1

SOPHOS

[Additional Information]

Sophos Central Endpoint and Server Protection

CE4515: Getting Started with Sophos Central XDR Data Lake

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central XDR Data Lake

In this chapter you will learn what the Sophos XDR Data Lake is and how to enable it.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

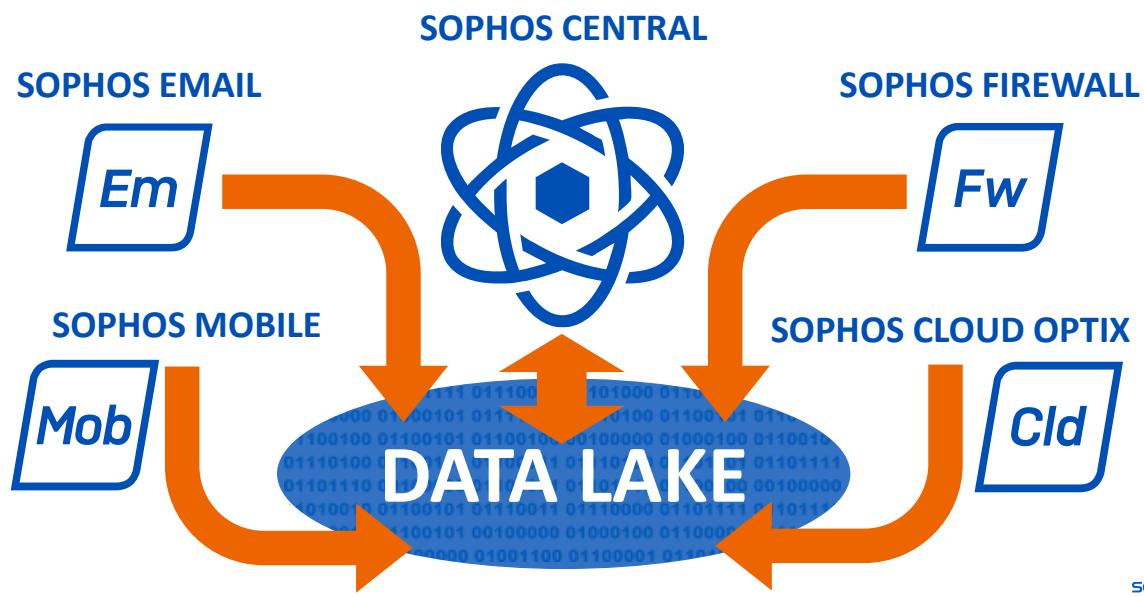
- ✓ Understand what Sophos XDR is
- ✓ How to configure Sophos Central global settings
- ✓ How to protect and manage devices with Sophos Central

DURATION **4 minutes**

SOPHOS

In this chapter you will learn what the Sophos XDR Data Lake is, and how to enable it.

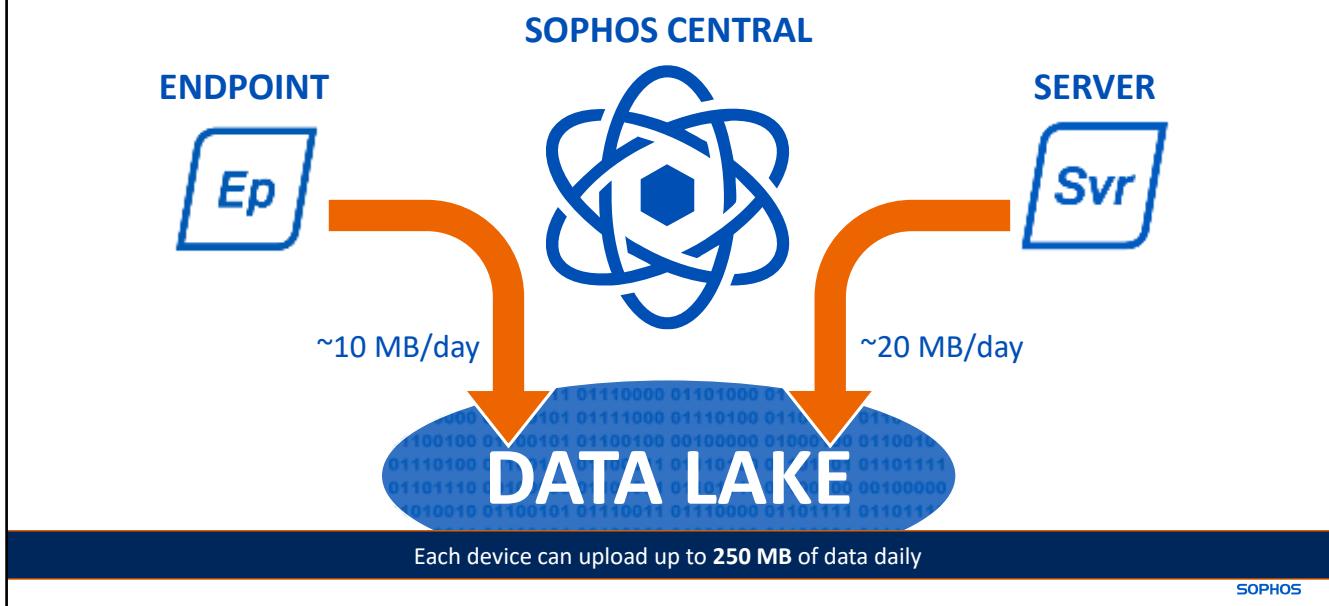
What is a Data Lake?



The Sophos Data Lake is a pool of information that can be collected from protected devices, Sophos Firewall, Sophos Email, Sophos Mobile, and Cloud Optix.

Sophos managed queries are run on protected devices at regular intervals to extract targeted information that could be useful when running a threat hunting investigation. Please note that not all available data from devices is stored in the Data Lake.

Data Lake Storage Limits



The amount of information sent to the Data Lake is dependent on the activity of the device and the queries that are run to collect the information.

A typical Windows endpoint will send about 10 MB of data per day, and a Windows server will send approximately 20 MB per day. This will vary because it is heavily dependent on what is running on those devices.

Each device can upload up to 250 MB of data daily. When devices reach this limit, they don't send or store more data until the limit is reset. On Windows, the reset occurs at midnight local time for that device. On Linux, the reset occurs every twenty four hours since the service started.

Data Lake Capabilities



Stores data for **30 days**



Stores data from cross-product sources and enables **cross-product querying**



Run queries against **online** or **offline** devices even when a device longer exists



Queries against the Data Lake **do not cause additional CPU load** on the devices

SOPHOS

The Data Lake stores data for thirty days. You can run queries against the stored information, whether the protected devices are online or offline, this includes devices that may have been wiped or re-imaged.

Data Lake queries do not cause additional CPU load on protected devices as the query is looking at the stored data. In comparison, Live Discover can access up to 90 days of data on a device, however, devices must be online to query the data.

Using the Data Lake, you can run multiple queries against the latest stored data of your whole estate.

Enabling Data Lake Uploads

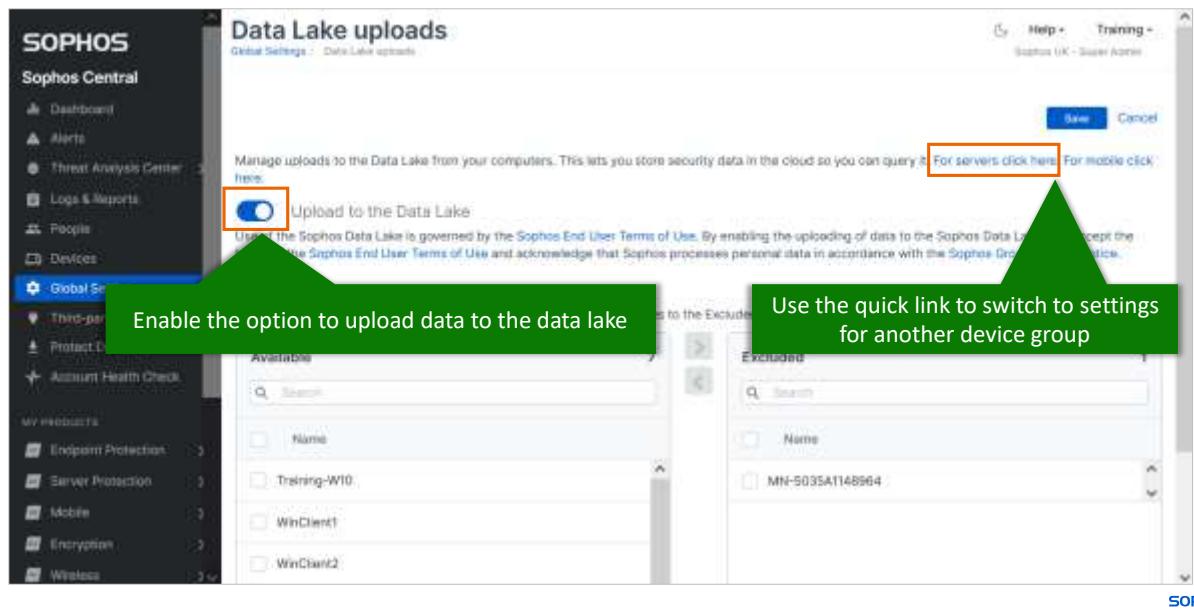
The screenshot shows the Sophos Central interface. The left sidebar has sections like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected), Third-party Connectors, Protect Devices, and Account Health Check. Under Global Settings, there are sections for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security, and Firewall Management. The Endpoint Protection section includes SSL/TLS decryption of HTTPS websites, Control decryption of websites and manage exclusions, and Device Migration. The Server Protection section includes Add Cloud Environments, Control Updates, and Live Response. Both sections have a 'Data Lake uploads' sub-section with the sub-description 'Control uploads to the Data Lake'. These sub-sections are highlighted with orange boxes. The bottom right corner of the screenshot area has the word 'SOPHOS'.

- To collect data from protected devices you must enable data lake uploads.
- Independent settings for endpoints and servers
- **Global Settings > Data Lake uploads**

To start collecting data from protected devices, you need to enable **Data Lake uploads** in your Sophos Central account.

Data Lake uploads are enabled independently for endpoints and servers. Navigate to **Global Settings** to access the **Data Lake uploads** setting for each device type.

Enabling Data Lake Uploads



Once you select a **Data Lake uploads** setting, you will see the option to ‘Upload to the Data Lake’. There is also a link included for the Data Lake upload settings for other device types.

Enabling Data Lake Uploads

The screenshot shows the 'Data Lake uploads' configuration page in Sophos Central. On the left, a sidebar lists various product categories like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings. Under Global Settings, 'Third-party Connectors' is expanded, showing Protect Devices and Account Health Check. The main panel has a title 'Data Lake uploads' and a sub-section 'General Settings: Data Lake uploads'. It includes a note about managing uploads to the Data Lake from computers, a toggle switch for 'Upload to the Data Lake' (which is turned on), and terms of use. Below this is a section titled 'Exclusions' with a note about disabling uploads for specific devices. Two tables are present: 'Available' (containing 'Training-W10', 'WinClient1', and 'WinClient2') and 'Excluded' (containing 'MN-503SAT148964'). At the bottom right is the 'SOPHOS' logo.

Once you have enabled Data Lake uploads, you can select to exclude individual servers or computers. Simply select the devices you want to exclude from the Data Lake upload and move them to the excluded table.

Remember to save your changes.

Data Lake Queries

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a dark sidebar lists navigation options: Dashboard, Threat Graphs, Live Discover (which is selected and highlighted in blue), Detection & Remediation, Defenses, Investigations, and Preferences. The main content area is titled "Threat Analysis Center - Live Discover" and includes a "Designer Mode" toggle. Below this, a navigation bar has tabs for All Queries, Endpoint Queries, and Data Lake Queries (the latter is also highlighted in blue). A tooltip for the Data Lake Queries tab explains: "Queries that are sent to a cloud repository. The devices don't need to be online. Data may be 15 minutes old." The main pane displays a "Cloud" icon and text about Data Lake queries getting data from the Data Lake. It features a search bar and several cards: "All queries [102]" (All available queries), "Recent queries [10]" (Queries run recently), "Anomalies [10]" (Unusual activity or new connections), "Cloud Optix [0]" (Public cloud activity logs), "Compliance [216]" (Compliance with security standards), "Devices [13]" (Device OS, patches, services, and more), and "ATT&CK [98]" (Sources based on attack tactics and techniques).

To run a Data Lake query, navigate to the **Threat Analysis Centre > Live Discover**. Select the **Data Lake Queries** tab to only view queries that can be run against the Data Lake.

Data Lake Queries

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with navigation options: Dashboard, Threat Graphs, Live Discover (which is selected and highlighted in blue), Defenses, Investigations, and Preferences. The main area is titled "Threat Analysis Center - Live Discover" and shows a query result for "User Account Control turned off (Data Lake)". The query is listed under the "User" category. A note indicates that this query checks whether User Account Control is turned off. Below the query, there's a section for "Sources" with "Data Lake" selected. A message states that no system impact data is available. At the bottom, there's a "Select a Time Period" dropdown with "Last 24 Hours" selected, and buttons for "Run Query" and "Schedule Query".

When you run a Data Lake query there is no need to select devices. This is because the queries are run on all the sources of information available in the Data Lake.

All results returned when a Data Lake query is run are stored in the Data Lake.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

What is the daily data allowance in megabytes per device to the Data Lake?
(enter a numerical value)

SOPHOS



Question 2 of 2

What is a benefit of running queries against the Data Lake?

Computers do not have to be online

Data is stored for 90 days

Select the devices to query

SOPHOS

Chapter Review

The Data Lake is a pool of information collected from protected devices.

You must enable Data Lake uploads for endpoints and servers independently and each device can upload up to 250 MB of data daily to the Data Lake.

Data Lake Queries are run against stored device information in the Data Lake.

SOPHOS

Here are the main things you learned in this chapter.

The Data Lake is a pool of information collected from protected devices.

You must enable Data Lake uploads for endpoints and servers independently and each device can upload up to 250 MB of data daily to the Data Lake.

Data Lake Queries are run against stored device information in the Data Lake.



Getting Started with Sophos Central XDR Live Discover

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4525: Getting Started with Sophos Central XDR Live Discover

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central XDR Live Discover

In this chapter you will learn what Live Discover is, and how to run Live Discover queries.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Sophos Central XDR is
- ✓ How to access and navigate Sophos Central
- ✓ How to protect and manage devices

DURATION **9 minutes**

SOPHOS

In this chapter you will learn what Live Discover is, and how to run Live Discover queries.

Live Discover

Provides the ability to run remote queries across multiple devices on your network



Queries return live and historic data for up to **90 days** of activity



Visibility into what is happening in your environment



Discovering risks **before** they result in a **breach**

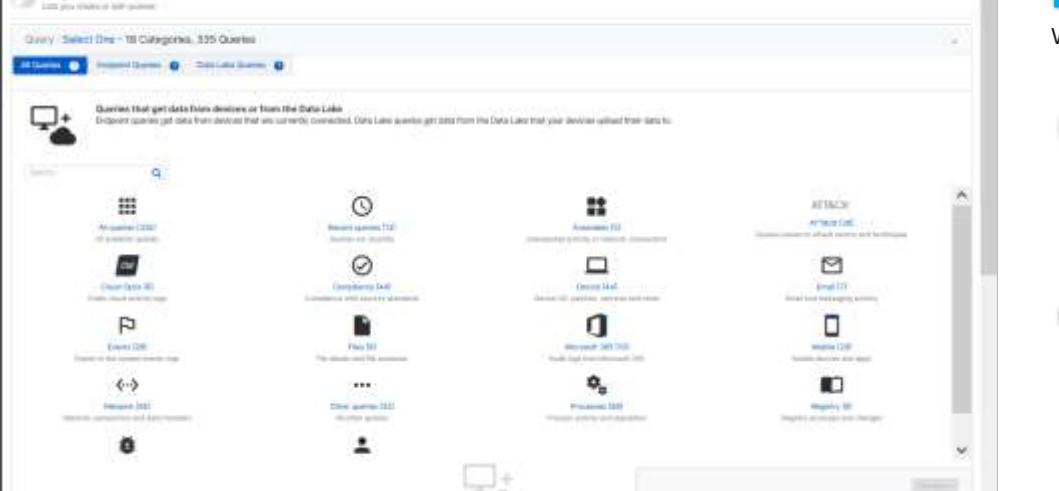


Performing **real-time threat investigations** and **security monitoring**

SOPHOS

Live Discover is a powerful search tool that provides the ability to run queries across multiple devices on your network. Queries can return live and historic data for up to 90 days of activity providing IT insight, advanced threat hunting as well as visibility into what is happening in your environment. Live Discover can be used to discover risks before they result in breaches and for performing real-time threat investigations and security monitoring.

Live Discover



The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. The left sidebar includes links for Threat Analysis Center, Live Discover, Threat Details, Threat Maps, and Preferences. The main area displays a grid of threat analysis categories:

- Attackers (200) - Malicious actors
- Cloud Spots (30) - Cloud-based malware
- Events (20) - Events on the system timeline
- Network (20) - Network connections and anomalies
- Script (5) - Scripts you wrote or imported
- Device (14) - Device (IP, port, connection and more)
- File (3) - File analysis and anomalies
- Process (12) - Process activity and anomalies
- Registry (3) - Registry changes and imports
- Services (1) - Services you created
- System (4) - System activity and anomalies
- Windows (1) - Windows-specific anomalies
- Unknown (11) - Unknown anomalies

At the top, there are tabs for Device, Hosted Device, and Data Lake Device, along with a search bar and a "Run Now" button.

Live Discover is based on OSQuery (an open source project) and leverages SQL query.

You can run a remote query for simple queries such as when was a device last patched. You can also ask more complex queries that return the standard deviation and variants of network communications of a device over a specific time period looking for anomalies.

Live Discover is supported on Windows, macOS and Linux operating systems. Please note that these operating systems have different schemas, therefore some pre-defined queries may only be available for specific operating systems.

Query Selection

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, a sidebar menu includes 'Threat Analysis Center' (selected), 'Dashboard', 'Threat Graphs', 'Live Discover' (highlighted in blue), 'Detections', 'Investigations', and 'Preferences'. The main area has a title 'Threat Analysis Center - Live Discover' and a sub-section 'Overview - Threat Analysis Center Dashboard - Live Discover'. A 'Designer Mode' toggle is shown. Below is a 'Query' section with the text 'Select One - 18 Categories, 345 Queries'. A 'Device selector' section shows '25 Endpoints available' with a note 'No endpoints selected'. A green callout box points to the 'Expand or minimize sections' button in the top right corner. A red box highlights the 'Available devices' tab under the device selector. A sidebar titled 'Filters' lists categories like Online Status, Name, Type, Operating system, Last user, Group, IP address, and Health status. The 'Available devices' table shows one entry: Training-W13, Computer, Windows 10 Enterprise, TRAINING-W13\Training.

Online status	Name	Type	OS	Last user
Online	Training-W13	Computer	Windows 10 Enterprise	TRAINING-W13\Training

The menu items in Live Discover can be expanded or minimized. Here we can see the 'Query' section is minimized and the 'Device selector' section is expanded.

Query Selection

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with navigation links like Detection, Threat Graphs, Live Discover (which is selected and highlighted in blue), Detections, Investigations, and Preferences. The main area is titled "Threat Analysis Center - Live Discover" and shows a "Designer Mode" toggle. Below that, it says "Query : Select One = 18 Categories, 345 Queries". There are three tabs: "All Queries" (selected), "Endpoint Queries" (with 7 items), and "Data Lake Queries" (with 7 items). A section titled "Queries that get data from devices or from the Data Lake" explains the difference between Endpoint and Data Lake queries. Below this, there are several cards for different query categories: "All queries [345]" (with a grid icon), "Recent queries [18]" (with a clock icon), "Anomalies [0]" (with a double bar chart icon), "ATT&CK [28]" (with a shield icon), "Cloud Optix [0]" (with a cloud icon), "Compliance [44]" (with a checkmark icon), "Device [44]" (with a laptop icon), and "Email [81]" (with an envelope icon). A search bar is at the top of the main content area.

Pre-defined or ‘canned’ queries are provided by Sophos, and over time additional queries will be added. These are queries that are available for use without the need for editing. For example, you can run a canned query that will list all registry keys that have been modified in the last 3 days.

Sophos’ canned queries are assigned to one or more categories using a tagging mechanism. You can view all queries that are available in the ‘All Queries’ category. You can also view any recent queries you have used. All other categories are listed alphabetically and include categories such as device, events, hunting and forensics, and network activity.

Query Selection

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Threat Analysis Center' and 'DETECTION AND REMEDIATION' sections containing 'Dashboard', 'Threat Graphs', 'Live Discover' (which is selected and highlighted in blue), 'Detections', 'Investigations', and 'Preferences'. The main area is titled 'Threat Analysis Center - Live Discover' with a sub-section 'Overview - Threat Analysis Center Dashboard / Live Discover'. It features a 'Designer Mode' toggle switch. Below this, a message says 'Query : Select One = 18 Categories, 345 Queries.' There are three tabs: 'All Queries' (selected), 'Endpoint Queries' (with a question mark icon), and 'Data Lake Queries' (with a question mark icon). A large green callout box points to the search bar, which contains the text 'table' and has an orange border. The callout box also contains the text 'Searches will return queries from all categories'. Below the search bar is a link '[Back to categories](#)'. The main table lists 18 categories with 345 queries. The columns are: Name, Description, Category (which is highlighted with an orange border), Source, System Impact, Created by, and Last modified. The first three rows are: 'App compatibility vulnerability ...' (Category: Compliance, Source: Data Lake, Created by: Not Available, Last modified: Jun 04, 2021); 'Application compatibility shims ...' (Category: Threat hunting, Source: Windows, Created by: Not Available, Last modified: Jul 21, 2021); and 'Core table certificates' (Category: Other queries, Source: Linux, macOS, Not Available, Last modified: Jun 18, 2021).

Name	Description	Category	Source	System Impact	Created by	Last modified
App compatibility vulnerability ...	Lists applications with special comp...	Compliance	Data Lake	Not Available	S	Jun 04, 2021
Application compatibility shims ...	Application compatibility shims can ...	Threat hunting	Windows	Not Available	S	Jul 21, 2021
Core table certificates	Core table certificates	Other queries	Linux, macOS	Not Available	UK Training	Jun 18, 2021

You can search for queries and all searches return matching queries from all categories. The list returned will display the query name, description, and category of each available query.

The sources column indicates which operating system the query is supported by and, where necessary, also indicates if it is a Data Lake or Endpoint query. The system impact will only be listed for those queries already run. The created by column indicates who created the query. All canned queries are indicated with the Sophos 'S' icon.

Query Selection

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with navigation links: Dashboard, Threat Drives, Live Discover (which is highlighted in blue), Defectors, Investigations, and Preferences. The main area is titled "Threat Analysis Center - Live Discover" and shows a query named "Brute force logons (Data Lake)". Below the query, it says "Events: Brute force logons (Data Lake)" and "Source: Data Lake". A callout box with a green arrow points from the text "Run new queries on a single device to test system impact" to the "Source: Data Lake" section. The callout box contains the text "Run new queries on a single device to test system impact". The top right corner of the interface shows "Help", "UK Training", "Sophos UK", and "Super Admin".

Once you select a query to run, the expected device impact is displayed. As we mentioned, any query that has not been run in your environment will have no expected system impact. We recommend running a new query on a single device to determine the system impact of running the query.

Device Selector

Device selector (25 Endpoints available)

No endpoints selected

Available devices Selected devices

Filters

Online Status: Online Offline

Name

Type: Server Computer

Operating system

Last user

Group

IP address

Health status

Reset to defaults Apply

Displaying 1 - 8

Online status	Name	Type	OS	Last user
Online	WinClient1	Computer	Windows 10 Pro	WINCLIENT1\Sophos
Online	WinClient2	Computer	Windows 10 Pro	WINCLIENT2\Sophos
Online	WinClient3	Computer	Windows 10 Pro	TRAININGDEMO\anable
Online	WinClient4	Computer	Windows 10 Pro	
Online	WinClient5	Computer	Windows 10 Pro	WINCLIENT5\TrainingDem
Online	WinServer1	Server	Windows Server 2019	TRAININGDEMO\administr

05

To run an Endpoint Live Discover query, you must select at least one device.

Online devices are automatically displayed, however, you can filter the list to display offline devices, specific device groups, only Windows devices, and more to suit your needs. You can select one or more devices to run the query against.

Once you have selected the devices click **Update selected device list**. If you need to remove devices, click the tick box to de-select them from the list and click **Update selected device list**. The number of devices will be updated.

Run a Query

The screenshot shows the 'Device selector' interface with 25 endpoints available. The 'Available devices' tab is selected. A sidebar on the left contains filters for Online Status (Online checked, Offline unchecked), Name, Type (Server and Computer checked), Operating system, Last user, Group, IP address, and Health status. The main table lists 8 devices, all marked as 'Online'. The columns include Name, Type, OS, and Last user. The 'Run Query' button at the bottom right is highlighted with a red box.

Online status	Name	Type	OS	Last user
<input checked="" type="checkbox"/> Online	WinClient1	Computer	Windows 10 Pro	WINCLIENT1\Sophos
<input checked="" type="checkbox"/> Online	WinClient2	Computer	Windows 10 Pro	WINCLIENT2\Sophos
<input type="checkbox"/> Online	WinClient3	Computer	Windows 10 Pro	TRAININGDEMO\anable
<input type="checkbox"/> Online	WinClient4	Computer	Windows 10 Pro	
<input type="checkbox"/> Online	WinClient5	Computer	Windows 10 Pro	WINCLIENT5\TrainingDem
<input type="checkbox"/> Online	WinServer1	Server	Windows Server 2019	TRAININGDEMO\administr
<input type="checkbox"/> Online	WinServer2	Server	Windows Server 2019	TRAININGDEMO\admind

For an Endpoint Live Discover query, once at least one device is selected, the **Run Query** option is displayed.

When you run a query for the first time, you may see a warning message. This is to notify you that the query you are about to run is untested in your environment.

There is minimal impact of running a query on your devices, and you can run a query across thousands of devices. Up to one hundred thousand rows of response data can be returned.

Query Results

The columns returned are determined by the data tables included in the query

The table schema query will list all the data tables available

source	eventid	Date_Time	Login_Count	LoginType	IP_Address	TargetUserName	data
WinClient2	4824	2022-08-18 14:50:09	6	10	192.168.1.180	administrator	{"EventData":
WinClient2	4824	2022-08-18 14:18:47	8	3	192.168.1.180	Administrator	{"EventData":
WinClient2	4824	2022-08-18 14:18:47	8	3	192.168.1.180	Administrator	{"EventData":
READING3					0.0.0.0	Administrator	{"EventData":
READING3					127.0.0.1	Administrator	{"EventData":
READING3					192.168.1.205	Administrator	{"EventData":
READING3	4824	2022-10-08 16:17:41	3	2	192.168.1.205	Administrator	{"EventData":
WinClient1	4824	2022-08-30 08:19:00	2	10	192.168.1.180	administrator	{"EventData":
WinClient1	4824	2022-08-30 08:19:31	2	3	192.168.1.180	Administrator	{"EventData":
WinClient4	4824	2022-10-07 14:05:57	1	10	192.168.1.180	administrator	{"EventData":
WinClient4	4824	2022-10-08 10:10:21	7	11	192.168.1.180	Administrator	{"EventData":
WinClient4	4825	2022-10-08 10:10:10	5	2	192.168.1.180	Administrator	{"EventData":

Queries are written to pull information from data tables that are populated with your device information.

The query ‘table schema’ provides a list of all the data tables that can be included in queries. If a canned query does not provide you with the data you want, you can choose to edit an existing query or create your own.

Query Results

The screenshot shows the Sophos Central XDR interface with the 'Live Discover' tab selected. A search bar at the top contains the query 'Auth History for a Username'. Below it, a table displays the results with columns: Username, eventid, Date_Time, LogonType, Domain, SourceIP, User, and Status. The table lists 10 entries from various clients (WinClient1 to WinClient10) and users (Administrator, sophosuser). A green callout box points to the 'Export' button in the top right corner of the table header, which is highlighted with a red border. Another green callout box points to the ellipsis menu icon (three dots) in the 'User' column of the first row, also highlighted with a red border. The text inside these boxes reads: 'You can export the returned data' and 'The ellipsis indicates that further actions can be taken based on the data returned in the query' respectively.

Username	eventid	Date_Time	LogonType	Domain	SourceIP	User	Status
WinClient2	...	4624	2022-08-18 14:50:09	6	10.0.0.1100	...	administrator
WinClient2	...	4624	2022-08-18 14:18:47	9	10.0.0.1100	...	Administrator
WinClient2	...	4624	2022-08-18 14:18:55	8	10.0.0.1100	...	Administrator
READING3	...	4624	2022-09-19 09:30:00	10	0.0.0.0	...	Administrator
READING3	...	4624	2022-09-19 09:30:00	10	0.0.0.0	...	Administrator
READING3	...	4624	2022-09-19 09:30:00	10	0.0.0.0	...	Administrator
WinClient1	...	4624	2022-08-30 09:19:41	2	10.0.0.1200	...	administrator
WinClient1	...	4624	2022-08-30 09:19:31	2	10.0.0.1100	...	Administrator
WinClient4	...	4624	2022-10-07 14:05:57	1	10.0.0.1100	...	administrator
WinClient4	...	4624	2022-10-08 10:10:21	7	10.0.0.1100	...	sophosuser
WinClient5	...	4625	2022-10-06 10:10:30	5	10.0.0.1100	...	Administrator

The information requested in the query will be collected, joined and presented to you as a result set of data.

You can choose to export the data returned, allowing you to interrogate the data using a tool of your choice. You can also use available pivoting options to perform further actions. If pivoting options are available for data, an ellipses menu is displayed.

Query Results

The screenshot shows the Sophos Central XDR interface with the 'Live Discover' tab selected. The main pane displays a table of events related to a user login attempt. One specific event (ID 4624) is highlighted with an orange box and ellipses (...), which has triggered a context menu. This menu is divided into three sections: 'Queries', 'Actions', and 'Enrichments'. The 'Actions' section contains two items: 'Scan this device' and 'Start a Live Response session'. The 'Enrichments' section lists several third-party tools for threat intelligence, each with its own link and icon. The top right corner of the main pane shows '9 / 9 Devices completed' and an 'Export' button.

Clicking the ellipsis will display the available actions for the data.

The queries section lists the available Data Lake and Live Discover queries that can use the data. These are known as pivot queries as they take the data returned and pivot it to run a new query.

The enrichments section provides links to third party websites that can be used to look up information about potential threats and tools.

The actions section includes available actions for further investigation or remediation. In the example you can select to either scan the device or start a Live Response session to that device.

Query Results

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. The left sidebar has a dark theme with white text and icons. The 'Live Discover' option is highlighted with a blue background. The main content area has a light gray background. At the top, it says 'Device Telemetry COMPLETE: 8 - data sent, 1 - no data sent, 0 - errors, 0 - no response'. Below this is a section titled 'Sophos Live Discover:' with a pie chart showing the status of 8 devices: 7 Complete, 1 Not responded yet. A table follows, showing details for 8 devices:

Device	System Impact	Execution time	Data XFR	Status	Type	Operating system	IP Address
DC	Large Impact (9%)	14240 ms	2.85 kb	Finished - OK	server	Windows Serv...	192.168.1.160
HEADEND3	Large Impact (9%)	1171 ms	3.87 kb	Finished - OK	server	Windows Serv...	192.168.1.166
Training-WD	Large Impact (9%)	8133 ms	3.61 kb	Finished - OK	computer	Windows 10 E...	192.168.1.219
WinClient1	Small Impact (2%)	1604 ms	1.64 kb	Finished - OK	computer	Windows 10 Pro	172.16.18.70
WinClient2	Large Impact (9%)	3551 ms	3.83 kb	Finished - OK	computer	Windows 10 Pro	172.16.18.80
WinClient3	Large Impact (9%)	1129 ms	2.93 kb	Finished - OK	computer	Windows 10 Pro	172.16.18.90
WinClient4	Large Impact (9%)	1026 ms	4.62 kb	Finished - OK			

At the bottom right of the table is a blue button labeled 'Run Query'.

In the device telemetry section, you can view which devices have responded to your query. If the query has completed successfully, and if there was no data in the available table(s) the ‘Complete, no data sent’ flag will be set. The table displays the following information:

- The status column which indicates whether the query finished and whether the device sent results. You can filter the device list according to device status
- The system Impact column which displays the query performance. A query that runs very quickly and generates little data is returned as having the smallest impact
- The data XFR column which displays the amount of data the query generated

Query Results

Complete, data sent

The query completed successfully, and data has been returned

Complete, no data sent

The query completed successfully, however, there was no data to return

Complete, errors

The query completed successfully, however, one or more devices have errors

Not responded yet

The query has been run, however, the device(s) have not responded

SOPHOS

The data in the telemetry section is split into four categories:

- Complete, data sent: The query completed successfully, and data has been returned
- Complete, no data sent: The query completed successfully, however, there was no data to return
- Complete, errors: The query completed successfully, however one or more devices returned errors
- Not responded yet: the query has been sent, however, the devices have not responded to the query

Audit Log

Live Discover queries are logged in the audit Log

The screenshot shows the Sophos Central interface with the 'Audit Log' report selected. The left sidebar includes links for Dashboard, Alerts, Threat Analysis Center, Logs & Reports (which is highlighted), People, Devices, Global Settings, Third-party Connectors, Protect Devices, Account Health Check, Endpoint Protection, Server Protection, and Mobile. The main area displays a table of audit log entries with columns for Date, Modified By, Item Type, Item Name, and Description. A green callout points to the second entry in the list, which is a 'Live Discover' query run on Nov 2, 2022, at 10:57:44 AM by 'ukcentral@sophosrai...'. The description for this entry is: 'Run query - Query name : Auth History for a Username; Query ID : e3333131-1eff-4cd4-a275-b13de97b50ca; Computers count : 0; Servers count : 3; Security VMs count : 0'. The status for this entry is 'Run query'.

DATE	MODIFIED BY	ITEM TYPE	ITEM NAME	DESCRIPTION
Nov 2, 2022 10:58:52 AM	ukcentral@sophosrai...	Live Discover	Run query - Query name : Auth History for a Username; Query ID : e3333131-1eff-4cd4-a275-b13de97b50ca; Computers count : 0; Servers count : 3; Security VMs count : 0	Run query
Nov 2, 2022 10:57:44 AM	ukcentral@sophosrai...	Live Discover	Run query - Query name : Auth History for a Username; Query ID : 9fa30b02-4d87-4bc9-9361-e5f79a0659d3; Computers count : 0; Servers count : 3; Security VMs count : 0	Run query
Nov 2, 2022 10:57:38 AM	ukcentral@sophosrai...	Live Discover	Run query - Query name : Auth History for a Username; Query ID : 8e12fe10-bee8-4bf1-8441-37a40b227b6f; Computers count : 0; Servers count : 3; Security VMs count : 0	Run query
Nov 2, 2022 10:57:07 AM	ukcentral@sophosrai...	Authentication	ukcentral@sophostraining.xyz	Successful
Nov 2, 2022 10:57:07 AM	ukcentral@sophosrai...	Authentication	Sophos/Google Authenticator	Attempts
Nov 2, 2022 10:50:52 AM	ukcentral@sophosrai...	Authentication	ukcentral@sophostraining.xyz	Successful
Nov 2, 2022 10:50:51 AM	ukcentral@sophosrai...	Authentication	ukcentral@sophostraining.xyz	Authentication
Nov 2, 2022 10:50:50 AM	ukcentral@sophosrai...	Authentication	ukcentral@sophostraining.xyz	Login attempt

For any Live Discover query run, a log of that query is included in the **Audit log**. You can access the audit log by navigating to **Logs & Reports > Audit Logs**.

In the Audit log, Live Discover queries are listed as **Live Discover** in the item type field. The date, time, user and query name are recorded in the report. Along with the IP address of the device that ran the query.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 3

You have selected devices for an Endpoint Live Discover query. The **Run Query** button is not available. Which of the following could be a solution for this issue?

Reduce the number of devices selected

Check the device operating system is supported

Confirm that you want to run the untested query

Click the Update selected device list button

SOPHOS



Question 2 of 3

What is the maximum number of days that an Endpoint Live Discover query can return data for?

SOPHOS

Question 3 of 3



Where would you click to view the available pivoting options in this query result?

The screenshot shows a user interface for a security event. At the top, there are several status indicators: 'Training-W10' (blue), '4624' (green), '2022-09-18 10:18:00' (grey), '11' (yellow), '10' (grey), '0.0.0.0' (grey), 'Administrator' (grey), and a dropdown menu with the path 'EventData->Auth...' (grey). Below these are four dark blue rectangular boxes labeled A, B, C, and D from left to right. Orange arrows point upwards from each box to specific UI elements above them. Box A points to a small grey arrow icon. Box B points to a larger orange double-headed vertical arrow icon. Box C points to a small orange double-headed horizontal arrow icon. Box D points to a small orange double-headed vertical arrow icon.

Chapter Review

Live Discover provides the ability to **run queries** across multiple devices on your network.

Any Endpoint Live Discover query will return live and historic data from the past **90 days of activity**.

Live Discover queries can be run to return data from **macOS**, **Windows** and **Linux** devices.

SOPHOS

Here are the three main things you learned in this chapter.

Live Discover provides the ability to run queries across multiple devices on your network.

Any Endpoint Live Discover query will return live and historic data from the past 90 days of activity.

Live Discover queries can be run to return data from macOS, Windows and Linux devices.



Sophos Central XDR Live Discover Query Scheduling and Editing

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4530: Sophos Central XDR Live Discover Query Scheduling and Editing

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central XDR Live Discover Query Scheduling and Editing

In this chapter you will learn how to select a Sophos canned query in Live Discover, edit it (if required) and run the query.

You will also learn how to select and remove the devices for an Endpoint Live Discover query, how to schedule a Data Lake query to run regularly.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Sophos XDR is
- ✓ How to run an Endpoint Live Discover query
- ✓ What the Sophos Data Lake is and how to run Data Lake queries

DURATION

10 minutes

SOPHOS

In this chapter you will learn how to select a Sophos canned query in Live Discover, edit it (if required), and run the query.

You will also learn how to select and remove devices for an Endpoint Live Discover query, and how to schedule a Data Lake query to run regularly.

Selecting a Canned Query

SOPHOS

Selecting a canned query.

Selecting a Canned Query

The screenshot shows the Sophos Threat Analysis Center interface with the 'Live Discover' tab selected. The main area displays a grid of canned query categories. A green callout box points to the 'Service [48]' category, which is highlighted with a red border. The categories and their counts are:

- All queries [316] (All available queries)
- Device [8] (Mobile device activity trips)
- Events [34] (Events in the system event log)
- Network [36] (Network connections and device transients)
- Process [16] (Service [48], patches, network and more)
- Registry [8] (Registry entries and changes)
- Attack [28] (Queries related to attack activity and monitoring)
- Compliance [44] (Compliance with security measures)
- File [56] (File access and file accessors)
- Other queries [22] (All other queries)

A green callout box contains the text: "Canned queries are categorized by Sophos".

Pre-defined or 'canned' queries are queries that have been written by Sophos and are available for use without the need for editing. They are split into categories making it easy to locate queries.

To select a canned query in Live Discover, navigate to **Threat Analysis Center > Live Discover**. The number in brackets indicates how many queries are available in the category.

Selecting a Canned Query

The screenshot shows the Sophos Central XDR Threat Analysis Center - Live Discover interface. On the left, there's a navigation sidebar with options like Threat Analysis Center, Threat Events, Live Discover (which is selected), Forensics, Investigations, and Preferences. The main area is titled 'Threat Analysis Center - Live Discover' and shows '18 Categories, 335 Queries'. A green callout box points to the list of queries, stating 'A list of available queries in the selected category is listed'. The query list includes categories such as BitLocker info, Certificates, Chocolatey packages, CPU Information, Data Lake upload details, Dell packages (Data Lake), and Devices with a restart pending, each with a brief description, source (Windows, Windows & macOS, or Data Lake), system impact, creator, and last modified date.

Name	Description	Source	System Impact	Created by	Last modified
BitLocker info	Lists the BitLocker status of the device.	Windows	Not Available		May 06, 2021
Certificates	Lists the installed Certificate Authorities from the issuer you specify.	Windows, macOS	Not Available		May 06, 2021
Chocolatey packages	Lists the Chocolatey packages installed on the device.	Windows	Not Available		Jul 21, 2021
CPU Information	Lists the CPU hardware details for the device.	Windows	Not Available		Jul 21, 2021
Data Lake upload details	Lists details of queries that uploaded data to the Data Lake. This only shows data from queries that have run since the content analysis process started, so some queries might not be included.	Windows, Linux	Not Available		May 04, 2021
Dell packages (Data Lake)	Lists Dellian packages on Linux devices	Data Lake	Not Available		Jun 04, 2021
Devices with a restart pending	Lists the reasons for any pending restart	Windows	Not Available		Jul 21, 2021

Once the query category has been selected, a list of available queries in that category is displayed.

Here we can see queries that will return BitLocker info, Certificates, and CPU information.

Searching for a Canned Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with options like Threat Response, Threat Discover, Live Discover (which is selected), Devices, Investigations, and Preferences. The main area is titled 'Threat Analysis Center - Live Discover' and shows 'Select One - 18 Categories, 335 Queries'. A search bar at the top has 'archive' typed into it. Below the search bar, there's a section titled 'Queries that get data from devices or from the Data Lake' with a note about endpoint and data lake queries. A green callout box with a triangle points to the 'Sources' column in the table below, which lists 'Windows, Linux, macOS'. The table also includes columns for Name, Description, Category, and Last modified.

Name	Description	Category	Sources	Last modified
Time schema	(Lists the column names and column data types)	Other queries	Windows, Linux, macOS	May 06, 2022

The supported operating systems

It is possible to search for queries. A query search will return queries that match the search term from all available categories, this is because the search will look for the search term in the last modified, created by, performance, name, and description fields. It will also check the query categories and return any that match the search term.

The results returned show the name, description and category of the query. It is worth noting the 'Sources' column, this will indicate which platforms the query is supported on. In this case only Windows, Linux and macOS operating systems are supported.

Viewing the Selected Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with navigation options: Threat Analysis Center, Threat Response, Threat Detections, Threat Intelligence, and Preferences. The 'Live Discover' option is currently selected and highlighted in blue. The main pane displays a table titled 'Table schema' with one row: 'Reported System Request'. This row includes columns for 'Description' (Windows, Linux, macOS), 'Expected Impact (Impact)', 'Last Run (Timestamp)', and 'Last Run (Timeago)'. A green callout box points to the 'Reported System Request' row with the text: 'View the name, supported OS, expected performance, data transfer and execution time of the query'. Below the table, there's a 'Device selector (14 Endpoints available)' section with a 'Selected devices' tab selected. At the bottom, there are filters for 'Status' (Online, Offline, Server), 'Operating system' (Windows 10, Windows 7, etc.), and a search bar.

Once a query is selected you can view the name, description, supported operating system, and the expected performance of the query.

Please note that you will only see the expected performance if the query has previously been run.

Expected Performance

Amount of data returned + Execution time = Expected performance

AGGRAGATE PERFORMANCE	EXECUTION TIME 0-5s	EXECUTION TIME 5-30s	EXECUTION TIME >30-120s	EXUCTION TIME >120s
0-1Kb	EXCELLENT	GOOD	FAIR	POOR
>1-5Kb	GOOD	GOOD	FAIR	POOR
>5-10Kb	FAIR	FAIR	FAIR	POOR
>10Kb	POOR	POOR	POOR	POOR

SOPHOS

The expected performance of a query is evaluated on two values;

- The amount of data returned
- The execution time on the endpoint

This table displays the expected performance based on execution time and the amount of data returned.

It is worth noting that there is a watchdog service running. This service will terminate a query if that query is using too much CPU or memory.

Run the Selected Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with navigation options: Threat Analysis Center, Threat Logins, Live Discover (which is selected), Threats, Investigations, and Preferences. The main area has a title 'Threat Analysis Center - Live Discover' and a sub-section 'Table schema'. It displays a table schema with columns: Device selector, Online status, Name, Type, IP address, and Last user. A filter bar at the top of the table lists 'Online Status' (selected), 'Name' (DC), 'Type' (Server), and 'IP address' (Windows DC). An orange box highlights the 'Run Query' button at the bottom right of the table area.

One or more devices must be selected before it is possible to run an Endpoint Live Discover query.

Export the Query Results

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, there's a sidebar with navigation links: 'DETECTION AND REMEDIATION', 'Dashboard', 'Threat Groups', 'Live Discover' (which is selected and highlighted in blue), 'Discoveries', 'Investigations', and 'Preferences'. The main content area has a title 'Device selector (14 Endpoints available)'. Below it, a table titled 'Table schema query results' displays 11 rows of data. The columns are: 'appName', 'name', 'column', 'type', and 'extension'. The data includes entries like 'appcompt_shms' for 'appcache' with type 'TEXT' and extension 'core'. At the top right of the main content area, there's a message 'See query execution: Thu Aug 2, 0100 (British Summer Time) [CSV] Consolidated — 77.8 KB' with a 'Show all download' link. On the far right, there's a 'Export' button with a red box drawn around it.

appName	name	column	type	extension
DC	appcompt_shms	executable	TEXT	core
DC	appcompt_shms	path	TEXT	core
DC	appcompt_shms	description	TEXT	core
DC	appcompt_shms	install_time	INTEGER	core
DC	appcompt_shms	type	TEXT	core
DC	appcompt_shms	sub_id	TEXT	core
DC	appcache	address	TEXT	core
DC	appcache	mac	TEXT	core
DC	appcache	interface	TEXT	core
DC	appcache	permanent	TEXT	core
DC	slm_packages	name	TEXT	core

The query results are displayed and can be exported as a .csv file.

Viewing the Selected Query

The screenshot shows the Sophos Threat Analysis Center interface with the 'Live Discover' tab selected. A green callout box points to the 'Designer Mode' toggle button, which is highlighted with a red border. Another green callout box points to the SQL query results area, also highlighted with a red border. The SQL code is as follows:

```
SELECT
    registry_registry.name AS 'table', --> main: display[0][0]
    registry_registry.type AS 'type' AS 'label',
    registry_registry.value AS 'value',
    registry_registry.modified AS 'modified'
FROM
    registry_registry
WHERE
    registry_registry.name = 'registry'
    AND registry_registry.type = 'string'
    AND registry_registry.value = '0.0.0.0'
    AND registry_registry.modified <= 1623446400000
ORDER BY
    registry_registry.modified DESC;
```

We do not expect you to know SQL in order to use Live Discover, however, the SQL used for any selected query can be viewed by enabling 'Designer Mode'. The SQL will display which data tables are being returned. Additionally, in designer mode you can edit the query should this be required.

Editing A Query

SOPHOS

Editing a query.

How to Edit an Existing Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, a sidebar lists navigation options: Overview, Threat Analysis Center Dashboard, Live Discover (which is selected and highlighted in blue), Threat Groups, References, Investigations, and Preferences. The main content area is titled 'Threat Analysis Center - Live Discover' and shows the 'Live Discover' tab selected. A 'Designer Mode' toggle switch is visible, with a callout bubble stating 'We need more information from this query...'. Below it, a query result table is displayed with the title 'Services installed on the device'. The table includes columns for 'Source' (Windows), 'Expected system impact' (Scripted input (Access)), 'Last Seen (Seconds)', and 'Count (Daily Ingested (All))'. A green callout bubble states 'No problem! We can edit this query.' A large magnifying glass icon is overlaid on the right side of the interface.

The canned queries that are available may return some data required, however, further data from devices could be needed.

This is where the option to edit a query becomes useful. To edit a query, you need to first enable 'Designer Mode'. Once designer mode has been enabled, you will see the **Edit** option for a query.

Editing a Query – What is the Query Asking?

All queries: Services installed on the device

Lists all services installed on the device
Created by Sophos

Sources: Windows

Expected performance: Poor to Excellent

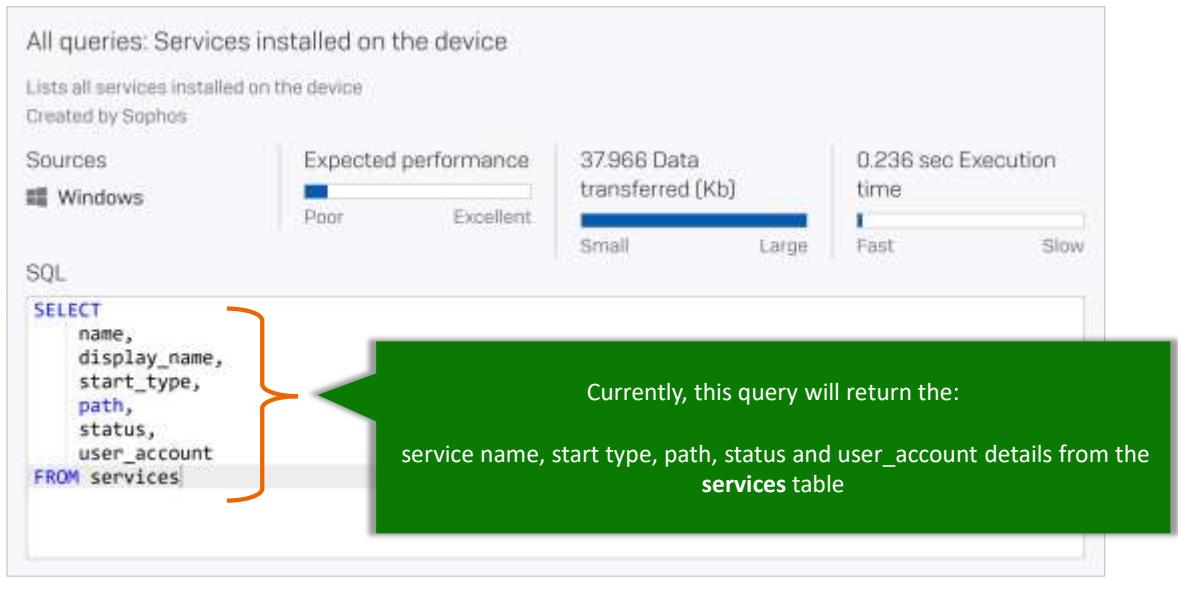
Data transferred [Kb]: 37.968 Data transferred [Kb] (Large)

Execution time: 0.236 sec Execution time (Fast)

SQL:

```
SELECT
    name,
    display_name,
    start_type,
    path,
    status,
    user_account
FROM services;
```

Currently, this query will return the:
service name, start type, path, status and user_account details from the services table



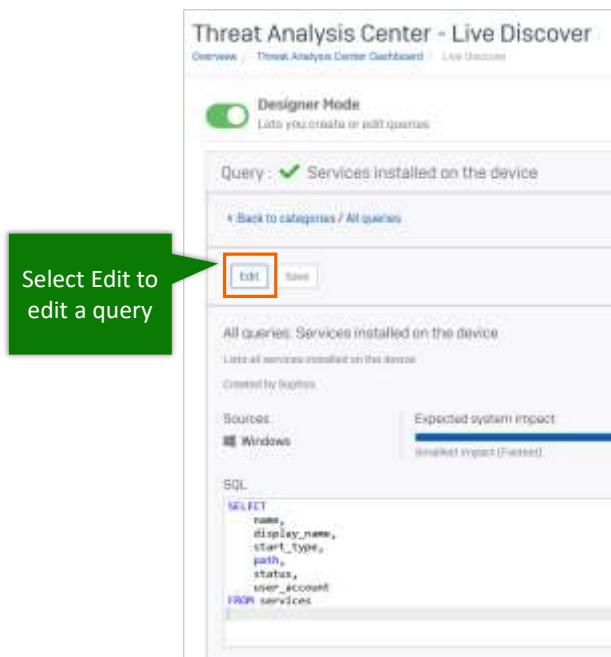
Let's look at an example.

The selected query will return the following data found in the services table for all devices it is run on;
Service Name, Start Type, Path, Status, and User_Account.

Editing a Query

epName	table	column	type	extension
SRV	services	name	TEXT	core
SRV	services	service_type	TEXT	core
SRV	services	display_name	TEXT	core
SRV	services	status	TEXT	core
SRV	services	pid	INTEGER	core
SRV	services	start_type	TEXT	core
SRV	services	win32_exit_code	INTEGER	core
SRV	services	service_exit_code	INTEGER	core
SRV	services	path	TEXT	core
SRV	services	module_path	TEXT	core
SRV	services	description	TEXT	core
SRV	services	user_account	TEXT	core

The services table has more data columns available



Select Edit to edit a query

Threat Analysis Center - Live Discover

Designer Mode
Allows you to create or edit queries

Query : Services installed on the device

Back to categories / All queries

All queries: Services installed on the device

Last run: All services installed on this device

Created by Sophos

Buckets: Windows

Expected system impact:
(Minimal Impact / Fainter)

SQL:

```
SELECT
    name,
    display_name,
    start_type,
    path,
    status,
    user_account
FROM services
```

Looking at the schema table (having run the schema table query and exported it) there is more data in the services table that could be returned.

For this example, the existing query will be edited to include the description of the service.

To add this additional element, select **Edit** in the 'Query Selection' section.

Editing a Query

The screenshot shows the 'Edit' screen for a query named 'Services installed on the device with description'. The 'Category' is set to 'Device'. Below the form, there is a green button labeled 'Re-name the query'.

*Query Name: Services installed on the device with description

*Category: Device

Buttons: Edit, Save

SQL Editor:

```
*SQL
SELECT
    name,
    display_name,
    start_type,
    path,
    status,
    user_account,
    description
FROM services
```

A green button labeled 'Edit the SQL command.' is located below the SQL code.

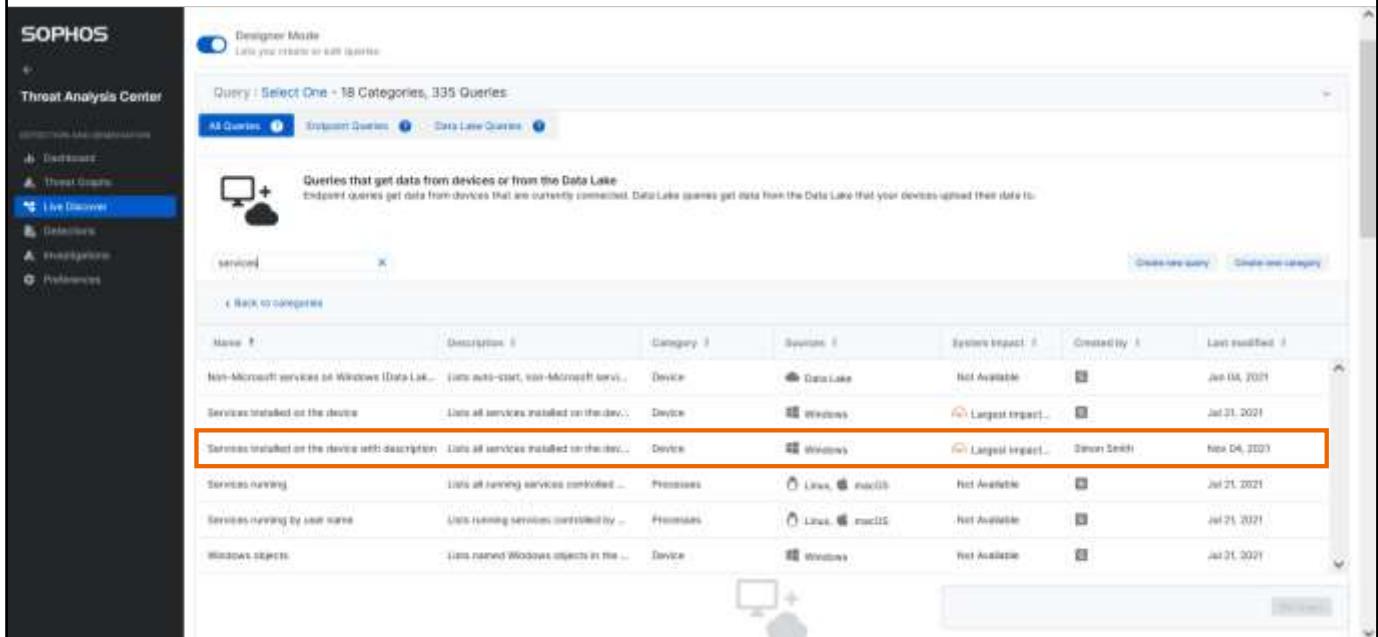
SOPHOS

The query is re-named so that it can be saved as a new query.

In the SQL field, the column name 'description' is added to the column data list. This is a list of the data columns that will be returned from the services table.

You will need to re-name the query and then click **Save** to save the changes.

Editing a Query



The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists categories: Threats, Devices, Threat Groups, Live Discover (which is selected), Detections, Investigations, and Policies. The main area is titled 'Query : Select One - 18 Categories, 335 Queries'. Below this are three tabs: All Queries, Unknown Queries, and Data Lake Queries. A sub-section titled 'Queries that get data from devices or from the Data Lake' is shown, with a note: 'Endpoint queries get data from devices that are currently connected. Data Lake queries get data from the Data Lake that your devices upload their data to.' A search bar at the top of this section contains the text 'services'. A table lists several queries, with one specific entry highlighted by a red border:

Name	Description	Category	Sources	Event Impact	Created by	Last modified
Non-Microsoft services on Windows (Data Lake)	Lists auto-start, non-Microsoft servi...	Device	DataLake	Not Available		Jan 14, 2021
Services installed on the device	Lists all services installed on the dev...	Device	Windows	Largest Impact...		Jul 31, 2021
Services installed on the device with description	Lists all services installed on the dev...	Device	Windows	Largest Impact...	Simon Smith	Nov 04, 2023
Services running	Lists all running services controlled ...	Processes	Linux, macOS	Not Available		Jul 21, 2021
Services running by user name	Lists running services controlled by ...	Processes	Linux, macOS	Not Available		Jul 21, 2021
Windows objects	Lists named Windows objects in the ...	Device	Windows	Not Available		Jul 21, 2021

In this example, we did not amend the category of the query. Therefore, the new query we have created can be found in the devices category and is listed alphabetically in the list of queries.

In the 'Created by' column you can view any edited or newly created queries as these will be listed as your Sophos Central account name.

Editing a Query

Designer Mode
Let you create or edit queries

Query : Services installed on the device with description

Back to categories / All queries

Edit Save Delete

All queries: Services installed on the device with description

Use of services installed on the device

Last used: 1 hour ago

Source: Windows Executed system impact: Standard Impact (Normal) Last updated: 2 hours ago 13.8 MB Data transferred: 0 KB 0.000 sec Execution time: 0 sec

File

Help

Device selector (14 endpoints available) Endpoint selected: v

Canned queries created by Sophos cannot be deleted

Last active query results 1 Device(s) examined

Selecting the edited query gives you the option to **Delete** or **Edit** the query.

Please note that canned queries created by Sophos cannot be deleted.

Editing a Query

The edited query has been run and returns the additional data added to the SQL command

Services installed on the device with description query results								
service_id	name	display_name	start_type	path	status	user_account	description	last_update
BC	ADWS	Active Directory Web...	AUTO_START	C:\Windows\AD...	RUNNING	LocalSystem	This service provides a Web Service interface to instances ...	2023-09-01T12:00:00Z
BC	AlRasua	AltSync Router Service	DEMAND_START	C:\Windows\Alras...	STOPPED	NT AUTHORITY\SYSTEM	Relays AltSync messages for the local AltSync clients. If this...	2023-09-01T12:00:00Z
BC	AGD	Application Layer Ge...	DEMAND_START	C:\Windows\Sys...	STOPPED	NET AUTHORITY\SYSTEM	Provides support for 3rd party protocol plug-ins for Intern...	2023-09-01T12:00:00Z
BC	AppHost	Application Identity	DEMAND_START	C:\Windows\System...	STOPPED	NET AUTHORITY\SYSTEM	Determines and verifies the identity of an application. Disc...	2023-09-01T12:00:00Z
BC	AppInfo	Application Informati...	DEMAND_START	C:\Windows\System...	STOPPED	LocalSystem	Facilitates the running of interactive applications with auth...	2023-09-01T12:00:00Z
BC	AppMgmt	Application Manage...	DEMAND_START	C:\Windows\System...	STOPPED	LocalSystem	Processes installation, removal, and enumeration requests f...	2023-09-01T12:00:00Z
BC	AppReadiness	App Readiness	DEMAND_START	C:\Windows\System...	STOPPED	LocalSystem	Notifies apps ready for use the first time a user logs in to thi...	2023-09-01T12:00:00Z
BC	AppVCClient	Microsoft App-V Client	DISABLED	C:\Windows\System...	STOPPED	LocalSystem	Manages App-V users and virtual applications.	2023-09-01T12:00:00Z
BC	AppDeploy	AppDeploy Deployment S...	DEMAND_START	C:\Windows\System...	STOPPED	LocalSystem	Provides infrastructure support for deploying store applic...	2023-09-01T12:00:00Z
BC	AudioEndpointBuild...	Windows Audio Engine	DEMAND_START	C:\Windows\System...	STOPPED	LocalSystem	Manages audio devices for the Windows Audio Service. It t...	2023-09-01T12:00:00Z
BC	Authz	Windows Authz	DEMAND_START	C:\Windows\System...	STOPPED	NT AUTHORITY\SYSTEM	Manages audits for Windows-based programs. If this service...	2023-09-01T12:00:00Z

The Sophos canned query provided the name of the services, however, for this example, more information was required regarding what the services do. The canned query was edited, and the ‘description’ data column was added to the query.

When the edited query is run, you will see in the results that the description column is returned. You can now view a description of each service that is installed on your protected devices.

Device Selection

SOPHOS

Device selection.

Device Selection

Device selector (12 Endpoints available)

No endpoints selected

Available devices Selected devices:

Filters

- Online Status
- Name
- Type
- Operating system
- Last user
- Group
- IP address
- Health status

Clear all Apply

Update selected devices list			
	Online status	Name	Type
<input type="checkbox"/>	Online	Client1	Computer
<input type="checkbox"/>	Online	Client2	Computer
<input type="checkbox"/>	Online	Client3	Computer
<input type="checkbox"/>	Online	Client4	Computer
<input type="checkbox"/>	Online	Client5	Computer
<input type="checkbox"/>	Online	Server1	Server

Displaying 1 - 8

SOPHOS

To run an Endpoint Live Discover query you need to select the device or devices you wish to run the query on.

Using filters you can refine your device list by online status, type, group, etc.

Device Selection

The screenshot displays two identical-looking tables for selecting devices. Each table has columns for Online status, Name, Type, and OS. A 'Hide filters' button is at the top left, and a 'Search' bar is at the top right.

Select single devices: In this interface, the checkbox next to Client1 is checked, while the one next to Client2 is unchecked. A green arrow points from the text 'Select single devices' to the checked checkbox of Client1.

Online status	Name	Type	OS
<input checked="" type="checkbox"/> Online	Client1	Computer	Win
<input type="checkbox"/> Online	Client2	Computer	Win

Select ALL devices: In this interface, both checkboxes next to Client1 and Client2 are checked. A green arrow points from the text 'Select ALL devices' to the checked checkboxes of Client1 and Client2.

Online status	Name	Type	OS
<input checked="" type="checkbox"/> Online	Client1	Computer	Win
<input checked="" type="checkbox"/> Online	Client2	Computer	Win

SOPHOS

Select a device using the check box next to the device name. To select all devices, select the check box next to the 'Name' column.

Device Selection

The screenshot shows the Sophos Central XDR interface under the 'Threat Analysis Center'. On the left, a sidebar lists navigation options: Dashboard, Threat Details, Live Discover (which is selected), Detectors, Investigations, and Preferences. The main area is titled 'Device Selector (14 Endpoints available)'. It features a 'Filters' section with dropdown menus for Online status, Name, Type, Operating system, IP address, and Health status. Below this is a table displaying 14 endpoint entries. The columns include: Online status, Name, Type, OS, Last user, Status, and IP address. The table shows five entries with the 'Online' status checked. An 'Update selected devices list' button is highlighted with a mouse cursor. At the bottom right of the table, there is a 'Displaying 1 - 5' message.

Online status	Name	Type	OS	Last user	Status	IP address
<input checked="" type="checkbox"/> Online	DC	Server	Windows Server 2012 · SOPHOS\administrator	Reading Office	192.168.1.9	
<input checked="" type="checkbox"/> Online	SRV1	Server	Windows Server 2012		192.168.1.10	
<input checked="" type="checkbox"/> Online	Training server	Server	Ubuntu 20.04.4 LTS	Reading Office	192.168.1.11	
<input checked="" type="checkbox"/> Online	WinClient1	Computer	Windows 10 Pro · WINGLET\winglet	Office Workers	172.16.16.1	
<input type="checkbox"/> Online	WinClient2	Computer	Windows 10 Pro · TRADINGTEAM\tradingteam		172.16.16.19	
<input type="checkbox"/> Online	WinClient3	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient4	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient5	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient6	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient7	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient8	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient9	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient10	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient11	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient12	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient13	Computer	Windows 10 Pro			
<input type="checkbox"/> Online	WinClient14	Computer	Windows 10 Pro			

Once you have selected the device or devices click **Update selected devices list** to save the selection.

Device Selection

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, there's a sidebar with navigation links: Threat Analysis Center, Threat Detection, Live Discover (which is selected), Dashboards, Investigations, and Preferences. The main area is titled "Device Selector (14 Endpoints available)". It has two tabs: "Available devices" (selected) and "Selected devices". A search bar at the top right says "3 Endpoints selected". Below the tabs is a "Filters" section with dropdown menus for Online status, Name, Type, Operating system, MAC address, Group, IP address, and Health status. There are "Reset to defaults" and "Apply" buttons. The main table lists 14 endpoints:

Online status	Name	Type	OS	Last user	Group	IP address
Online	DC	Server	Windows Server 2022	SOPHOS\Administrator	Reading Office	192.168.1.3
Online	Srv3	Server	Windows Server 2022			192.168.1.8
Online	Training-Workstation	Server	Ubuntu 20.04.4 LTS		Reading Office	192.168.1.9
Online	WinClient1	Computer	Windows 10 Pro	WNC1\CLIENT1\Sophos	Office Workers	192.168.10.10
Online	WinClient2	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.11
Online	WinClient3	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.12
Online	WinClient4	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.13
Online	WinClient5	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.14
Online	WinClient6	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.15
Online	WinClient7	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.16
Online	WinClient8	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.17
Online	WinClient9	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.18
Online	WinClient10	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.19
Online	WinClient11	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.20
Online	WinClient12	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.21
Online	WinClient13	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.22
Online	WinClient14	Computer	Windows 10 Pro	THAMNIDES\MC\clientuser		192.16.16.23

SOPHOS

You will then see that the number of selected devices is amended.

Remove a Device

The image displays two screenshots of the Sophos Central XDR 'Device selector' interface. Both screenshots show a table of devices with columns: Name, Type, OS, Last user, and Group.

Top Screenshot: The 'Selected devices' tab is active. A blue box highlights the 'Update selected devices list' button. The status bar at the top right says '1 Endpoint selected'. The device table shows one entry: 'Server1' (Server, Windows Server 2012 Datacenter, globitraining). The status bar at the bottom says 'Displaying 1-1 of 1'.

Name	Type	OS	Last user	Group
Server1	Server	Windows Server 2012 Datacenter	globitraining	

Bottom Screenshot: The 'Available devices' tab is active. A red box highlights the 'No endpoints selected' message at the top right. The device table shows the same entry as the top screenshot. The status bar at the bottom says 'Displaying 1-1 of 1'.

Name	Type	OS	Last user	Group
Server1	Server	Windows Server 2012 Datacenter	globitraining	

SOPHOS

To remove a device, un-tick the selection box next to the device and click **Update selected devices list**.

Scheduling Queries

SOPHOS

Scheduling queries.



Additional information in
the notes

Scheduled Queries

Create scheduled queries to run regularly

Only Data Lake queries can be scheduled

SOPHOS

Administrators can use scheduled queries to run regular reports based on the information available in the Data Lake.

It is important to understand that it is only possible to schedule Data Lake queries as these can be run on devices that are both online and offline.

[Additional Information]

A video showing the scheduled reports is available in Sophos Tech Videos here:

<https://techvids.sophos.com/watch/P5WkjrUHsvAxMujH6zG5hL>

How to Schedule a Query

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a sidebar menu has 'Live Discover' selected. The main area is titled 'Threat Analysis Center - Live Discover' and shows a query named 'Pending Windows updates (Data Lake)'. A green callout bubble points to the 'Schedule Query...' button at the bottom right of the screen.

Select the option to **Schedule Query**

It is simple to setup a scheduled query. Navigate to **Threat Analysis Center > Live Discover** and select a Data Lake query.

Before you schedule a query, we recommend that you run the query first in order to confirm that the data returned is what you want to see regularly and that the variables required are applied.

Once you have selected the query you will see the option to either **Schedule Query** or **Run Query**.

Click **Schedule Query**.

How to Schedule a Query

The screenshot shows the 'Schedule Query' dialog box. At the top, it says 'Schedule Query'. Below that, there are fields for 'NAME' (containing 'ATTCK - Generic TTP Detection MITRE ATTCK Caldera 2021-05-11') and 'DESCRIPTION' (containing 'Scheduled Query'). To the right, a progress bar indicates 'Remaining scheduled queries & report templates 94/100'. Under 'QUERY FREQUENCY', the 'Monthly' option is selected. It also shows 'Day of month' set to '1' and 'End date' set to '11/11/2021', with a checkbox for 'Until I cancel' which is unchecked. At the bottom right, there are 'Cancel' and 'Create Scheduled Query' buttons, with the latter being blue.

SOPHOS

The query can now be scheduled. Change the name and add a description if required.

Determine the frequency of the scheduled query. In this example we have selected for the query to run daily Monday to Friday and will run until the user cancels the schedule.

Please note that the query will be run at midnight in the time zone the administrator created it in. This remains true even if the administrator later logs in from a different time zone.

Click **Create Scheduled Query**.

Viewing Scheduled Queries

The screenshot shows the Sophos Threat Analysis Center preferences page. On the left, a sidebar lists 'Threat Analysis Center' sections: Dashboard, Threat Graphs, Live Discover, Detections, Investigations, and Preferences (which is selected). A green callout box points to the 'Preferences' button with the text 'View your scheduled queries'. The main area is titled 'Threat Analysis Center - Preferences' and shows 'Scheduled queries'. A blue box highlights the 'Scheduled queries' tab. A green callout box points to the 'Activity Scheduled' bar at the top right of the table with the text 'View how much space you have left for scheduled queries'. The table lists scheduled queries with columns: Query name, Frequency, Admin name, Devices queried, Schedule status, and Last run. The first query is 'Pending Windows updates Data Lake 2022-11-02'.

Query name	Frequency	Admin name	Devices queried	Schedule status	Last run
Pending Windows updates Data Lake 2022-11-02	Weekly	UK Training	All devices	Enabled	Nov 11, 2021 10:28 AM
Pass-the-hash attacks Data Lake 2021-11-11	--	Simon Smith	All devices	Enabled	Nov 11, 2021 10:28 AM
Top threat indicators on Windows devices 2021-11-11	--	Simon Smith	All devices queried	Disabled	Jun 30, 2021 11:18 AM
Recent Windows updates	Weekly	UK Training	All devices queried	Enabled	Jun 25, 2021 3:59 PM

Scheduled queries are viewed by navigating to **Threat Analysis Center > Preferences > Scheduled Queries**.

Newly created scheduled queries will appear at the top of the query list. There is a limit to the number of queries that can be scheduled, the 'Activity Scheduled' bar indicates how much space you have left.

Viewing Scheduled Queries

The screenshot shows the Sophos Threat Analysis Center - Preferences interface. On the left, there's a sidebar with navigation links like Dashboard, Threat Graphs, Live Discover, Detections, Investigations, and Preferences (which is highlighted). The main area is titled "Threat Analysis Center - Preferences" and has tabs for Environments, Scheduled queries (which is selected and highlighted in blue), and Email notifications. Below these tabs is a table titled "Report Templates" with a search bar. The table has columns for Query name, Frequency, Admin name, Devices queried, Schedule status, and Last edited. There are 5 scheduled queries listed:

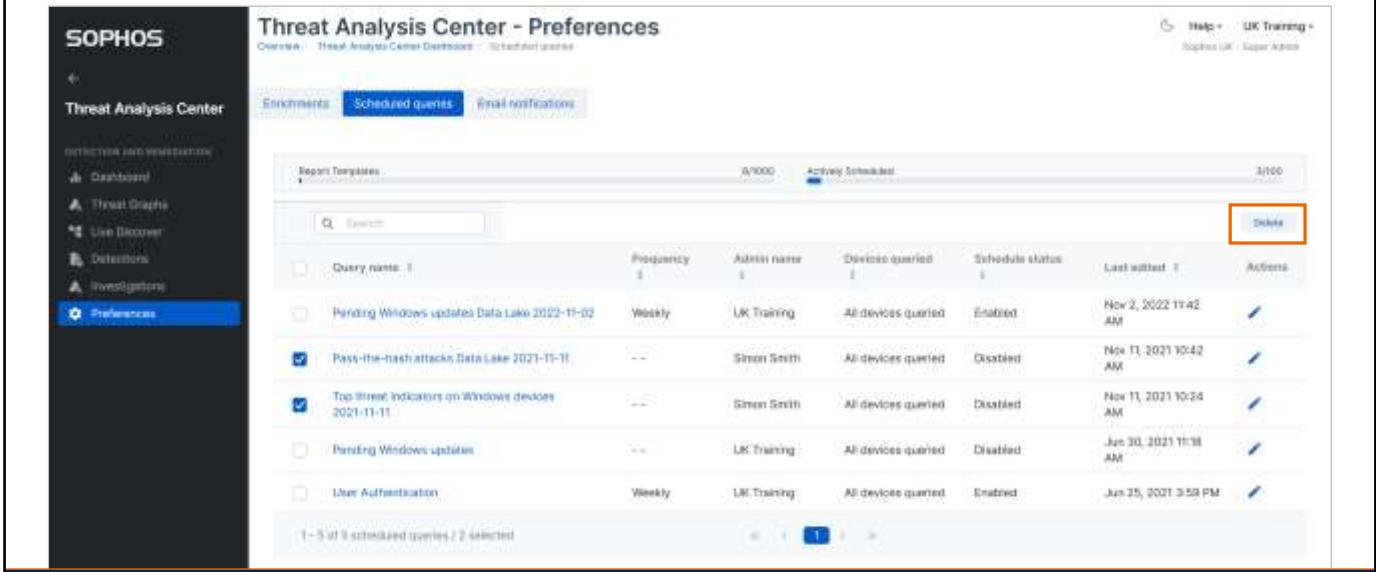
Query name	Frequency	Admin name	Devices queried	Schedule status	Last edited	Actions
Pending Windows updates Data Lake 2022-11-02	Weekly	UK Training	All devices queried	Enabled	Nov 2, 2022 11:42 AM	
Pass-the-hash attacks Data Lake 2021-11-11	--	Simon Smith	All devices queried	Disabled	Nov 11, 2021 10:42 AM	
Top threat indicators on Windows devices 2021-11-11	--	Simon Smith	All devices queried	Disabled	Nov 11, 2021 10:28 AM	
Pending Windows updates	--	UK Training	All devices queried	Disabled	Jun 30, 2021 11:18 AM	
User Authentication	Weekly	UK Training	All devices queried	Enabled	Jun 25, 2021 3:59 PM	

At the bottom of the table, it says "1 - 5 of 5 scheduled queries / 0 selected".

The scheduled query list displays the frequency of the query along with the administrator who created it and the schedule status. The actions option allows you to:

- View the query that is scheduled including the variables that are included
- Disable the schedule or edit the frequency of the scheduled query
- View the results of the query

How to Delete a Scheduled Query



The screenshot shows the Sophos Threat Analysis Center - Preferences interface. The left sidebar has 'Threat Analysis Center' selected. The main area shows a table of scheduled queries. One row is selected, and the 'Delete' button in the Actions column is highlighted with a red box.

Query name	Frequency	Admin name	Devices queried	Schedule status	Last edited	Actions
Pending Windows updates Data Lake 2022-11-02	Weekly	UK Training	All devices queried	Enabled	Nov 2, 2022 11:42 AM	
Pass-the-hash attacks Data Lake 2021-11-11	--	Simon Smith	All devices queried	Disabled	Nov 11, 2021 10:42 AM	
Top threat indicators on Windows devices 2021-11-11	--	Simon Smith	All devices queried	Disabled	Nov 11, 2021 10:28 AM	
Pending Windows updates	--	UK Training	All devices queried	Disabled	Jun 30, 2021 11:18 AM	
User Authentication	Weekly	UK Training	All devices queried	Enabled	Jun 25, 2021 3:59 PM	

Deleting a scheduled query will delete the schedule and all associated results

To delete a scheduled query, simply select the query you want to delete from the list and click **Delete**.

You will need to confirm you want to delete the query. Please note that when you delete a query it will delete the schedule and all associated results.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!

Question 1 of 2

True or False: To search for a query you must first select the required category.

True

False



Question 2 of 2

Which of these queries can be scheduled?

All Queries

Endpoint Queries

Data Lake Queries

SOPHOS

Chapter Review

Canned queries are queries that have been written by Sophos. To edit a canned query, you must enable 'Designer Mode'.

A query search will return queries that match the search term from all available categories.

Only Data Lake queries can be scheduled

SOPHOS

Here are the main things you learned in this chapter.

Canned queries are queries that have been written by Sophos. To edit a canned query, you must enable 'Designer Mode'.

A query search will return queries that match the search term from all available categories.

Only Data Lake queries can be scheduled.



Getting Started with Sophos Central XDR Threat Graphs

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4550: Getting Started with Sophos Central XDR Threat Graphs

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Getting Started with Sophos Central XDR Threat Graphs

In this chapter you will learn what a threat graph is and the use cases for threat graphs, including possible follow-up actions.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access and navigate Sophos Central
- ✓ How threats are detected and reported in Sophos Central

DURATION **6 minutes**

SOPHOS

In this chapter you will learn what a threat graph is, and the use cases for threat graphs, including possible follow-up actions.

Threat Graph Use Cases

Detection

- “Could the threat have been intercepted earlier?”
- “What can be discovered about the threat or particular incident?”
- “What makes this incident malicious?”
- “Where else has this threat been observed?”
- “How is this incident similar to other threats?”

Response

- “Which components of this threat are malicious?”
- “How can the threat be contained whilst investigation is conducted?”
- “How can a threat be mitigated once it has been contained?”
- “How can a response to similar threats be automated?”

SOPHOS

Threat graphs list any detections in the past 90 days across your network. The information provided does not necessarily require an action, however, the threat graph can aid investigation into a threat.

You may ask yourself if it could have been possible to intercept the threat earlier, or you may want further information on the detection. What makes the detected threat malicious? What other elements were involved? Or simply, how can you identify areas for improved security on your network?

When responding to threats, you want to ensure that the threat is contained and to ensure the rest of your network is protected.

Opening a Threat Graph

The screenshot shows the Sophos Threat Analysis Center Dashboard. On the left, there's a sidebar with navigation links: Dashboard (highlighted with a red box), Threat Graphs (also highlighted with a red box), Live Discover, Detectors, Investigations, and Preferences. The main area has a title 'Threat Analysis Center - Dashboard' and a sub-section 'Recent Investigations'. It lists six threat investigations with columns for Priority (High), Investigation ID, Status (Not Started), Created at (e.g., 2022-11-02-001), Assigned to (Sophos), Created by (Sophos), Age (e.g., 8 days), Detections (e.g., 13), Last modified (Nov 2, 2022 8:16:51 PM), Last detection (Nov 2, 2022 8:16:51 PM), and Summary (Initial Detection: WIN-MITRE-Beh...). Below this is a 'Recent detections' section with a table showing counts for Threat (13), Impact (14), and Device (8) across various categories like MITRE ATT&CK, Devices, and Connectors. To the right is a 'Most recent threat graphs' section with two tabs: 'Sophos generated' (selected) and 'Admin generated'. It shows a table with columns for Time created, Priority, Name, User, and Device, listing entries like 'Nov 2, 2022 6:35 PM', 'Medium', 'MLPE-A', 'n/a', and 'PC'. A 'See all threat graphs' button is also present.

All threats will be listed in the threat graphs list. On the Threat Analysis Center **Dashboard**, you can view your most recent threat graphs.

View all threat graphs by selecting **Threat Graphs** in the left-hand menu or by selecting **See all threat graphs** from the 'Most recent threat graphs' widget.

The threat graphs list can be filtered by priority, device, or status.

Opening a Threat Graph

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation links: Dashboard, Threat Graphs (which is selected and highlighted in blue), Live Discover, Detectors, Investigations, and Preferences. The main area is titled "Threat Analysis Center - Threat Graphs". It displays a table of threat entries with columns: Status, Time-created, Priority, Name, User, Device, and Device type. One specific entry, "EICAR-Av-Test" from Oct 31, 2022, at 7:18 PM, is highlighted with a red box around its name.

Status	Time-created	Priority	Name	User	Device	Device type
New	Oct 31, 2022 6:35 PM	Medium	MICRO-A	n/a	READING-W10	Server
New	Oct 31, 2022 6:36 AM	Medium	MICRO-A	n/a	DC	Server
New	Oct 31, 2022 6:36 AM	Low	EICAR-Av-Test	n/a	DC	Server
New	Oct 31, 2022 6:37 AM	Low	MICRO-A	n/a	DC	Server
New	Oct 31, 2022 7:18 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 7:37 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 7:37 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:08 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:48 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:49 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer
New	Oct 31, 2022 8:57 PM	Low	EICAR-Av-Test	TRAINING-W10\Training	Training-W10	Computer

Select a threat graph from the list by selecting the threat name to view the full threat graph.

Detailed View

The screenshot shows the Sophos Threat Analysis Center interface for the 'EICAR-AV-Test' threat graph. At the top, there's a navigation bar with links for Help, UK Training, Service Desk, and Support. Below the navigation is a horizontal timeline showing the flow from 'Training-W10' to 'Root Cause' (Google Chrome), then to 'Beacon' (eicar-test.com), and finally 'Detected' (Oct 31, 2022 12:17 PM) and 'Cleared'. On the left, a sidebar lists Threat Analysis Center options: Dashboard, Threat Graphs, Live Discover, Detectors, Investigations, and Preferences. The main content area has two sections: 'Summary' and 'Suggested next steps'. The 'Summary' section includes fields for Detection name (EICAR-AV-Test), Root cause (192.168.1.216), Possible data involved (no business files), and Where (On Training-W10 that belongs to TRAINING-W10). A red box highlights the 'Detection name' field, and a green arrow points down to the 'Where' field. The 'Suggested next steps' section contains three items: 'Set a status for the threat graph' (Priority Low, Status: New), 'Investigate 2 processes that we've marked with an "uncertain" reputation. See graph below for details.', and 'Isolate this device while you investigate' (with a link to 'Isolate'). Below the summary is a 'Details' section for 'EICAR-AV-Test' with tabs for Summary and Main Information. It shows the threat type as Virus and worm, last updated on Oct 31, 2022, 10:09:58 (GMT), and provides a download link for the Virus Removal Tool. The 'Affected Operating Systems' section shows 'Windows'.

In the detailed view of a threat graph, you will see a simplified flow of the incident. This includes the endpoint name and IP address, the root cause and beacon event (if identified) and when the threat was detected and removed.

The date and time of the incident is also displayed. You can click on the detection name to view the Sophos Threat Analysis page which provides further details of the threat.

Suggested Next Steps

The screenshot shows the Sophos Threat Analysis Center interface. At the top, there's a navigation bar with links for Help, UK Training, Service Uptime, and Support. Below the navigation is a horizontal timeline with icons for Training-W10 (IP 192.168.1.216), Root Cause (Google Chrome), Beacon (eicar.com), and Detected (Oct 31, 2022 12:17 PM). A large orange box highlights the "Suggested next steps" section on the right.

Suggested next steps:

- Set a status for the threat graph (Priority Low, Status New)
- Investigate 2 processes that we've marked with an "uncertain" reputation. See graph below for details
- Isolate this device while you investigate
- Scan the device
- Run a Live Discover query

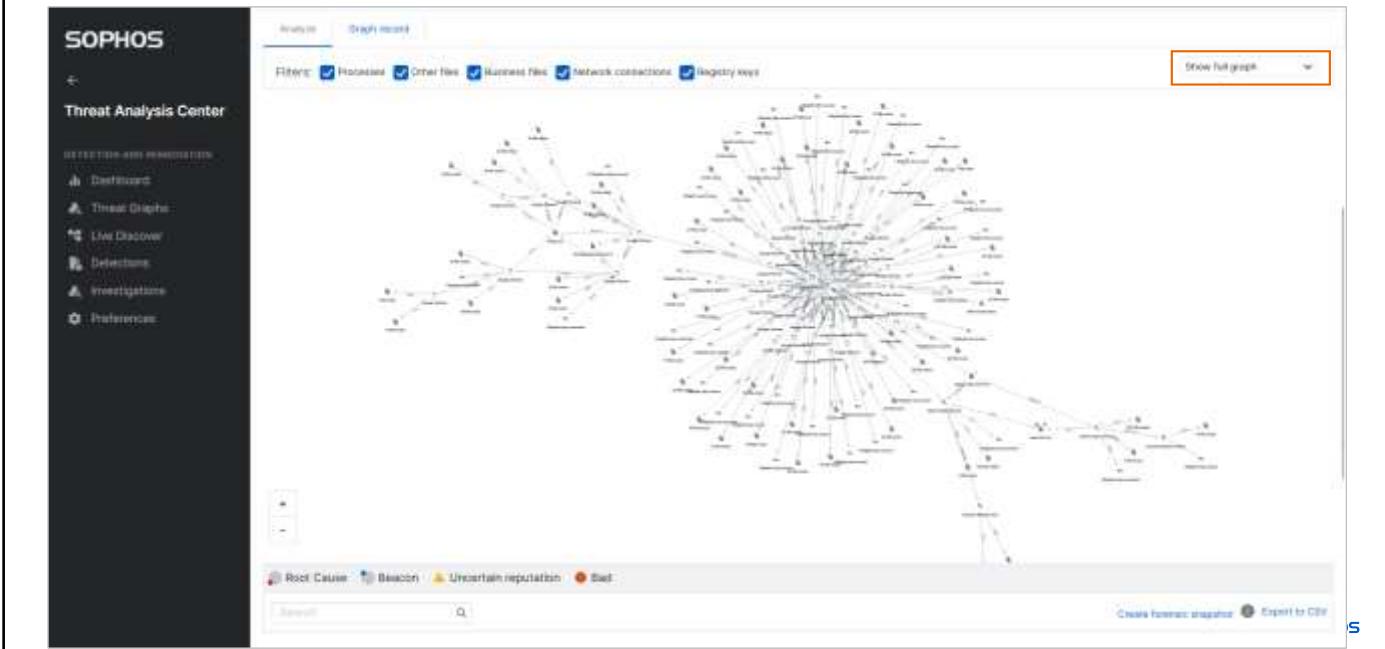
The main area contains a threat graph with nodes and edges, and a summary table with the following data:

Detected name:	EICAR-AV-Test
Root cause:	106.0.6249.110.106.0.6249.303.Chrome_update.exe
Possible data involved:	no business files
Where:	On Training-W10 that belongs to TRAINING-W10\Training
When:	Detected on Oct 31, 2022 12:17 PM

In the suggested next steps section, you can:

- Set the priority of the threat graph
- Set the status of the threat graph
- Isolate the device from the network
- Scan the device depending on how you wish to investigate the threat
- Or run a Live Discover query

Incident Flow Graph



A graphical representation of the incident flow is displayed. The full graph is shown by default.

Using the drop-down menu you can view the direct path of the threat. The graph uses simple, clear iconography to help distinguish between the types of components. Coloured markers are used to denote the root cause, beacon event and items with an uncertain or bad reputation.

Threat Intelligence

The screenshot shows the Sophos Threat Analysis Center interface. On the left is a sidebar with navigation options: Dashboard, Threat Details, Live Discover, Detectors, Investigations, and Preferences. The main area displays a threat graph with nodes like 'sophos_https_test.exe' and 'elcar.txt.com'. A green callout box points to the 'elcar.txt.com' node, which has a flyout menu open. The flyout menu includes tabs for Report summary, Machine learning analysis, File properties, and File breakdown. It also features a 'Request Intel Intelligence' button and a note about sending files to SophosLabs. Below the graph, a legend identifies symbols for Root Cause, Beacon, Uncertain reputation, and Bad.

Select a component from the graph to view more information

When you select a component from the graph, you can view additional information about it in the flyout menu.

The flyout menu displays the available information for the component selected. The available tabs show the process details, report summary, machine learning analysis, file properties, and file breakdown.

You can **request the latest threat intelligence** from SophosLabs in the **Process details** tab to gain further insight into the threat.

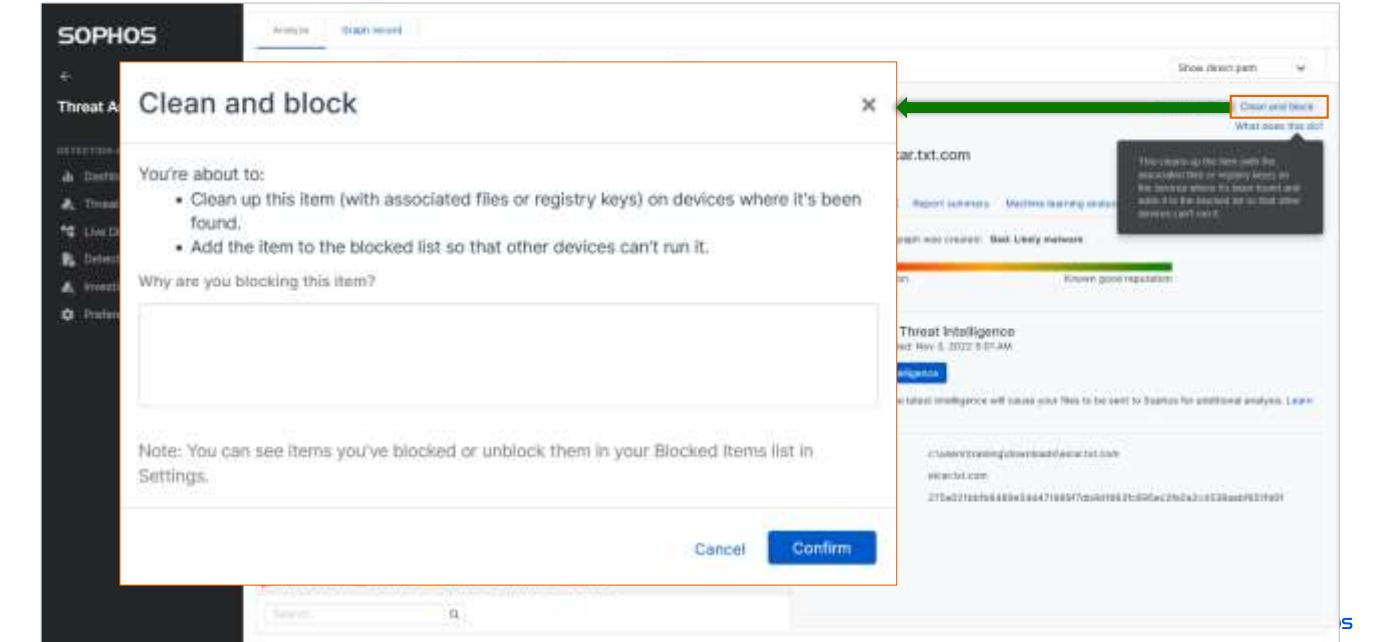
Threat Intelligence

The screenshot shows the Sophos Central XDR Threat Graphs interface. On the left, there's a sidebar with navigation icons. The main area displays a threat intelligence report for a file named "elcar.txt.com". The report includes sections for "Process details", "Report summary", and "SophosLabs Threat Intelligence". A fly-out menu is open at the top right, showing options like "Download PDF", "Clean and block", and "What items this file?". A green arrow points from the "Download PDF" option to the text "From the fly out menu you can select to perform additional actions.".

From the fly out menu you can select to perform additional actions.

Selecting **Download PDF** will download a copy of the threat intelligence report for the component selected.

Threat Intelligence



Selecting to **Clean and block** the detected item will clean up the item along with its associated files and registry keys on devices where it has been identified. It also adds the item to the blocked list so that other devices are unable to run the item.

We recommend entering a reason for blocking any item so that other administrators understand why an item has been blocked. Click **Confirm** to complete the action.

Please note that these options will only appear for those components where threat intelligence is available and where a clean and block action is appropriate.

Artefacts

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation options: Dashboard, Threat Graphs, Live Discover, Detectors, Investigations, and Preferences. The main area displays a threat graph with nodes like 'chrome_patch.packed.7z' and '192.0.2.49.101.198.153.49.102.191...' connected by arrows. Below the graph is a table of detected artefacts:

Name	Type	Reputation	Time Logged	Interactions
sophos_http_test.exe	Process	Uncertain reputation	Oct 31, 2022 9:45 AM	1383
192.0.2.49.101.198.153.49.102.191...	Process	Uncertain reputation	Oct 31, 2022 9:21 AM	180
chrome.exe	Process	Good	Oct 31, 2022 9:21 AM	411
httpd.exe	Process	Good	Oct 31, 2022 8:56 AM	325
192.0.2.49.101.198.153.49.102.191...	Process	Good	Oct 31, 2022 8:55 AM	15
chrome_patch.packed.7z	Other file	-		4
chrome.exe	Other file	Good		38
192.0.2.49.101.198.153.49.102.191...	Other file	Bad: Likely malware		1588
192.0.2.49.101.198.153.49.102.191...	Other file	Uncertain reputation		2

A green callout box in the top right corner says "Export the details to a CSV or create a forensic snapshot". Below the table are buttons for "Create forensic snapshot" and "Export to CSV".

At the bottom of a threat graph you can view all of the artefacts involved in the detected threat.

These can be searched and filtered, or exported to a CSV file. You can also create a forensic snapshot on the device to aid further investigation.

Graph Record

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation links: Dashboard, Threat Graphs, Live Discover, Defectors, Investigations, and Preferences. The main area is titled 'Graph Record' and contains a summary table and a 'Suggested next steps' section. A green callout box points to the 'Graph record' tab in the top navigation bar with the text: 'Enter notes into the Graph record to document investigative steps taken'.

Summary		Suggested next steps
Detection name:	EICAR-AV-Test	Set a status for the threat graph Priority: Medium Status: In progress
Root cause:	106.0.5249.119,106.0.5249.109_chrome_update.exe	Investigate 2 processes that we've marked with an "uncertain" reputation. See graph below for details
Possible data involved:	no business files	Isolate this device while you investigate
Where:	On Training-WIN that belongs to TRAINING-WIN\Training	Scan the device
When:	Detected on Oct 31, 2022 12:17 PM	Run a Live Discover query

Below the summary table, there are three log entries:

- UK Training + Nov 3, 2022 10:57 AM: Marked as medium priority.
- UK Training + Nov 3, 2022 10:07 AM: Started work on this graph.
- Oct 31, 2022 21:14 PM: Created graph.

You can also view the graph record, which can be used to log comments and actions taken. For example, the isolation status of the device, or the results of an investigation.

If you select to scan or isolate the device, run a Live Discover query, or change the priority and status of the threat graph, the actions are automatically added to the graph record.



Additional information in
the notes

Follow Up Actions

Submit a sample of any uncertain reputation files or suspicious files to Sophos for analysis

Block any URLs or IP addresses that have been identified as suspicious

Use application control to block or monitor applications across your network

SOPHOS

A threat graph can aid investigation into a detected threat. Following an investigation, some of the actions you may choose to take could be:

- To submit a sample of any uncertain reputation files or suspicious files to Sophos for analysis
- Block any URLs or IP addresses that have been identified as suspicious
- Use application control to block or monitor applications across your network

[Additional Information]

Further information and threat graph examples for malware detections can be found in knowledge base article [KB-000036359](https://support.sophos.com/support/s/article/KB-000036359). <https://support.sophos.com/support/s/article/KB-000036359>

Activity: Threat Graphs



Where can you find more information about the detected threat using the links available in the threat graph details?

Threat Analysis Center - EICAR-AV-Test

Overview Threat Analysis Center Dashboard Threat Details EICAR-AV-Test

Training-WT0 → Root Cause → Beacon → Detected → Cleaned

192.168.1.110 Windows Explorer test.com Sep 1, 2022 5:14 PM

Summary

Description name:	EICAR-AV-Test
Root cause:	Exploit.E9E
Possible data involved:	7 business files
Where:	On Training-WT0 that belongs to SOPHOS\SOFSAdministrator
When:	Detected on Sep 1, 2022 5:14 PM

Suggested next steps

Set a status for the threat graph	Priority: Medium	Status: New
The device has been isolated. Remove from isolation.	Isolate the device	
Run a Live Discover scan		

SOPHOS

In this activity, where can you find more information about the detected threat using the links available in the threat graph details.

Activity: Threat Graphs



Selecting the threat name will open a new tab containing information about that threat.

The screenshot shows the Sophos Threat Analysis Center interface. At the top, there's a navigation bar with links like Overview, Threat Analysis Center Dashboard, Threat Graphs, and EICAR-AV-Test. Below the navigation is a horizontal timeline diagram showing the flow from a host (Training-W10) to a root cause (Windows Explorer), then to a beacon (test.com), and finally to the threat itself (Detected). The main area is titled 'Summary' and contains details such as the detection name (EICAR-AV-Test), root cause (Windows Explorer), possible data involved (7 business files), where it was found (On Training-W10 that belongs to SORICKS\Administrator), and when it was detected (Sep 1, 2022 5:14 PM). A callout box highlights the 'EICAR-AV-Test' entry in the 'Detected name' field. To the right, a new tab is open with the title 'EICAR-AV-Test' and displays detailed threat information, including a summary table and a section for 'Affected Operating Systems'.

Selecting the threat name will open a new tab containing information about that threat.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

Where in a threat graph can you log investigative actions and comments about the threat detection?

Analyze

Artefacts

Graph record

SOPHOS



Question 2 of 2

What detections are displayed in a Threat Graph?

Any detections in the past
30 days

Any detections in the past
90 days

Any detections that require
action

Any detections that are
being investigated

SOPHOS

Chapter Review

Threat graphs are created for **informational and guided investigation**.

Threat graphs list any detections in the past **90 days** across your network.

Threat graphs **do not necessarily** require action.

SOPHOS

Here are the three main things you learned in this chapter.

Threat graphs are created for informational and guided investigation.

Threat graphs list any detections in the past 90 days across your network.

Threat graphs do not necessarily require action.



An Introduction to Sophos Central XDR Detections and Investigations

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4555: Getting Started with Sophos Central XDR Detections and Investigations

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

An Introduction to Sophos Central XDR Detections and Investigations

In this chapter you will learn what XDR detections and investigations are and how they can be used to protect your environment.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Understanding of what Sophos XDR is and its capabilities
- ✓ How to access Sophos Central

DURATION **11 minutes**

SOPHOS

In this chapter you will learn what XDR detections and investigations are, and how they can be used to protect your environment.

Threat Detections

Detections can be used to examine devices, processes, users, and events for signs of potential threats

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation links: Home, Threat Graphs, Live Discover, Detections (which is selected and highlighted in blue), Investigations, and References. The main area is titled 'Detections' and shows a table of threat findings. The table has columns for Rank, Count, Category, Last Seen, MITRE ATTACK, Devices, Connectors, Rate, and Investigation. There are seven entries listed:

Rank	Count	Category	Last Seen	MITRE ATTACK	Devices	Connectors	Rate	Investigation
1	240	Threat	Oct 7, 2022 1:07:38 PM	XX Discovery	XX Whois...	XX 5...	XX 0 mins...	XX MITRE-V...
2	218	Threat	Oct 6, 2022 4:01:52 PM	XX Credential...	XX Whois...	XX 5...	XX 0 mins...	XX MITRE-G...
3	172	Threat	Oct 13, 2022 8:25:42 PM	XX Defense L...	XX Whois...	XX 5...	XX 0 mins...	XX MITRE-V...
4	162	Threat	Oct 12, 2022 8:11:22 PM	XX Discovery	XX PEACE...	XX 5...	XX 0 mins...	XX MITRE-V...
5	152	Threat	Oct 7, 2022 3:50:49 PM	XX Credential...	XX Whois...	XX 5...	XX 0 mins...	XX MITRE-G...
6	541	Threat	Oct 4, 2022 10:22:40 AM	XX Defense L...	XX Whois...	XX 5...	XX 0 mins...	XX MITRE-V...

At the bottom right of the table, it says 'Last updated: Nov 1, 2022, 9:38 PM'. The Sophos logo is in the bottom right corner of the main window.

Detections can be used to examine devices, processes, users, and events for signs of potential threats that other Sophos features have not blocked.

For example, unusual commands that indicate attempts to inspect your systems, establish persistence, avoid security, or steal credentials.

Threat Detections

The screenshot shows the Sophos Threat Analysis Center dashboard. On the left, a sidebar lists navigation options: Threat Analysis Center, Detection and Remediation (Dashboard, Threat Graphs, Live Discover, Detections, Investigations, Preferences). The main area has three main sections:

- Recent detections:** A table showing 10 recent detections. The columns are Risk (red), Count (1-4), Category (Threat), MITRE ATT&CK (Impact...), Devices (Training...), Connectors (Training...), and Last seen (2 hrs, a day, 18 days, 1m 18 days, 1m 20 days). The entire section is highlighted with an orange border.
- Most recent threat graphs:** A table showing threat graphs generated by Sophos and Admin. It includes columns for Time created, Priority, Name, User, and Device (Training-W10, Training-W10, Training-W10). A green callout box points to this section with the text: "Recent detections are displayed in the Threat Analysis Center dashboard".
- Recent Live Discover queries:** A table showing successful logon queries. Columns include Query name (Successful logon (Data Lake)), Admin name (Simon Smith), Date (Oct 28, 2022 12:00 AM), and Status (Finished).
- Recently scheduled queries:** A table showing scheduled queries. Columns include Query name (Pay-the-hatch attacks..., Top threat indicators on..., Pending Windows updat...), Frequency (--), Admin name (Simon Smith, Simon Smith, UK Training), Source (Data Lake, Data Lake, Data Lake), and Last edited (Nov 11, 2021 10:42 AM, Nov 11, 2021 10:24 AM, Jun 30, 2021 11:18 AM).

Detections identify activity on your devices that is considered unusual or suspicious but has not been blocked. Detections show activities that you might need to investigate.

Recent detections are displayed on the Threat Analysis Center Dashboard.

Threat Detections

The screenshot shows the Sophos Threat Analysis Center interface. The left sidebar has a dark theme with white text and icons. It includes links for Dashboard, Threat Groups, Live Recovery, Investigations, and Preferences. The 'Detections' link is highlighted with a blue border. The main content area is titled 'Detections' and shows a table of threat findings. The table has columns for Risk, Count, Category, Last seen, MITRE ATT&CK, Devices, Connectors, Rule, and Investigations. There are 29 applied detections from the last 24 hours. Each detection row contains a checkbox, a risk score icon, a count, a category (e.g., Threat), a detailed description, a timestamp, and various status indicators.

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
3	8	Threat	Nov 1, 2022 1:03:54 PM	Defense E...	Training...	5	WIN-MITRE-V...	
3	16	Threat	Nov 1, 2022 1:29:56 PM	Credential...	Training...	5	WIN-MITRE-B...	
3	1	Threat	Nov 1, 2022 12:08:41 PM		Training...	5	EVENT-8625	
3	7	Threat	Nov 1, 2022 11:58:58 AM	Defense E...	Training...	5	WIN-MITRE-B...	
3	4	Threat	Nov 1, 2022 11:24:10 AM	Exfiltration	Training...	5	WIN-MITRE-B...	
3	1	Threat	Nov 1, 2022 11:24:10 AM	Collection	Training...	5	WIN-MITRE-B...	

To view all detections, navigate to **Threat Analysis Center > Detections**.

Detections are based on data that devices upload to the Sophos Data Lake. To view detections, you must enable **Data Lake uploads** in **Global Settings**.

Sophos checks the data against threat classification rules. When there's a match, a detection is shown. The score indicates the malicious intent of the activity.

Threat Detections

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with 'SOPHOS' at the top, followed by 'Threat Analysis Center' and several navigation items: Dashboard, Threat Graphs, Live Discover, Detections (which is selected and highlighted in blue), Investigations, and Preferences. The main area is titled 'Detections' and shows a table of threat detections. At the top of the table are filters: 'Show filters' (with '29 applied'), 'Last 1 Hour', 'Last 24 Hours', 'Last 7 Days', 'Last 30 Days' (which is selected and highlighted in blue), and 'Custom range'. To the right of the filters are columns for 'Last seen', 'MITRE ATT&CK', 'Devices', 'Connectors', 'Rule', and 'Investigations'. A modal window titled 'Filters' is open on the left, showing two sections: 'Risk' and 'Category'. Under 'Risk', there's a list from 0 (Not determined) to 10 (Highest). Under 'Category', there are three checked options: Threat, Vulnerability, and Process. The table lists six detection entries, each with a timestamp, attack tactic (Impact), device (Win10), connector (WinCloud), rule (WIN-MITRE-B...), and investigation link (2022-10-14-0...).

Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
Oct 14, 2022 11:06:47 AM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-10-14-0...
Oct 5, 2022 2:31:53 PM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-10-05-0...
Oct 7, 2022 2:07:33 PM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-10-07-0...
Oct 3, 2022 10:27:22 AM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-10-03-0...
Nov 1, 2022 11:24:10 AM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-11-01-001
Oct 13, 2022 5:29:03 PM	Impact	Win10	WinCloud	WIN-MITRE-B...	2022-10-13-0...

By default, only detections with a risk score of 7 or more will be displayed in the detections list. The risk score can be used to prioritize investigations.

You can change which detections are displayed by using the filter. Click **Show filters** and then select to filter the list on either risk, category, classification rule or attack tactic.

To make this process quicker if you want to view all detections, you can use the **Select all** option for risk and attack tactic. This makes it quick and easy to view all detections.

You can also filter the list to show detections based on a time period.

Detection Details

RISKRisk is measured on a scale from 1 (lowest risk) to 10 (highest risk)
Only detections with a risk score of 7 or more are displayed in the detection list by default

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
<input type="checkbox"/> > 10	1	Threat The adversary is trying to manipulate, interrupt, or ...	Oct 14, 2022 11:06:47 AM	Impact	READY...	5	WIN-MITRE-B...	2022-10-14-0...
<input type="checkbox"/> > 10	1	Threat The adversary is trying to manipulate, interrupt, or ...	Oct 5, 2022 2:31:53 PM	Impact	Training...	5	WIN-MITRE-B...	2022-10-05-0...

This is the name of the rule that was matched for the detection to be displayed

CLASSIFICATION RULE

SOPHOS

Detections are grouped according to the classification rule they matched and the date they were detected.

For each detection, the risk score is displayed. The risk score is a measure used to indicate how risky a threat could be. It is a scale from one to ten. A score of 0 indicates that a risk score could not be determined.

The classification rule for each detection is the name of the rule that was matched for the detection to be triggered and displayed.

Detection Details

COUNT

The number of times the classification rule has been matched

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
<input type="checkbox"/> > 10	1	Threat The adversary is trying to manipulate, interrupt, or ...	Oct 14, 2022 11:06:47 AM	Impact	<input type="checkbox"/> READI...	5	WIN-MITRE-B...	2022-10-14-0...
<input type="checkbox"/> > 10	1	Threat The adversary is trying to manipulate, interrupt, or ...	Oct 5, 2022 2:31:50 AM	Impact	<input type="checkbox"/> TR...	5	WIN-MITRE-B...	2022-10-05-0...

The last detection date and time based on the classification rule that day

LAST SEEN

DEVICES

The device(s) where the rule was last matched

SOPHOS

The count is the number of times the classification rule has been matched on a certain day.

The last seen date and time is based on the classification rule matched that day.

The devices column displays the device where the rule was last matched and the number of other devices with the same detection that day.

Detection Details

The screenshot shows the 'Detection Details' section of the Sophos Central XDR interface. A green callout box points to the 'CATEGORY' column header. Below it, a table lists detections categorized as Threat. The first row has a red circle icon with '30' and a count of '2'. The second row has a yellow circle icon with '3' and a count of '1'. The third row has a green circle icon with '1'. The fourth row is partially visible with '1' and '1'. The 'Category' column contains the word 'Threat' for all rows. A tooltip is shown over the first 'Threat' entry, providing a detailed description of the adversary's intent:

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data; in some cases, business processes can look fine, but may have been altered to benefit the adversary's goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidential breach.

Risk	Count	Category	Details
30	2	Threat	The adversary is trying to manipulate, interrupt, or ...
3	1	Threat	Detection events from Sophos Detections Journal.
1	1		

Below the table, there are sections for Devices, Connectors, Rule, and Investigations, each with a table of items. The bottom right corner of the screenshot says 'SOPHOS'.

The threat category displays the category of the detection, either threat, vulnerability or process along with a description of the expected behaviour. For example, the category in this example is a threat where the adversary is trying to manipulate, interrupt or destroy your systems and data. Hovering over the field will display more information.

Detection Details

Displays the identified attack tactic and technique

MITRE ATT&CK

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
<input type="checkbox"/>	2	Threat The adversary is trying to manipulate, interrupt, or...	Nov 1, 2022 2:08:33 PM	Impact	Trainin...	S	WIN-MITRE-B...	2022-11-01-001
<input type="checkbox"/>	10	Threat The adversary is trying to maintain their foothold. P...	Nov 1, 2022 2:33:22 PM	Persistence	Trainin...	S	WIN-MITRE-B...	
<input type="checkbox"/>	20	Threat The adversary is trying to avoid being detected. Def...	Nov 1, 2022 2:33:22 PM	Defense E...	Trainin...	S	WIN-MITRE-B...	
<input type="checkbox"/>	34	Threat The adversary is trying to steal account names and...	Nov 1, 2022 2:33:22 PM	Credential...	Trainin...	S	WIN-MITRE-B...	

SOPHOS

The Mitre ATT&CK column displays the identified attack tactic and technique.

Detection Details

The screenshot shows a table of detections with various columns: Risk, Count, Category, Last seen, MITRE ATT&CK, Devices, Connectors, Rule, and Investigations. Two detections are highlighted:

- Risk:** Threat (10)
- Count:** 2
- Category:** Threat
- Last seen:** Nov 1, 2022 2:08:33 PM
- MITRE ATT&CK:** Impact (highlighted with a red box)
- Devices:** 5
- Connectors:** WIN-MITRE-B...
- Rule:** 2022-11-01-001
- Investigations:** 2022-11-01-001

Risk: Threat (5)

Count: 1

Category: Threat

Last seen: Nov 1, 2022 2:00:01 PM

MITRE ATT&CK: Impact (highlighted with a red box)

Devices: 5

Connectors: SOPHOS-DET...

Rule: 2022-11-01-001

Investigations: 2022-11-01-001

A callout box from the first detection points to the Impact link in the MITRE ATT&CK column of the second detection.

MITRE ATT&CK Detail View:

- Technique:** Data Encrypted for Impact
- Description:** Attacker may encrypt sensitive or large volumes of data in plaintext to increase its durability or reduce transmission time. They can also encrypt sensitive data before exfiltrating them or data exfiltration systems. This is particularly common in勒索软件 (Ransomware). This may be done in order to extract monetary compensation from a victim or to prevent decryption by an adversary (throughout or to render corresponding recovery of data where the key is held or lost).
- Notes:** In the case of ransomware, it is critical that consumers use files like ZIP files, documents, PDFs, images, videos, audio files, and source code that are encrypted with different encryption or flagged under specific file formats. Attacker may repackage ransomware files before launching, such as PDF and Microsoft Office documents. Malicious or stolen documents, files, emails, or links can also gain access to compromised files they're trying to steal. In some cases, attackers may encrypt entire system files, user accounts, and the MBR.
- Links:** To learn more about this technique, click here for more information. Learn more about this technique in the following articles: Compromised File Encryption, Ransomware, and勒索软件 (Ransomware), and勒索软件 (Ransomware) (2022-11-01-001). Read about how threat actors can use this technique in the following article: Threat Actor Techniques: Encrypting Data to Demand Ransom.

SOPHOS

Most detections are linked to the MITRE ATT&CK framework, hovering over the attack technique will provide a link where you can find more information on the specific attack technique.

Clicking on the link will open a new window in your Internet browser which redirects you to the attack framework providing you more information.

Detection Details

The screenshot shows the Sophos Central XDR Detections interface. At the top, there's a navigation bar with links for Overview, Threat Analysis, Central Dashboard, and Detections. On the right side of the header are links for Help, UK Training, Sophos UK, and Super Admin. Below the header is a toolbar with filters: Show filters, 20 applied, Last 1 Hour, Last 24 Hours, Last 7 Days, Last 30 Days, Custom range, and a Refresh button.

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
15	2	Threat The adversary is trying to manipulate, intercept, or... [Expand]	Nov 1, 2022 2:08:33 PM	Impact	2 Train... 2 Team... 2 Scan... 2 Log... 2 File... 2 Network... 2 Process... 2 Registry... 2 Task... 2 Service... 2 Credential... 2 Persistence... 2 Defense E... 2 Exploit E... 2 Privilege Escalation... 2 Reconnaissance... 2 Lateral Movement... 2 Persistence... 2 Impact	5	WIN-MITRE-B... 2022-11-01-001	
15	10	Threat The adversary is trying to maintain their footprint. [Expand]	Nov 1, 2022 2:33:22 PM	Persistence	2 Train... 2 Team... 2 Scan... 2 Log... 2 File... 2 Network... 2 Process... 2 Registry... 2 Task... 2 Service... 2 Credential... 2 Persistence... 2 Defense E... 2 Exploit E... 2 Privilege Escalation... 2 Reconnaissance... 2 Lateral Movement... 2 Persistence... 2 Impact	5	WIN-MITRE-B... 2022-11-01-002	
15	20	Threat The adversary is trying to avoid being detected. [Expand]	Nov 1, 2022 2:33:22 PM	Defense E...	2 Train... 2 Team... 2 Scan... 2 Log... 2 File... 2 Network... 2 Process... 2 Registry... 2 Task... 2 Service... 2 Credential... 2 Persistence... 2 Defense E... 2 Exploit E... 2 Privilege Escalation... 2 Reconnaissance... 2 Lateral Movement... 2 Persistence... 2 Impact	5	WIN-MITRE-B... 2022-11-01-003	
15	34	Threat The adversary is trying to steal account names and... [Expand]	Nov 1, 2022 2:33:22 PM	Credential... Steal...	2 Train... 2 Team... 2 Scan... 2 Log... 2 File... 2 Network... 2 Process... 2 Registry... 2 Task... 2 Service... 2 Credential... 2 Persistence... 2 Defense E... 2 Exploit E... 2 Privilege Escalation... 2 Reconnaissance... 2 Lateral Movement... 2 Persistence... 2 Impact	5	WIN-MITRE-B... 2022-11-01-004	
15	14	Threat The adversary is trying to steal account names and... [Expand]	Oct 31, 2022 8:12:31 PM	Credential... Steal...	2 Train... 2 Team... 2 Scan... 2 Log... 2 File... 2 Network... 2 Process... 2 Registry... 2 Task... 2 Service... 2 Credential... 2 Persistence... 2 Defense E... 2 Exploit E... 2 Privilege Escalation... 2 Reconnaissance... 2 Lateral Movement... 2 Persistence... 2 Impact	5	WIN-MITRE-B... 2022-11-01-005	
15	1	Threat Sophos Web Control blocked access to a website. [Expand]	Oct 31, 2022 6:39:49 PM	Train... Team... Scan... Log... File... Network... Process... Registry... Task... Service... Credential... Persistence... Defense E... Exploit E... Privilege Escalation... Reconnaissance... Lateral Movement... Persistence... Impact	5	SOPHOS-MT... 2022-10-31-001		

To view further details of a detection, click the arrow next to the risk score. This will expand the detection details.

SOPHOS

Detection Details

The screenshot shows the Sophos Central XDR interface. On the left, a sidebar titled 'Threat Analysis Center' includes links for Dashboard, Threat Graphs, Live Discover, Detections (which is selected), Investigations, and Preferences. The main area displays a threat summary: 'Threat' (Nov 1, 2022 2:08:33 PM) with the note 'The adversary is trying to manipulate, interrupt, or ...'. Below this, a card for 'Training-W10' (Nov 1, 2022 2:08:33 PM) lists various detection parameters like detectionCreatedAt, attackType, category, severity, mitreAttacks, detectionAttack, id, detectionType, geolocation, intelixFileReputation, connectorGeneratedAI, and rawData. A large modal window is open over the main content, showing 'Queries' and 'Actions' sections. The 'Actions' section contains links to 'Scan this device', 'Start Live Response session', and other options. The 'Object' section at the bottom of the modal lists fields: calendar_time, counter, customer_id (with value '5550411b-07d2-48bd-9679-bc09a660403d'), and customer_region (with value 'EU-West-T').

When viewing the expanded detection details, more detailed information is displayed.

Clicking on any of the ellipsis menus presents you with additional options and actions. In this example, you could select to run a Data Lake query, scan the device or start a Live Response session.

Investigations

- Provides to the tools to investigate potential threats
- Groups suspicious events based on detections
- Investigations are created automatically and focus on detections that may require additional investigation

The screenshot shows the Sophos Central Threat Analysis Center interface. On the left, a sidebar titled 'Threat Analysis Center' lists categories: User Agent, Threat Groups, User Devices, Detections, Investigations (which is selected and highlighted in blue), Malicious URLs, and Preferences. The main area is titled 'Investigations' and displays a table of current investigations. The table columns include: Priority (High, Medium, Low), Investigation ID (e.g., 2022-11-02-001, 2022-11-02-002, etc.), Status (Not Started, Unassigned), Assigned To (Unassigned), Created (e.g., 2022-11-02 08:00:00), Age (e.g., 5 days), Devices (e.g., 0.1), Connections (e.g., 0.1), Detections (e.g., 0.1), Last Modified (e.g., Nov 2, 2022, 09:05:51 AM), and Last Detected (e.g., Nov 2, 2022, 09:05:51 AM). Below the table, there are navigation buttons (Back, Forward, Home) and a 'Summary' link.

Priority	Investigation ID	Status	Assigned To	Created	Age	Devices	Connections	Detections	Last Modified	Last Detected	Summary
High	2022-11-02-001	Not Started	Unassigned	2022-11-02 08:00:00	5 days	0.1	0.1	0.1	Nov 2, 2022, 09:05:51 AM	Nov 2, 2022, 09:05:51 AM	Initial Detection: WIN-MTTE-BROWSER...
High	2022-11-02-002	Not Started	Unassigned	2022-11-02 08:00:00	5 days	0.1	0.1	0.1	Nov 6, 2022, 3:40:49 AM	Nov 6, 2022, 9:00:23 PM	Initial Detection: SOPHOS-DET-BROWSER...
High	2022-11-02-003	Not Started	Unassigned	2022-11-02 08:00:00	5 days	0.3	0.1	0.1	Nov 6, 2022, 3:40:49 AM	Nov 6, 2022, 9:00:27 PM	Initial Detection: WIN-MTTE-BROWSER...
High	2022-11-02-004	Not Started	Unassigned	2022-11-02 08:00:00	5 days	0.3	0.1	0.1	Nov 6, 2022, 3:40:49 AM	Nov 6, 2022, 9:00:29 PM	Initial Detection: WIN-MTTE-BROWSER...
High	2022-11-02-005	Not Started	Unassigned	2022-11-02 08:00:00	5 days	0.6	0.1	0.1	Nov 6, 2022, 3:40:49 AM	Nov 6, 2022, 9:00:31 PM	Initial Detection: WIN-MTTE-BROWSER...
High	2022-11-02-006	Not Started	Unassigned	—	—	—	—	—	Nov 6, 2022, 3:40:49 AM	Nov 6, 2022, 9:00:31 PM	Initial Detection: WIN-MTTE-BROWSER...

The **Investigations** page in Sophos Central groups suspicious events together to aid investigation into potential threats. Like detections, investigations are based on data held in the Data Lake, therefore you must ensure that **Data Lake uploads** are enabled for all devices to view investigation details.

Investigations are created automatically in Sophos Central and focus on detections that may require additional investigation. Investigations are based on the detection type which corresponds with the classification rule of a detection, the risk level and the device where it occurred.

You can create your own investigations.

Investigation Priority

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation options like Dashboard, Threat Graphs, User Discover, Detections, Investigations (which is selected), Integrations, and Preferences. The main area displays an 'Investigation Record' for '2022-11-04-001'. The record includes fields for Priority (set to High), Status (Not Started), Investigation ID (2022-11-04-001), Assigned To (Type to assign), and various timestamps and device information. A large green callout box with the text 'Change the priority of an investigation' points to the priority dropdown menu.

An investigation record displays the priority, status, and investigation ID. These details can be edited to suit your requirements.

The priority of an investigation can be amended to reflect how important the investigation is.

Investigation Progress

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with navigation options like Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is selected), Integrations, and Preferences. The main area displays an investigation record for '2022-11-04-001'. A dropdown menu is open over the 'Status' field, showing options: Not Started (selected), In Progress, On Hold, Archived, and Closed. A green callout box with the text 'Change the status of an investigation' points to this dropdown. The investigation summary section contains the text 'Initial Detection: KYN-MITRE-Behavioral-TA0004D-T1498'. The bottom right corner of the screen shows a watermark: 'Last updated: Nov 8, 2022, 2:57 PM'.

You can change the status of the investigation to indicate whether the investigation is in progress, on hold, archived or closed.

Investigation ID

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a sidebar menu includes options like Dashboard, Threat Graphs, User Discover, Detections, Investigations (which is selected), Integrations, and Preferences. The main content area displays the 'Investigation Record' for '2022-11-04-001'. Key details shown include:

- Investigation ID:** 2022-11-04-001
- Creation date:** Nov 4, 2022 12:25 AM
- Created by:** Sophos
- Sentences:** 0
- Last update:** Nov 4, 2022 2:01 PM
- Deadline:** 30 days after the investigation is closed.
- Device:** Training-WIN-WinClient1
- Connectors:** Sophos
- Assigned to:** Type to assign

Below the record, there's an 'Investigation Summary' section with a note about initial detection (W32-MITRE-Behavior) and a 'View full trail' link. A 'Detection List' section is also present at the bottom.

The investigation ID can be amended to give it a more meaningful name. This makes finding the investigation you want and sharing investigative tasks easier for administrators.

Investigation Assignment

The screenshot shows the Sophos Central Threat Analysis Center interface. On the left, a sidebar menu includes 'Dashboard', 'Threat Graphs', 'User Discover', 'Discoveries', 'Investigations' (which is selected), 'Integrations', and 'Preferences'. The main content area displays an 'Investigation Record' for '2022-11-04-001'. The record shows the following details:

- Severity:** High
- Status:** Not Started
- Investigation ID:** 2022-11-04-001
- Created by:** Sophos
- Selections:** 0
- Creation date:** Nov 4, 2022 12:25 AM
- Most recent detection:** Nov 4, 2022 2:01 PM
- Last update:** Nov 4, 2022 2:01 PM
- Data expires:** 30 days after the investigation is closed.
- Bases:** Training-WIN
- Connectors:** Staples

A green callout box points to the 'Assigned to' section, which lists 'Administrator' with a checked checkbox. Other administrator users listed are Ben Smith, Central Demo Admin, Ed Kongsberg, and Rob Admin. A 'Reset' button is also present in this section.

You can assign the investigation to any user with an administrator role in Sophos Central. It is useful to ensure that investigation work is not duplicated among your administrators.

Investigation Details

The screenshot shows the 'Investigation Record' section of the Sophos Central XDR interface. At the top, there are dropdown menus for 'Severity' (High), 'Status' (In Progress), and 'Investigation' (Training Example). Below these are several data fields:

Investigation ID	2022-11-04-001	Creation date	Nov 4, 2022 12:25 AM	Devices	Training-W10
Created by	Sophos	Most recent detection	Nov 4, 2022 2:01 PM	Connectors	Sophos
Detections	6	Last update	Nov 8, 2022 3:12 PM	WinClient1	
		Data expires	30 days after the investigation is closed.		

Three callout boxes highlight specific information:

- Who created the investigation and how many detections are currently included
- Creation date, most recent detection date, the last update and the date the data expires
- Which devices have detections and connectors details

SOPHOS

The investigation details summary displays the investigation ID, Sophos will be listed for all automatically created investigations.

The amount of detections included in the investigation is listed along with the creation date of the investigation, the most recent detection, the last update and the date that the data included in the investigation will expire. We do not close automatically created investigations, however, we do delete them after 30 days if the status is **Not Started** or **Closed**.

The devices where the potential threats have been detected are displayed allows you to see at a glance how many devices are affected by the potential threat.

Investigation Summary

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a sidebar lists navigation options: Threat Analysis Center, DETECTION AND INVESTIGATION (Dashboard, Threat Graphs, Live Discover, Detections, Investigations, Integrations, Preferences), and a user icon. The 'Investigations' option is selected and highlighted in blue. The main content area has two main sections: 'Investigation Summary' and 'Detection List'. The 'Investigation Summary' section contains a summary box with the following text:
Initial Detection: WIN-MITRE-Behavioral-TA0040-T1486
Checked devices are up-to-date
Started full system scan on both devices

A green callout box with the text 'Add any summary notes to an investigation' points to the bottom right of the summary box.

The 'Detection List' section shows a table with the following columns: Risk, Count, Category, Last seen, MITRE ATT&CK, Devices, Connectors, Rule, and Investigations. One row is visible, representing a Threat detection:

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Rule	Investigations
?	10	Threat	Nov 4, 2022 2:01:27 PM	Impact	Tr... 1 more...	🔗	WIN-MITR...	Training E...

An 'Investigation Notes' section is located at the bottom of the detection list.

In the 'Investigation Summary' you will see a summary of what has happened during the investigation. You can write any summary notes, when you click out of the summary box the details are automatically saved and can be edited at any time.

Clicking the **View audit trail** link will re-direct you to the 'Audit log' in Sophos Central. Investigations are listed with the item type 'Investigation'.

Detection List

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a sidebar lists navigation options: Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is selected), Integrations, and Preferences. The main area is titled 'Investigation Summary' and displays the following information:

- Initial Detection: WIN-MITRE-Behavioral-TA0040-T1486
- Checked devices are up-to-date
- Started full system scan on both devices

Below this is a 'Detection List' table with the following columns: Risk, Count, Category, Last seen, MITRE ATT&CK, Devices, and Actions. The first row shows a single threat detection:

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Actions
?	10	Threat	Nov 4, 2022 2:01:27 PM	Impact	1 more...	Add detections

A green callout box points to the 'Actions' dropdown menu, which includes the option 'Add detections'. The 'Actions' menu also lists 'Remove selected detections' and other options.

The detections included in the investigation are grouped. An overview of the detection is displayed, expanding the detection will display each of the detection details.

The drop-down actions menu gives you the options to either add or remove detections from an investigation.

Detections List

- Detections can be added to multiple investigations



Type B detection
Type C detection



Type B detection



Type D detection
Type B detection

Investigation One

Device	Detection Type
Detection B for Device One	Detection B for Device One
Detection C for Device One	Detection B for Device Two
	Detection B for Device Three

Investigation Two

Device	Detection Type
Detection D for Device Three	Detection D for Device Three
	Detection B for Device Three

SOPHOS

Detections can be added to multiple investigations. It is useful to understand why. Let's look at an example.

A type 'B' detection is found on device one which creates a new investigation which we will call 'investigation one'.

A type 'C' detection is found on device one, because it is found on the same device, the detection is added to 'investigation one'.

The type 'B' detection is found on device two. Because it is the same detection type as found on device one, the detection is added to 'investigation one'.

A type 'D' detection is found on device three, because this is a new detection type on a different device, 'investigation two' is created.

The type 'B' detection is found on device three and so the detection is added to 'investigation one'. The detection was found on device three so the detection is also added to 'investigation two'.

Investigation Notes

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with various navigation options like Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is selected), Integrations, and Preferences. The main area is titled 'Investigation Notes' and contains a rich text editor toolbar. Below the toolbar, a heading says 'Observe-Orient-Decide-Act'. It includes a note about documenting investigations and provides prompts for verdicts and actions. There are sections for 'Related investigations' (linking to others or closing as a duplicate) and 'Early Exit' (closing the investigation with a note). It also lists steps for each detection: 'Observe', 'External connections', and questions about external IPs, URLs, and threat intel. A general note at the bottom says to click anywhere in the box to begin typing.

In the ‘Investigation Notes’ section you can document investigative steps taken. Sophos provides prompts to aid all investigations that include housekeeping investigations, checking external and internal connections, understanding the detections including the tactic and technique identified.

The notes prompt you to check how frequently detections are being created, is there an errant file that is causing multiple detections and investigations to be created?

Finally, it prompts you to determine what action should be taken from the investigation. It could be that no action is required, however, we recommend checking all suspicious detections to ensure your network is secure.

Creating Investigations Manually

Create a new investigation and then added detections to it

Actions ▾

Create New Investigation

Priority	Investigation	Status	Assigned to	Created by	Age	Devices	Connectors	Detections	Last modified	Last detection	Summary
High	2022-11-0...	Not Started	Unassigned	S...	a day	1	1	1	Nov 7, ... a day	Nov 7, 2022 10:04:46 AM	Initial Detection: WIN-MITR...
High	2022-11-0...	Not Started	Unassigned	S...	2 days	1	1	2	Nov 6, ... 2 days	Nov 6, 2022 5:08:22 PM	Initial Detection: SOPHOS...
High	Training Ex...	In Progress	Administrat...	S...	5 days	2	1	6	Nov 8, ... an hour	Nov 4, 2022 2:03:27 PM	Initial Detection: WIN-MITR...
High	2022-11-0...	Not Started	Unassigned	S...	5 days	2	1	2	Nov 3, ... 5 days	Nov 3, 2022 4:28:05 PM	Initial Detection: WIN-MITR...
High	2022-11-0...	Not Started	Unassigned	S...	6 days	6	1	13	Nov 2, ... 6 days	Nov 2, 2022 0:46:41 PM	Initial Detection: WIN-MITR...

You may want to create your own investigation. You can create an investigation and then add detections to it by navigating to **Threat Analysis Center > Investigations > Actions > Create New Investigation**.

Creating Investigations Manually

The screenshot shows the Sophos Threat Analysis Center dashboard. On the left, there's a sidebar with navigation options: Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is selected and highlighted in blue), Integrations, and Preferences. The main content area has a title "Training Example 3" and a breadcrumb trail: Channel / Threat Analysis Center Dashboard / Investigations / Training Example 3. The main panel is titled "Investigation Record" and displays the following details:

Priority	Last updated	Investigation	Assigned to
LOW	Nov 8, 2022 4:53 PM	Training Example 3	Type to assign

Below this, there are sections for "Investigation ID" (2022-11-09-002), "Created by" (UK Training), "Creation date" (Nov 8, 2022 4:53 PM), "Most recent interaction" (dropdown), "Last update" (dropdown), and "Close express" (30 days after the investigation is closed). There's also a "More" link and a "View audit trail" button. At the bottom, there's a "Detection List" section with a "Last updated" timestamp (Nov 8, 2022, 4:53 PM) and an "Actions" button.

Once you have given the investigation a name, you can configure the priority, progress and assignment. You can also enter a summary.

Creating Investigations Manually

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with the Sophos logo and navigation links: Dashboard, Threat Graphs, Live Discover, Detections, Investigations (which is highlighted in blue), Integrations, and Preferences. The main area has tabs for 'Dashboard' (selected), 'UK Training', and 'Most recent detection'. Below these are sections for 'Investigation Summary' (with a note 'Created for demonstration'), 'Detections List' (empty with a note 'No detections found'), and 'Investigation Notes' (empty). A modal window titled 'Add detections' is open over the detections list, showing a dropdown menu with 'Selected detections' and a 'Run' button.

You can add detections to your investigation using the actions drop-down menu and selecting the detections from the detections list.

Once you have added your detections they will appear in the investigation. You can also remove them if required.

Creating Investigations Manually

The screenshot shows the Sophos Threat Analysis Center interface. On the left, a dark sidebar lists navigation options: Dashboard, Threat Graphs, Live Discover, **Detections** (which is selected), Investigations, Integrations, and Preferences. The main area is titled "Detections" and shows a table of detected threats and vulnerabilities. The table columns include Risk, Count, Category, Last seen, MITRE ATT&CK, Devices, Connectors, and Actions. There are four rows of data:

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Actions
Threat	54	Threat	Nov 7, 2022 5:43:55 PM	Comm... Wi... Defen...	1 more... 1 more... 1 more...	5 S 5	Add to Investigation Create new investigation
Vulnerability	4	Vulnerability	Nov 7, 2022 5:38:19 PM	Comm... Wi... Threat...	1 more... 1 more...	S COMPU...	
Threat	4	Threat	Nov 7, 2022 5:33:08 PM	Comm... Wi...	1 more...	S	WIN-MITR...
Threat	30	Threat	Nov 7, 2022 5:22:14 PM	Defen... Wi... Wi...	1 more... 1 more... 1 more...	5 S 5	WIN-MITR...

At the bottom right of the table, it says "Last updated: Nov 8, 2022, 4:45 PM".

You can create a new investigation from the detections page by selecting a detection and selecting the actions drop-down menu.

Name the investigation and click **Create Investigation**.

Investigations and Detections

The screenshot shows the Sophos Threat Analysis Center Detections page. The left sidebar has a dark theme with navigation links: Dashboard, Threat Graphs, User Overview, **Detections**, Investigations, Integrations, and Preferences. The main content area has a light background with a header 'Detections' and a breadcrumb 'Overview > Threat Analysis Center Dashboard > Detections'. It includes a time range selector with options: Show filters, Last 1 hour, Last 24 hours, Last 7 days, Last 30 days, Custom range. A table lists detections:

Risk	Count	Category	Last seen	MITRE ATT&CK	Devices	Connectors	Status	Investigations
Medium	1	Threat The adversary is trying to communicate with compromised...	Nov 7, 2022 5:43:35 PM	Command and Control	WinClient1	5	WIN-MITRE-BIN...	Training Example
Medium	1	Vulnerability SRP path rules missing	Nov 7, 2022 5:38:18 PM	WinServ1	5	COMPLIANCE-SL...	Training Example	
Medium	2	Threat The adversary is trying to communicate with compromised...	Nov 7, 2022 5:33:08 PM	Command and Control	WinClient1	5	WIN-MITRE-VOL...	Training Example
Medium	7	Threat The adversary is trying to avoid being detected. Defense Evasion	Nov 7, 2022 5:22:14 PM	Defense Evasion	WinClient1	1 hour	WIN-MITRE-VOL...	Training Example
Medium	1	Threat The adversary is trying to communicate with compromised...	Nov 7, 2022 5:18:13 PM	Command and Control	WinClient1	5	WIN-MITRE-VOL...	Training Example
Medium	1	Vulnerability SRP path rules missing	Nov 7, 2022 5:08:02 PM	WinServ1	5	COMPLIANCE-SL...	Training Example	

At the bottom right of the table, it says 'Last updated: May 8, 2022, 5:00 PM'.

Investigations that are ‘In Progress’ will be listed on the detections page. Clicking on the investigation name will redirect you to the investigation.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!

Question 1 of 2



Select where you would click to find out more information about the attack technique.

The screenshot shows a threat detection in Sophos Central XDR. At the top, there's a header with a yellow circular icon, the number '2', the word 'Threat', a timestamp ('Oct 19, 2022 10:49:11 AM'), and several status indicators like 'Defense E...', 'SRV', and a shield icon. Below the header, four numbered boxes (A, B, C, D) are arranged in a 2x2 grid. Orange arrows point from each box to specific UI elements above them: Box A points to the yellow circular icon and the number '2'; Box B points to the 'SRV' indicator; Box C points to the shield icon; and Box D points to the 'Defense E...' indicator.

A

B

C

D

SOPHOS



Question 2 of 2

True or False: To view XDR detections you must enable Data Lake uploads.

True

False

SOPHOS

Chapter Review

Detections **identify activities** that are unusual or suspicious but **not blocked**.

Detections and investigations are **based on data held in the Data Lake**, Data Lake uploads must be enabled for detections and investigations to be created.

Sophos checks the data against threat classification rules and **applies a risk score to all detections**.

SOPHOS

Here are the three main things you learned in this chapter.

Detections identify activities that are unusual or suspicious but not blocked.

Detections and investigations are based on data held in the Data Lake, Data Lake uploads must be enabled for detections and investigations to be created.

Sophos checks the data against threat classification rules and applies a risk score to all detections.



Sophos Central XDR Live Response

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE4560: Sophos Central XDR Live Response

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

Sophos Central XDR Live Response

In this chapter you will learn how to enable and use Live Response.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access and navigate Sophos Central
- ✓ How to apply global settings
- ✓ How to protect and manage devices in Sophos Central

DURATION **4 minutes**

SOPHOS

In this chapter you will learn how to enable and use Live Response.

Live Response Overview

- Direct command line interface
- Privileged remote terminal session
- Perform IT operation actions remotely

The screenshot shows the Sophos Central Endpoint Protection interface for a device named 'Training-W10'. The 'Live Response' tab is highlighted in orange. On the left, there's a sidebar with icons for Firewall, Antivirus, Endpoint Protection, and Device. Below the sidebar are buttons for 'Connect Now', 'Device', 'Live Response' (which is active), and 'More options'. The main area has tabs for 'SUMMARY', 'Events', 'STATUS', and 'FILES'. Under 'Recent Events', it lists several log entries with timestamps and descriptions. Under 'Agent Summary', it shows the last agent update was 3 minutes ago, and the last deployment was successful. A table below lists assigned products: Core Agent, Sophos Intercept X, Endpoint Protection, Device Encryption, and RDS, each with a status indicator and a timestamp.

Assigned Product	Status	Last Deployment
Core Agent	✓	08/22/2022 11:10 AM
Sophos Intercept X	✓	08/22/2022 11:10 AM
Endpoint Protection	✓	08/22/2022 11:10 AM
Device Encryption	✗ Pending	08/22/2022 11:10 AM
RDS	✓	08/22/2022 11:10 AM

Live Response provides direct command line access to any managed device from Sophos Central.

The direct command line is a privileged remote terminal session that gives full system level access to any Sophos protected device in your network.

Use Case Scenarios

Install and uninstall software

Browse the file system to identify anything unexpected

View list of running processes and choose to terminate anything suspicious

View log files

Reboot a device that has pending updates

Edit configuration files or registry keys

SOPHOS

You can use Live Response to run a terminal command remotely on any protected endpoint in your network. For example, you can:

- Install and uninstall software
- View a list of running processes and choose to terminate anything suspicious
- Reboot a device that has pending updates
- Browse the file system to identify anything unexpected
- View log files
- Edit configuration files or registry keys

How to Get Started



Administrator must have Super Admin role

Select Live Response from Global Settings

The screenshot shows the Sophos Central XDR interface. On the left, there's a navigation sidebar with various menu items like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is highlighted with a blue selection bar), Third-party Connectors, External Devices, Account Health Check, and several sections under System Resources: Endpoint Protection, Server Protection, Mobile, Encryption, and Wireless. To the right of the sidebar, there are two main sections: 'Device Migration' and 'Endpoint Protection'. Under 'Endpoint Protection', there's a 'Live Response' section with a sub-section 'Data Lake options'. Below that is another 'Live Response' section with a sub-section 'Data Lake options'. The entire 'Live Response' area is highlighted with a red box. At the bottom right of the interface, the word 'SOPHOS' is visible.

To use Live Response an administrator must have the Super Admin role assigned to them.

Live Response must be enabled for supported endpoints and servers in **Global Settings**.

You will see that 'Live Response' is listed in the 'Endpoint Protection' and 'Server Protection' sections in **Global Settings**. To enable Live Response for your endpoints and your servers, you will need to ensure you have enabled it in both sections.

How to Get Started

Live Response

[Global Settings](#) | [Live Response](#)

Allow Live Response connections to
Computers

Help + UK Training +
Sophos UK - Super Admin

[Save](#) [Cancel](#)

Manage Live Response for your computers, which lets you connect directly to computers to investigate and remediate possible security issues. For servers, [click here](#)

Allow Live Response connections to computers

If you turn this on, you can use Live Response to connect to any supported computer on your network.

Note: To start Live Response sessions you must be a Super Admin or have a role that includes "Start Live Response sessions on computers". You must also use multi-factor authentication.

Live Response

[Global Settings](#) | [Live Response](#)

Allow Live Response connections to
Servers

Help + UK Training +
Sophos UK - Super Admin

[Save](#) [Cancel](#)

Manage Live Response for your servers, which lets you connect directly to servers to investigate and remediate possible security issues. For computers, [click here](#)

Allow Live Response connections to servers

If you turn this on, you can use Live Response to connect to any supported server on your network.

Note: To start Live Response sessions you must be a Super Admin or have a role that includes "Start Live Response sessions on servers". You must also use multi-factor authentication.

SOPHOS

Use the slider to allow live response connections.

How to Get Started

The screenshot shows the 'Live Response' settings page in Sophos Central XDR. At the top, there are global settings and a note about connecting directly to computers for investigation. A large green callout box on the right side points to the 'Excluded' list, which contains several computer names. The 'Available' list includes various endpoints and servers.

Manage Live Response for your computers, which will you connect directly to computers to investigate and remediate possible security issues. For servers, click here.

Allow Live Response connections to computers

If you turn this on, you can use Live Response to connect to any supported computer on your network.

Note: To start Live Response sessions you must be a Super Admin or have a role that includes "Start Live Response sessions on computers". You must also use multi-factor authentication.

Exclusions

If you want to block Live Response connections to any of your computers, add those devices to the Excluded list below.

Available

Search	Available
DESKTOP-PROJECTA	<input type="checkbox"/>
laptopk Virtual Machine	<input checked="" type="checkbox"/>
Training-WW	<input type="checkbox"/>
WinClient1	<input type="checkbox"/>
WinClient2	<input type="checkbox"/>
WinClient3	<input type="checkbox"/>
WinClient4	<input type="checkbox"/>
WinClient5	<input type="checkbox"/>
Windows-MD	<input type="checkbox"/>

Excluded

Search	Excluded
MacBook Air	<input type="checkbox"/>
VM-0000000000000000	<input type="checkbox"/>

Select computers to exclude from Live Response

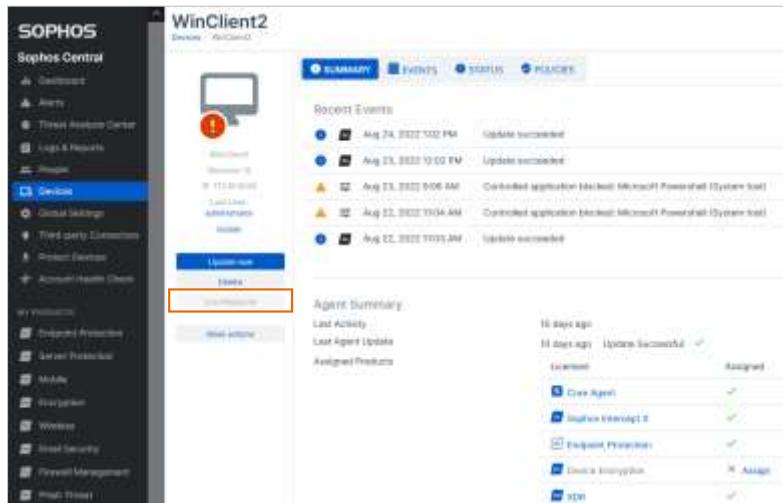
SOPHOS

You can also select endpoints and servers to exclude from Live Response. This will block any Live Response connections to those devices in the excluded list.

How to Get Started

Live Response will be disabled if:

- ◆ The device is offline
- ◆ Live Response is not enabled
- ◆ The device is excluded from Live Response



The screenshot shows the Sophos Central interface. On the left, a sidebar menu includes 'Devices' which is currently selected and highlighted in blue. The main content area displays a device summary for 'WinClient2'. At the top right of the summary card, there is a large 'Live Response' button, which is also highlighted with a red box. Below the summary card, there is a timeline of recent events, an 'Agent Summary' section, and a 'Licenses' section.

SOPHOS

Once enabled, Live Response is launched from the **Devices** page in Sophos Central.

The Live Response option will be greyed out if:

- The device is offline
- Live Response is not enabled
- The device is excluded from Live Response

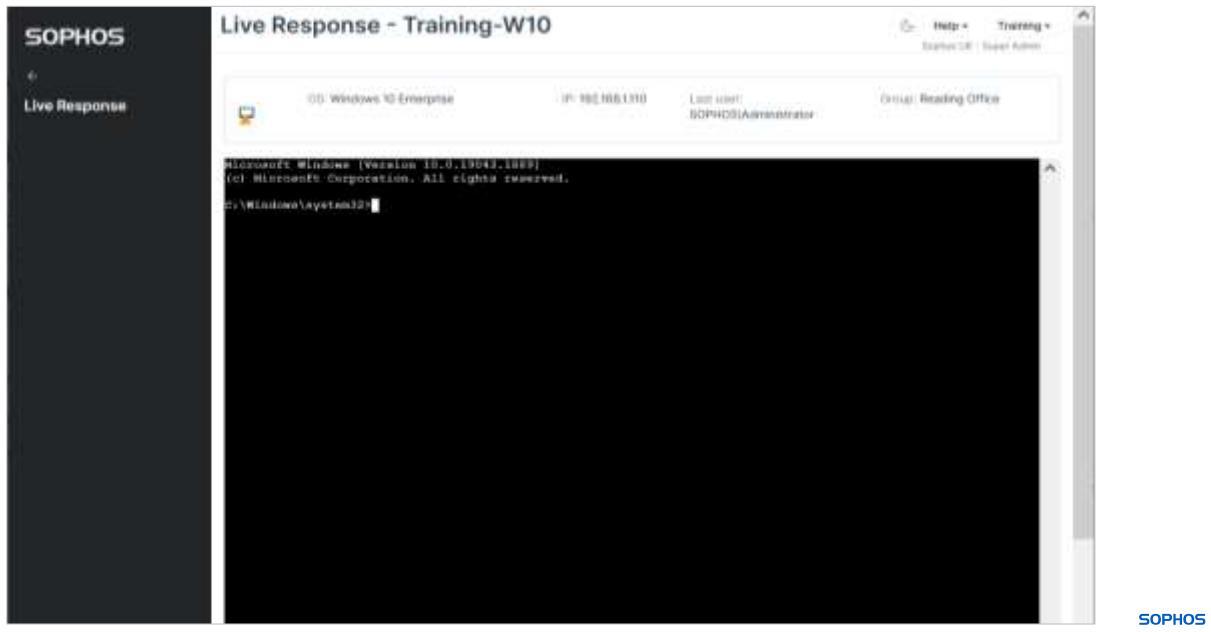
Start a New Session

The screenshot shows the Sophos Central XDR interface. On the left, there's a sidebar with 'Endpoint Protection' selected. Under 'Computers', several devices are listed: 'Pc-1', 'Pc-2', 'Pc-3', and 'Pc-4'. In the center, a modal window titled 'Live Response - Training-W10' is open, prompting the user to 'Start new session'. It asks for a purpose (e.g., 'Describe the purpose of your session') and has a text input field with placeholder text 'Review test machine'. A note at the bottom states: 'Note: Commands run in Live Response sessions are recorded for auditing purposes.' At the bottom of the modal are 'Close' and 'Start' buttons. To the right of the modal, the 'Agent Summary' section is visible, showing a table of assigned products. The table includes columns for 'Product', 'Status', and 'Version'. The products listed are 'Core Agent' (Status: Running Successfully, Version: 10.0.11.0), 'Sophos Endpoint X' (Status: Running, Version: 10.0.11.0), 'Sophos Firewall' (Status: Running, Version: 10.0.11.0), 'Network Encryption' (Status: Not Assigned), and 'SOCX' (Status: Running, Version: 10.0.11.0). The 'SOPHOS' logo is in the bottom right corner.

Click **Live Response** to start a terminal session on the selected device. Enter the session purpose which has a minimum of 10 characters. The description should directly relate to what you plan to do on the device.

Click **Start** to start the session. You will need to ensure that pop-ups for Sophos Central are allowed in your Internet browser.

Run Commands



The Live Response window will be opened, and the connection status will display when the client has been connected to.

Once the connection has been established you can run the commands that are required.

End the Session



Once you have completed the remote session click **End Session**.

This will terminate the running session to the device.

Audit Logs

The screenshot shows the Sophos Central XDR interface. On the left, there's a sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, and Log & Reports (which is currently selected). Below that is a section for 'MY PRODUCTS' listing Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, and Email Security.

The main content area has a title 'Logs & Reports' with a subtitle 'View logs and reports to help analyze and improve your security'. It includes a 'Show filters' dropdown and four filter categories: 'Template Name', 'Legacy?', 'Source', and 'Created'.

Under 'Logs', there are two main sections:

- General Logs**: Contains a 'Events' section (describing security events) and an 'Audit Logs' section (described as a record of all activities and changes made to the system). The 'Audit Logs' section is highlighted with an orange box and a green arrow pointing up to it from the bottom.
- Endpoint & Server Protection Logs**: Contains a 'Data Loss Prevention' section (describing activity triggered by DLP rules) and a 'Live Response session audit' section (described as showing activity in each Live Response session). The 'Live Response session audit' section is highlighted with an orange box and a green arrow pointing right to it from the bottom.

At the bottom right of the interface is the 'SOPHOS' logo.

An audit log is created for all Live Response sessions that are started and ended. This log can be found in **Logs & Reports > Audit Logs**.

A **Live Response session audit** is also available. This session audit displays the date and time of each session along with the device name and IP address.

Session Log



A screenshot of a Windows Notepad window titled "5550411b-07d2-48bd-9679-bc09w660403d_e5a5b028-adab-41bd-83e2-b8fa205fcf7_2022-09-03T11_16_41.2372_browser.txt - Notepad". The window contains the following text:

```
{"version": 2, "width": 120, "height": 40, "timestamp": 1662203801, "env": {"SHELL": "/bin/bash", "TERM": "xterm-256color"}},  
8.23609998855591 cd \users  
78.40499997139 dir  
74.15499997139 cd he[BACKSPACE][BACKSPACE]training  
100.699900012016
```

The Notepad window has standard Windows-style controls at the top and status bar at the bottom.

SOPHOS

The session log can be downloaded and shows the commands that were issued during the session.

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

True or False: Live Response is enabled by default for all administrators with the Super Admin role.

True

False

SOPHOS



Question 2 of 2

How can you review the commands that have been performed during a live response session?

[View the Audit Log](#)

[View the Live Response session audit](#)

[Download and view the session log](#)

[Save the session whilst using Live Response](#)

SOPHOS

Chapter Review

Live Response is a **direct command line interface** that provides a **remote terminal session**.

Live Response requires an **administrator** to have a **Super Admin role**.

Live Response must be **enabled** in **global settings**.

SOPHOS

Here are the three main things you learned in this chapter.

Live Response is a direct command line interface that provides a remote terminal session.

Live Response requires an administrator to have a Super Admin role.

Live Response must be enabled in global settings.



How To Find Help From Sophos

Sophos Central Endpoint and Server Protection

Version: 4.0v1



[Additional Information]

Sophos Central Endpoint and Server Protection

CE5005: How To Find Help From Sophos

December 2022

Version: 4.0v1

© 2022 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.

Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.

While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.

Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

How to Find Help from Sophos

In this chapter you will learn how to find help with your Sophos products and how to keep up to date with the latest news and alerts from Sophos.

RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ There is **no recommended knowledge or experience** prior to completing this chapter

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how to find help with your Sophos products, and how to keep up to date with the latest news and alerts from Sophos.



Additional information in
the notes

How to Find Help

sophos.com/support

The screenshot shows the Sophos Support website with a blue header. The header includes the Sophos logo, navigation links for Services & Products, Solutions, Partners, Support, and a search bar labeled "Search Support". A red box highlights the "Go to Support Portal" link in the Support menu. Below the header, the main page features the text "Sophos Support" and a search bar. At the bottom, there are links for "Join the Community" and "Twitter Support", along with the Sophos logo.

Should you need support, navigate to **sophos.com/support** to access documentation, downloads, training, and support packages. Clicking **Go to Support Portal** will re-direct you to the Support Portal.

[Additional Information]

<https://www.sophos.com/support>

How to Find Help

The screenshot shows the Sophos Support Portal's overview page. At the top, there's a blue header bar with the word "Support" on the left and navigation links for "Overview", "Support Packages", "Downloads", "Documentation", "Training", and "Go to Support Portal" on the right. Below the header are six cards arranged in a 2x3 grid, each with an icon and a title. Each card has a small blue circular arrow icon in the bottom right corner.

Icon	Title	Description
	Read Documentation	Product Setup and Configuration
	Knowledge Base	Solutions to Known Issues
	Techvids	Product Support Videos
	Sophos Central Status	Check Central Downtime & Outages
	Contact Us	Support Cases & Live Chat
	Rapid Response	For Malware and Ransomware

SOPHOS

The overview page provides quick access to the Support Portal, documentation, technical videos and to chat with our support agents or to view Sophos Central status and the latest malware information. There are several ways to find information and support for Sophos products.

Documentation



Additional information in
the notes

[sophos.com/support/documentation](https://www.sophos.com/support/documentation)

The screenshot shows the Sophos Support Documentation page. At the top, there's a navigation bar with links for PRODUCTS, SOLUTIONS, PARTNERS, and COMPANY. Below the navigation is a search bar and a login link. The main content area has tabs for DOCUMENTATION and VIDEO, with DOCUMENTATION selected. On the left, there are two dropdown menus: 'Product' (listing Sophos Web, SafeGuard, Enterprise, Firewall, and Central Admin) and 'Version' (listing 9.4, 9.208, 9.207, 9.206, and 9.205). The central part of the page displays a list of articles. One article is highlighted with a blue box: 'Support Certification Program (SCP)' by Technical Team - Sophos Support, published on 11/09/10. A call-to-action button 'Click Here To Register' is present. On the right, there's a sidebar titled 'For Critical Cases:' with instructions for opening support cases and a 'LOG IN' button.

Documentation, including product user guides, release notes, pocket guides, and other useful information.

[Additional Information]

<https://www.sophos.com/support/documentation>

Knowledge Base



Additional information in
the notes

support.sophos.com

SOPHOS

PRODUCTS SOLUTIONS PARTNERS COMPANY



LOGIN



Results 1-10 of 6,104 in 0.27 seconds

RELEVANCE DATE UPDATED

RECOMMENDED

② Sophos Central: How to Turn On
Remote Assistance

Current Support Status:

All systems normal

Last update to status: 06 August, 2019, 11 minutes ago (Automatic)

Preferred Language:

English (US)

Click Here To Register

To open a new support case, please log into the Support Portal using your SophosID. If you do not have a SophosID, click on 'Click Here To Register'.

RECOMMENDED

② Sophos Endpoint: Disable Tamper
Protection

You cannot disable Tamper Protection if you need to make a change to the local Sophos configuration or uninstall an existing Sophos product. This article describes the steps to disable Tamper Protection from various Sophos products.

For Critical Cases:

You receive a phone number when you submit an issue ticket. Once you have this number, call us for immediate assistance. Select your region below to view the contact number to call.

Select your region:



SOPHOS

The Sophos Knowledgebase, for technical documents on specific configurations and issues.

[Additional Information]

<https://support.sophos.com>

Sophos Community



Additional information in
the notes

community.sophos.com

Using the Sophos community you can reach our dedicated staff for help, as well as participating in discussions, and receiving assistance. This is a forum that allows you to raise questions, share knowledge, and discuss your experiences with our products.

[Additional Information]

<https://community.sophos.com>



sophos.com/labs

Latest Research

HashCorp

Sophos Named 2022 Emerging Partner of the Year

January 2022

Sophos wins HashiCorp Emerging Partner of the Year 2022



January 2022

Remove All The Callbacks – BlackByte Ransomware Disables EDR...



January 2022

Two Exchange Server vulns veer dangerously close to ProxyShe...

See More

SOPHOS

SophosLabs provides access to an inside look into our reports, real-time data, and our threat reports.

[Additional Information]

<https://sophos.com/labs>



Additional information in
the notes

Threat Information

<https://sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx>

The screenshot shows the Sophos Threat Center page for 'Viruses and Spyware'. At the top, there's a navigation bar with links for 'Products', 'Solutions', 'Partners', and 'Support'. Below the header, the main content area has a title 'Viruses and Spyware' and a sub-section 'Find SophosLabs data about viruses, spyware, suspicious behavior and files, adware, PUA, and controlled applications and devices.' A sidebar on the left contains a search bar and a list of 'Recent threats and analysis' with various threat types like 'Top Threats', 'Top Unresolved', 'Top Phishing', etc. On the right, there's a 'Download a free Virus Removal Tool' button and a 'Security Solutions' section listing products like Endpoint Protection, Network Protection, Server Protection, Mobile Security, and Office Security.

SophosLabs keeps a library of all known threats. You can search for a threat and view important information such as a threats characteristics, or how it spreads. The threat library also includes suggested instructions on how to remove the threat.

[Additional Information]

<https://sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx>

Sophos TechVids

 Additional information in the notes

techvids.sophos.com

 Sophos Community | Documentation | SophosZone

Welcome to Sophos TechVids!

**SOPHOS
TECHVIDS**

techvids.sophos.com

Browse Videos by Categories



Antivirus
Intelligent



Endpoint
(ED) Firewall



Sophos
Central



Sophos
XG Series



Sophos
Intercept X

SOPHOS

Sophos provides a series of technical videos that cover configuration tasks, self-help, remediation, and how-to videos for common issues.

[Additional Information]

<https://techvids.sophos.com>



Additional information in
the notes

Sophos Support

support.sophos.com

Create a **Customer Care** case for:

- Access and support portal issues
- Licensing and ordering
- Updating contact information
- MFA resets

Create a **Technical Support** case for:

- Issues with a Sophos product that you are unable to resolve
- Advanced hardware replacements for appliances
- Software downloads or updating issues

For critical cases, create a technical support case and then call Sophos Support quoting your case number

SOPHOS

Support cases are opened through the support portal at sophos.com/support. Login with your Sophos ID, if you do not have a Sophos ID, you can create one. In the support portal, you can create a customer care case for issues such as:

- Access and support portal issues
- Licensing and ordering
- Updating contact information
- Multifactor authentication resets

Sophos Technical Support provides comprehensive support through highly trained technical support representatives, create a technical support case for:

- Issues with a Sophos product that you are unable to resolve
- Advanced hardware replacements for appliances
- Software downloads or updating issues

For critical cases, we recommend that you create a technical support case first. Once you have received the automated case number, follow-up the case with a call to the technical support team.

[Additional Information]

How to use the Sophos Support Portal to raise a support case:

<https://techvids.sophos.com/watch/yBi5NcvMQTNWVyunmm4u1>

Sophos Support

-  Include any errors and symptoms
-  Include the steps to reproduce the issue
-  Include all troubleshooting steps completed
-  Include all logs and additional information gathered

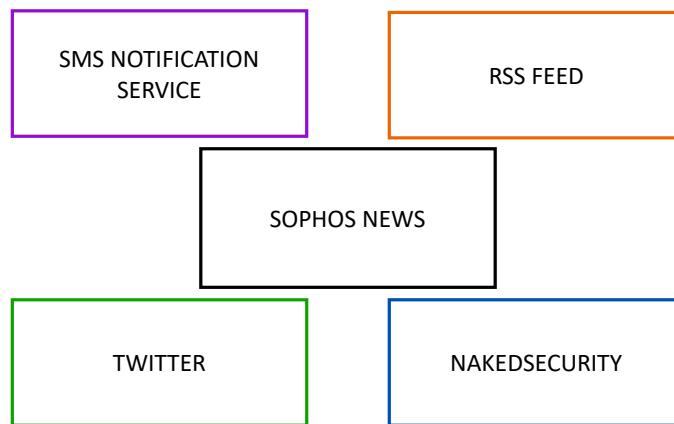
SOPHOS

When raising a support case it is important to be specific about the issue and provide all of the information you have collected. This enables our support team to assist you as quickly as possible. When raising a support case, you should include any errors that are displayed along with details of all the symptoms experienced. If the issue can be reproduced, please provide detailed steps on how to reproduce the issue and any troubleshooting steps you have taken when trying to resolve the issue. If you have collected log files or run any commands during your troubleshooting, please include all of this information.



Additional information in
the notes

Sophos News and Alerts



SOPHOS

We want to make sure you are aware of everything we are doing with our products, from tips to updates and improvements. You can keep up to date with the latest alerts and news by visiting our blog sites for our Sophos community, Sophos News and Sophos Naked Security.

You can also subscribe to our Sophos Central status page for email and SMS alerts, follow Sophos on Twitter, and subscribe to our RSS feed. If a high profile incident occurs, we publish advisory banners to our support and community pages linking to applicable documentation, knowledgebase articles, and additional information.

[Additional Information]

Further information about how to contact your support team, get alerted and be informed can be found in knowledge base article **KB-000038559**. <https://support.sophos.com/support/s/article/KB-000038559>

Sophos News



Additional information in
the notes

news.sophos.com

The screenshot shows the Sophos News website with a blue header bar. The header includes the 'SOPHOS NEWS' logo, a search bar, and navigation links for 'Products & Services', 'Security Updates', 'Press Releases', 'About Sophos', 'Security News', and 'Report A Bug'. Below the header, there's a section titled 'Recent articles' featuring a large image of a filing cabinet. To the right of the image is a news article thumbnail with the title 'Are threat actors turning to archives and disk images as macro usage...'. Further down the page, there are two more news thumbnails: one showing wrapped gifts and another showing a landscape with a path.

Sophos News publishes the latest news about Sophos, our products, and the latest information for reporters who want to write about Sophos.

[Additional Information]

<https://news.sophos.com>



Additional information in
the notes

SMS Notification Service

sms.sophos.com

The screenshot shows the Sophos SMS Notification Service interface. At the top left is the Sophos logo. On the right, there's a button labeled "Subscribe to Sophos Notifications". Below the header is a search bar with the placeholder "All systems names..." and a note: "Search results are offered for 9 Web, 102 Cloud, 200 Devices, and 2253 endpoints". The main area features a grid of green circular icons representing service status across different time intervals (00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00) and categories (Cloud, Server, Desktop, Mobile, Network, Endpoint). A legend at the bottom left identifies the icons: green for "All audience service", blue for "Information", yellow for "Performance issue", red for "Service disruption", and light blue for "Scheduled maintenance". The Sophos logo is also present in the bottom right corner.

The Sophos SMS Notification Service is a free of charge service that provides proactive SMS alerting for Sophos products and services. You are immediately prompted in the event an issue arises, so you will know exactly what is happening, what the impact is, and how to fix it.

You can sign up for the service and select the products you would like to receive alerts for. Once configured, you will receive instant notifications on technical issues or product updates. The SMS message will contain the product name and a link to a knowledgebase article on our support page where you can find more details.

[Additional Information]

Sign up for SMS Alerts: <https://sms.sophos.com>

FAQ: <https://sophos.com/medialibrary/pdfs/support/sophos-sms-faq.pdf>



Additional information in
the notes

Really Simply Syndication (RSS) Feeds

sophos.com/company/rss-feeds

SOPHOS

Products

Solutions

Partners

Support

Business Press Events Careers Contact Network Security News

RSS Feeds

Get our latest updates straight to your computer.

We send the following news, latest virus alerts, reports of the most prevalent viruses and trojans, and product advisories straight to your computer:

What are Info feeds?

An Info feed is a regularly updated summary of web content, with links to full versions of that content. By adding RSS or Atom feeds into a feed reader, you will receive summaries of our latest news, product advisories or virus and threat alerts.

Why should I use Info feeds?

You don't have to spend time searching for the content you want and we keep you informed so you can act on valuable information.

How do I use Sophos Info feeds?

- You will need a feed reader to display and subscribe to the feeds. There are readers available on the market; some are free; some are application specific.
- Drag the RSS or Atom feed for the information feed you want into your feed reader. Or you can click on the RSS or Atom feed and copy the feed URL into your feed reader.

Can I add these feeds to my website?

You can add RSS to your own website for free and very simply via the RSS feed. You can make it available after providing a few details, such as the URL of the feed you want to add.

RSS Feeds

- [Latest News](#)
- [Latest Security](#)
- [Latest Virus Alerts](#)
- [Latest Malicious Behavior and Threats](#)
- [Latest Virus Alerts](#)
- [Latest Controlled Infection](#)
- [Recent Products](#)
- [Latest Technical Notes](#)
- [Old Technical Notes](#)

SOPHOS

Really Simple Syndication (RSS) is a format for delivering regularly changing web content. We syndicate content such as our latest news, product advisories and virus alerts as RSS feeds that you can load into your news reader.

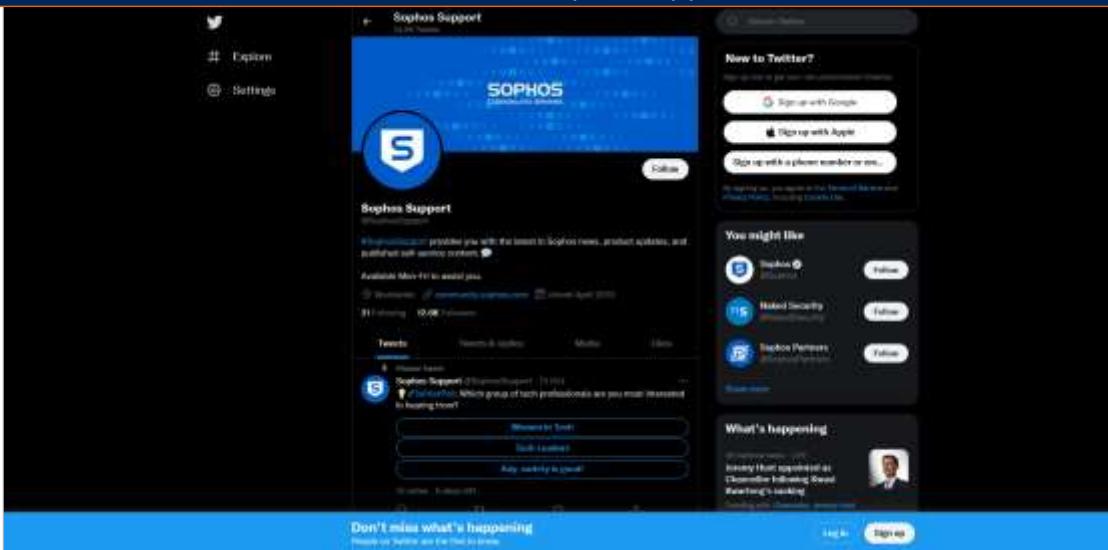
[Additional Information]

<https://sophos.com/company/rss-feeds>

Twitter

 Additional information in the notes

twitter.com/sophossupport



SOPHOS

At Sophos, we use Twitter to help educate and connect with partners, customers, and interested prospects. When we send out alerts via social media, it allows channel followers and Twitter users searching for #sophos to find out the latest information. Follow Sophos to hear about community solutions, news, articles, the latest product releases, and hot issues.

[Additional Information]

<https://twitter.com/sophossupport>



Additional information in
the notes

NakedSecurity

nakedsecurity.sophos.com

The screenshot shows the homepage of nakedsecurity.sophos.com. At the top, there's a navigation bar with links for 'HOME', 'TOP STORIES', 'SEARCH', and 'CONTACT'. Below the header, a large banner features a classical statue holding a shield with the 'naked security PODCAST' logo. To the right of the banner, a news article is displayed with the headline 'S3 Ep104: Should hospital ransomware attackers be locked up for life? [Audio + Text]'. Below the banner, there are four cards representing different threat types: Microsoft (12 items), Linux (11 items), Apple (10 items), and Android (11 items). The Sophos logo is visible in the bottom right corner.

Naked security is Sophos' award-winning threat newsroom, giving you news, opinions, advice and research on cyber security issues and the latest threats.

[Additional Information]

<https://nakedsecurity.sophos.com>

Knowledge Check

SOPHOS

Take a moment to check your knowledge!



Question 1 of 2

What does the SophosLabs page provide information on?

Access to the Sophos
Community

Knowledgebase articles on
known threats

Documentation on how to
remediate known threats

Real-time data and threat
reports

SOPHOS



Question 2 of 2

Enter the URL address for the Sophos Support website.

SOPHOS

Chapter Review

Help can be found by navigating to sophos.com/support.

Contact Sophos Support via the [Support Portal](#), [live chat](#), and [Twitter](#).

Stay up to date with Sophos news and alerts by joining the [Sophos Community](#), signing up for news alerts using [SMS](#) or [RSS-feeds](#).

SOPHOS

Here are the three main things you learned in this chapter.

Help can be found by navigating to [sophos.com/support](#).

Contact Sophos Support via the Support Portal, live chat, and Twitter.

Stay up to date with Sophos news and alerts by joining the Sophos Community, signing up for news alerts using SMS or RSS-feeds.

