

# Getting Started with Sophos Central Troubleshooting

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE0535: Getting Started with Sophos Central Troubleshooting

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 Troubleshooting

In this chapter you will learn the troubleshooting process that is used for Sophos Central

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Experience of using Sophos Central
- ✓ Knowledge of Sophos Central protection features and requirements

DURATION     **4 minutes**

SOPHOS

In this chapter you will learn the troubleshooting process that is used for Sophos Central.

# Privileges Required



Ability to disable tamper protection



Administrator rights to the device



Administrator rights to the network and/or Active Directory

SOPHOS

To perform troubleshooting for devices protected by the Sophos Endpoint Agent, you will need sufficient privileges on protected devices, and in some cases the network.

A few examples are:

- The ability to disable Sophos tamper protection
- Administrator rights to the device
- Administrator rights for the network and/or the Active Directory

# Overview of the Troubleshooting Process



## Define

Define the issue



## Analyze

Root cause analysis



## Verify

Verification testing

SOPHOS

The troubleshooting process used throughout this course is split into three phases; Define the issue, perform root cause analysis, and verification testing.

You will see the troubleshooting process steps indicated for each scenario discussed throughout this course using the 1, 2 and 3 progress icons shown here.

Let's look at these three phases in more detail.

## Define the Issue

1



### Define

Define the issue

Identify the **specific symptoms** of the problem

Identify any **error messages** related to the problem

Confirm the steps required to **reproduce** the error or symptom

SOPHOS

The first step of troubleshooting any scenario with Sophos Central is to define the issue. Identify the specific symptoms of the issue and any error messages involved.

You should also confirm the steps required to replicate the issue or re-create the error.

# Root Cause Analysis



## Analyze

Root cause analysis

Search the Sophos **Knowledgebase** and **Community** for the symptoms or error identified

Check the **configuration** of the affected function and the **log files** for additional information

Use **troubleshooting tools** for further investigation as required

SOPHOS

The root cause analysis phase is when you identify what is causing the issue or error. This can involve a few different steps, for example:

- Searching the Sophos knowledge base and community for the error or symptom identified. If the error is known, the cause and solution may already be documented
- Checking the configuration of the affected function and the log files to gather additional information. You may find a configuration error that when changed will resolve the issue, or information in the logs that clearly indicates the cause of the error or issue
- Making use of troubleshooting tools to further investigate the error or issue

If you are unable to identify the root cause of an issue or are unable to resolve an issue, we recommend that you contact Sophos Support with a detailed description of the problem, including replication steps and any errors you encounter, along with any root cause analysis steps you have taken.

## Verification Testing

3

3

### Verify

Verification testing

Complete the steps to **resolve** the issue

Follow the steps to **reproduce** the issue to confirm it is now resolved

SOPHOS

Once you have determined the probable root cause, you can then perform verification testing.

This means completing the resolution steps and confirming that the issue has been resolved, or that the error is no longer showing.



Additional information in  
the notes

# Product Lifecycle

## Product Lifecycle

Sophos maintains several retirement calendars for products and hardware.



Sophos Endpoint and Server Protection: Retirement calendar for supported platforms and operating systems:

[Retirement Calendars](#)

Sophos Product End Of Sale / End Of Life - Frequently Asked Questions:

[Frequently Asked Questions](#)

SOPHOS

It is important to ensure that the software you are running in your estate has not been retired. Sophos maintains several retirement calendars for products and hardware. Retirement calendars primarily list end of sale and end of life dates and can also include migration paths and successor product recommendations amongst other important information.

If you encounter an issue with a Sophos product, please ensure the version you're running has not been retired.

### [Additional Information]

Retirement calendar for supported platforms and operating systems **KB-000034756**.

<https://support.sophos.com/support/s/article/KB-000034756>

Sophos Product End Of Sale / End Of Life - Frequently Asked Questions. <https://www.sophos.com/en-us/medialibrary/PDFs/Support/sophos-product-lifecycle-faq.pdf>

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!

# Question 1 of 2



Match the stage of the troubleshooting process to its description.

Define

DROP

Complete the resolution steps

Analyze

DROP

Identify the specific symptoms of the issue

Verify

DROP

Identify what is causing the issue or error

SOPHOS



## Question 2 of 2

In which phase of the troubleshooting do you confirm the steps required to reproduce the error or symptom?

Define the issue

Root cause analysis

Verification testing

SOPHOS

# Chapter Review

Troubleshooting requires **sufficient privileges** to the protected devices and in some cases the network

The troubleshooting process has **three phases**; **Define** the issue, **root cause analysis** and **verification** testing

SOPHOS

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

Troubleshooting requires sufficient privileges to the protected devices and in some cases the network.

The troubleshooting process has three phases; Define the issue, root cause analysis and verification testing.



# An Introduction to Sophos Troubleshooting Tools

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE0540: An Introduction to Sophos Troubleshooting Tools

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 Troubleshooting Tools

In this chapter you will learn the tools that are provided with the Sophos Endpoint Agent to assist with troubleshooting

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

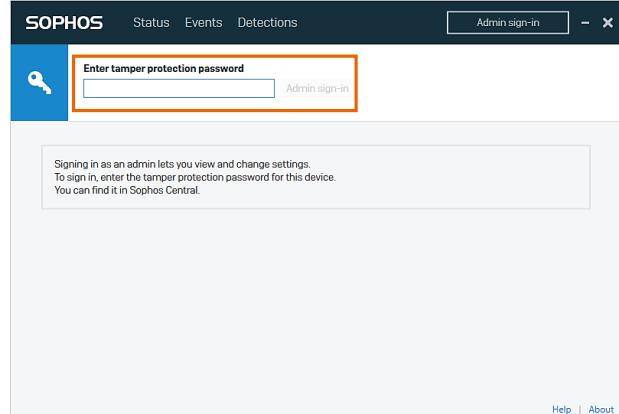
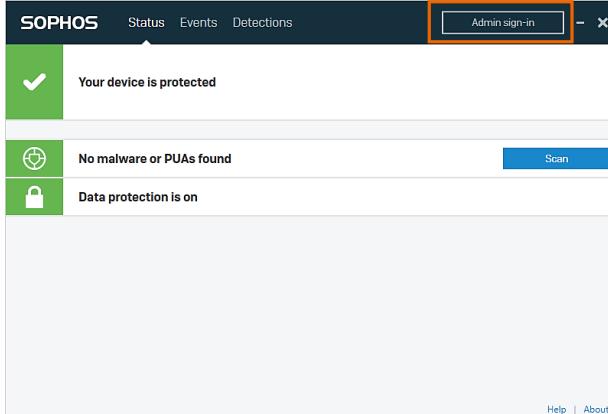
- ✓ Experience of using Sophos Central Admin
- ✓ Knowledge of Sophos Central protection features

DURATION      **10 minutes**

SOPHOS

In this chapter you will learn the tools that are provided with the Sophos Endpoint Agent to assist with troubleshooting.

# Sophos Endpoint Agent



SOPHOS

The Sophos Endpoint Agent provides the starting point for troubleshooting.

By default, tamper protection is enabled for protected devices, preventing users from making any changes to policies. An administrator can sign into the Sophos Endpoint Agent allowing them management of the device.

# Admin Sign-In

The screenshot shows the Sophos Settings interface. On the left, under 'Tamper Protection', it says 'On' and has a link to 'Disable Tamper Protection'. Below that is 'Tamper Protection Password Details' with a current password '840372106082' and a 'Generate New Password' button. On the right, there's a section titled 'Override Sophos Central Policy for up to 4 hours to troubleshoot' with a checked checkbox. Other settings include 'Enable Deep Learning' (on), 'Real Time Scanning' (Files on, Internet off), 'Controls on Users' (Peripheral Control, Web Control, Tamper Protection on), 'Runtime Protection' (Ransomware Detection, Exploit Mitigation, Malicious Behavior Detection all on), and 'Safe Browsing', 'Network Threat Protection', 'AMSI Protection' (all off). The bottom right has 'Help | About' and the Sophos logo.

The **Admin Sign-In** requires entry of the tamper protection password, which can be viewed on the **Summary** page for a device in Sophos Central. Once this password has been entered, the **Settings** page allows an administrator to override the policies for up to four hours. This includes the option to disable **Tamper Protection**.

# About

The screenshot shows the Sophos About page with the following content:

- Update Status**: Shows a green checkmark and the message "Last update: 22 June 2022 10:50". A blue button labeled "Update Now" is highlighted with a red box.
- Products**: Lists product versions:
  - Core Agent 2.20.13
  - Endpoint Advanced 10.8.114
  - Sophos Intercept X 2021.3.1.12
  - Device Encryption 2022.1.0.41
- Troubleshooting**: Includes a blue button labeled "Open Endpoint Self Help Tool" highlighted with a red box, and links to "Community forum" and "Legal Information".
- Navigation**: Buttons for "Help" and "About" at the bottom right, with "About" highlighted with a red box.

The **About** page provides two very useful options for troubleshooting. The **Update Now** button performs an immediate update.

This page also provides a link to the Sophos Endpoint Self Help tool where you can view additional tools and information as well as the ability to launch the Sophos Diagnostic Utility.



Additional information in  
the notes

## Endpoint Self Help – Health Status

SOPHOS

The Sophos Endpoint Self Help tool (ESH) reports on the status of each component of the Sophos Endpoint Agent. The Endpoint Self Help tool can also be launched from the start menu of a device.

### [Additional Information]

More information about the Endpoint Self Help Tool can be found here: **KB-000036448**.

<https://support.sophos.com/support/s/article/KB-000036448>

# Endpoint Self Help

The screenshot shows two side-by-side windows of the Sophos Endpoint Self Help tool. Both windows have a dark header bar with 'SOPHOS' and 'Endpoint Self Help' on the left, and 'Status' and 'Tools' on the right. A red box highlights the 'Management Communication' item under 'Health State' in the left window, and another red box highlights the 'Policy' item under 'Last Time Policy Received' in the right window.

**Left Window (Health State):**

- Health State
- System
- Installed Components
- Services
- Management Communication** (highlighted)
- Update
- Device Encryption
- Policy

Management Communication  
Last Communication Succeeded at 11:18:16 Jun 22, 2022 (UTC+01:00)

Connection Details  
Server https://mcn2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep  
Server Address 52.19.70.38  
Proxy No proxy used

Remediation  
For help with issues reported on this page, read [Knowledge Base Article KB-000036450](#)

Did this help you? Yes

Launch SDU Refresh

**Right Window (Last Time Policy Received):**

- Health State
- System
- Installed Components
- Services
- Management Communication
- Update
- Device Encryption
- Policy** (highlighted)

Last Time Policy Received
AMSI Not since 10:41:54 Jun 22, 2022 (UTC+01:00)
Device Encryption 10:44:11 Jun 22, 2022 (UTC+01:00)
Heartbeat 10:46:13 Jun 22, 2022 (UTC+01:00)
HitmanPro.Alert 10:46:14 Jun 22, 2022 (UTC+01:00)
LiveQuery 10:44:11 Jun 22, 2022 (UTC+01:00)
Management Communication System 10:41:57 Jun 22, 2022 (UTC+01:00)
Network Threat Protection 10:46:14 Jun 22, 2022 (UTC+01:00)
SAV 10:44:12 Jun 22, 2022 (UTC+01:00)
Sophos AutoUpdate Not since 10:41:54 Jun 22, 2022 (UTC+01:00)
Sophos Core 10:44:10 Jun 22, 2022 (UTC+01:00)
Sophos Core Customer 10:44:10 Jun 22, 2022 (UTC+01:00)
Sophos Endpoint Firewall 10:44:11 Jun 22, 2022 (UTC+01:00)
Sophos User Interface Not since 10:41:54 Jun 22, 2022 (UTC+01:00)

Launch SDU Refresh

The Sophos Endpoint Self Help tool identifies if any of the components have issues and provides links to troubleshooting articles containing error scenarios and instructions for resolution.

It also displays a list of policy types and the time each policy was last received by the endpoint.

SOPHOS

# Endpoint Self Help – Installed Components

The screenshot shows the Sophos Endpoint Self Help interface. On the left is a sidebar with the following items:

- Health State
- System
- Installed Components** (highlighted with an orange border)
- Services
- Management Communication
- Update
- Device Encryption
- Policy

At the bottom of the sidebar are two buttons: "Launch SDU" and "Refresh". At the top right of the sidebar are "Status" and "Tools" icons.

The main area is titled "Installed Components" and lists the following software components:

Component	Status	Version
Sophos AMSI Protection	Installed	V. 1.8.59
Sophos AutoUpdate	Installed	V. 6.12.86
Sophos Clean	Installed	V. 3.9.14.1
Sophos Data Protection Agent	Installed	V. 2.3.231.0
Sophos Diagnostic Utility	Installed	V. 6.11.234
Sophos Endpoint Agent	Installed	V. 2.20.13
Sophos Endpoint Defense	Installed	V. 3.0.1.947
Sophos Endpoint Firewall	Installed	V. 2.0.20.20
Sophos Endpoint UI	Installed	V. 2.4.230.0
Sophos File Scanner	Installed	

SOPHOS

The **Installed Components** listed may vary depending on the license and the software components chosen for installation.

# Endpoint Self Help - Services

Service	Status
HitmanPro.Alert service	Running
Sophos AutoUpdate	Running
Sophos Device Encryption	Running
Sophos Endpoint Defense	Running
Sophos File Scanner	Running
Sophos Health	Running
Sophos Live Query	Running
Sophos MCS Agent	Running
Sophos MCS Client	Running
Sophos Network Threat Protection	Running
Sophos System Protection	Running
Sophos Clean	Stopped
Sophos Safestore	Stopped

SOPHOS

The **Services** tab lists all of the services running on the endpoint that are related to the Sophos Endpoint Agent. The status of each service is listed allowing you to see if there is a service that is stopped or not running.



Additional information in  
the notes

## Endpoint Self Help – Known Issues

The screenshot shows the Sophos Endpoint Self Help interface. The top navigation bar has 'Status' and 'Tools' buttons, with 'Tools' highlighted by an orange box. The main content area is titled 'Known Issues' and displays a message: 'No issues found' with a green checkmark icon, followed by '55 rules completed successfully.' A 'Run' button is located in the top right corner of this section. Below this, there's a 'Remediation' section with a link to 'Knowledge Base Article KB-000040244'. At the bottom right, there's a feedback button asking 'Did this help you?' with a 'Yes' option selected.

SOPHOS

The **Tools** window provides a method to run a set of rules that analyze the health of the Sophos Endpoint Agent.

Select **Run** to detect any issues that are known to Sophos support. If a known issue is detected, you will be provided with a link to a knowledgebase article to rectify the fault.

### [Additional Information]

More information on the rules in place can be found here: **KB-000040244**.

<https://support.sophos.com/support/s/article/KB-000040244>

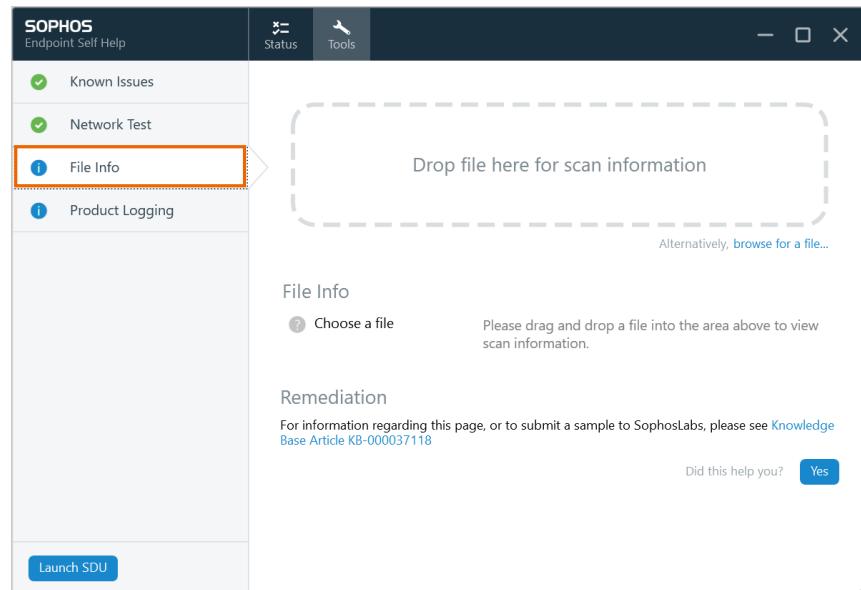
# Endpoint Self Help – Network Test

The screenshot shows the Sophos Endpoint Self Help application window. The left sidebar has four items: Known Issues, Network Test (which is selected and highlighted with an orange border), File Info, and Product Logging. The main content area is titled "Network Test" and contains a "Run" button. Below it, there is a list of issues: "Sophos Extensible List (SXL) lookups can't be done because a message relay is in use.", followed by two expanded items: "Updating" and "Management Communication", each with a green checkmark icon. At the bottom of the main area, there is a "Remediation" section with a link to a Knowledge Base Article (KB-000042966). A "Did this help you?" poll with "Yes" and "No" buttons is also present. A "Launch SDU" button is located at the bottom left of the sidebar.

SOPHOS

The **Network Test** page provides a method to check specific communication channels directly to Sophos and, if configured, to an Update Cache and Message Relay. The tests will provide feedback on areas of failure.

# Endpoint Self Help – File Info



SOPHOS

The **File Info** tab provides a method to analyze portable executable files to display the characteristics used by Sophos to determine if a file is a threat. Using these characteristics, it displays the file reputation and whether it is controlled, malicious, or potentially unwanted. Other file types will display limited information.

# Product Logging

The left screenshot shows the 'Product Logging' page with a prominent orange warning box stating 'Elevated privileges required' and 'Administrator privileges are required to configure product logging.' The right screenshot shows the same page after configuration, with the 'Logging Level' dropdown set to 'Warning'. Both screenshots include a sidebar with links like Known Issues, Network Test, File Info, and Product Logging.

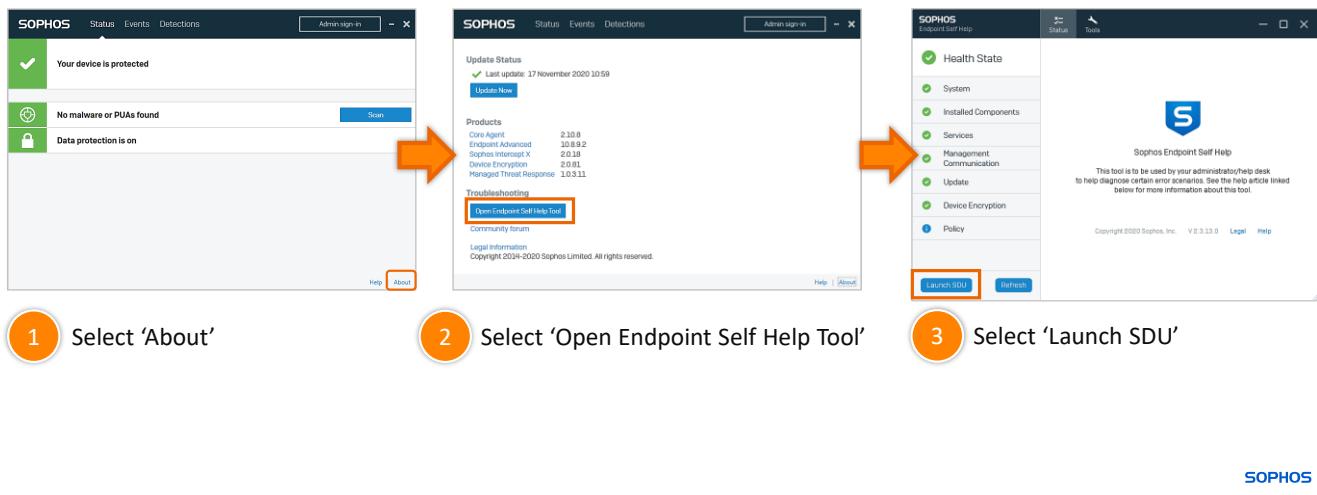
The **Product Logging** page provides an option to configure different log levels on various Sophos components and features.

To configure product logging, user account control elevation is required. This means standard users can easily perform an administrative task by entering valid credentials for a local administrator account.

Product logging may be required when investigating issues and should only be used when requested by Sophos support or when following documented guidance.

# Sophos Diagnostic Utility (SDU)

The Sophos Diagnostic Utility is designed and used by Sophos Technical Support to assist in troubleshooting and diagnosing issues.



The Sophos Diagnostic Utility collects vital system information as well as log files for all Sophos products that are installed on the device. It is available on Windows, macOS, and Linux.

The SDU is a tool designed and used by Sophos technical support to assist in troubleshooting and diagnosing issues. On Windows endpoints the SDU can be run from the Self-Help tool.

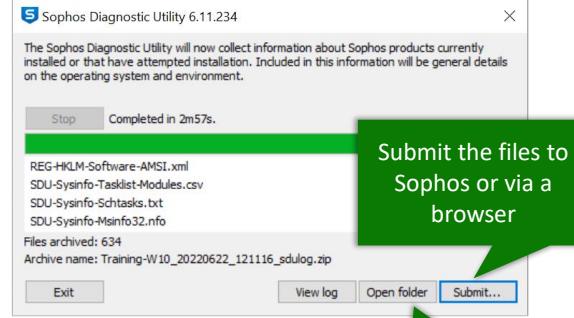
1. From the Sophos Endpoint Agent select **About**
2. Select **Open Endpoint Self Help Tool**
3. Select **Launch SDU**

The Sophos Diagnostic Utility will begin to collect logs and system information from the device.



Additional information in  
the notes

# Sophos Diagnostic Utility - Windows



Sophos Diagnostic Utility (SDU): How to locate and download:

Sophos Diagnostic Utility (SDU): Using the utility and sending files to Sophos Technical Support:

[Sophos Diagnostic Utility](#)

[Sending Files to Sophos](#)

SOPHOS

The SDU exports all relevant logs and configuration information into an archive and allows the administrator to send them to Sophos support.

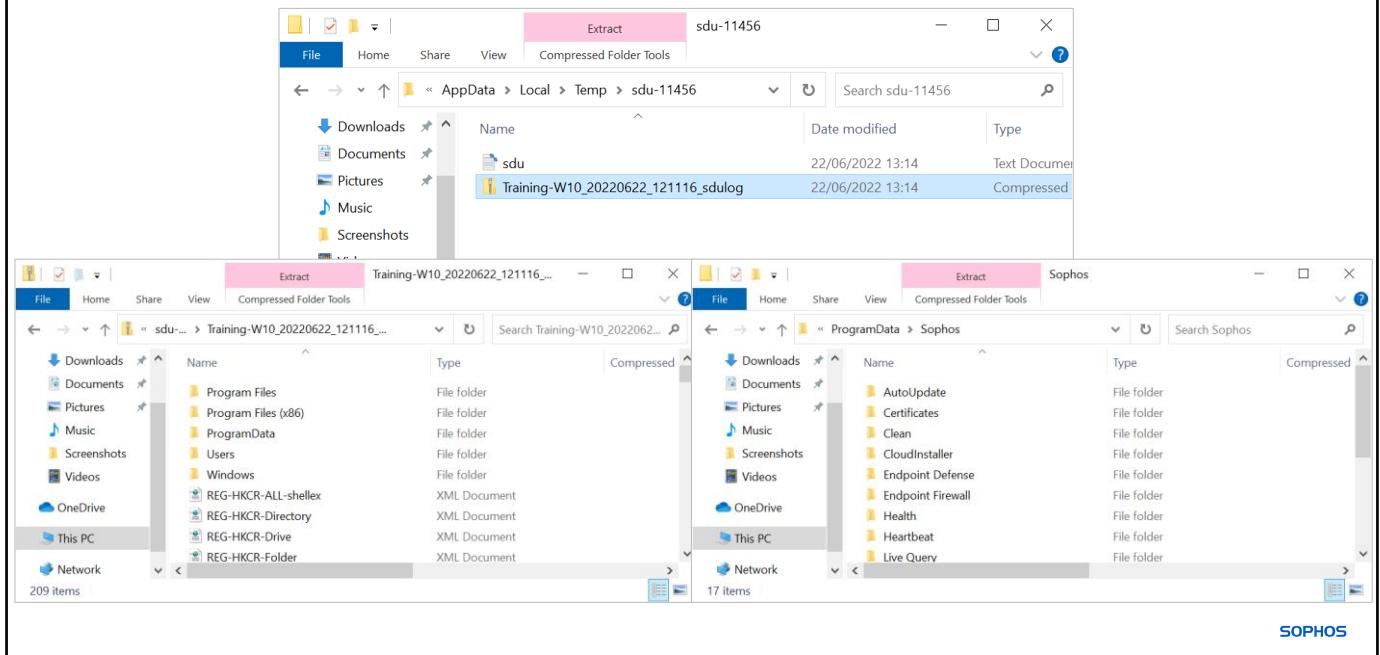
## [Additional Information]

Further information on how to download and run the Sophos Diagnostic Utility can be found here **KB-000033500**. <https://support.sophos.com/support/s/article/KB-000033500>

We also supply information on sending the files to Sophos support here **KB-000033508**.

<https://support.sophos.com/support/s/article/KB-000033508>

# Sophos Diagnostic Utility Output



The SDU creates a zip file in the user's temporary folder. The zip file can also be opened by a Sophos support technician and used to locate log files and other information, for example the contents of the Sophos folder.



Additional information in  
the notes

# Sophos Diagnostic Utility - Windows

You can also trigger the Sophos Diagnostic Utility to run remotely from Sophos Central. Once the utility has finished running it will automatically upload the output to Sophos Support.

The screenshot illustrates the process of triggering the Sophos Diagnostic Utility (SDU) on a remote device (Client5) via Sophos Central:

- 1 HOS**: Shows the main Sophos Central dashboard with the "Devices" menu selected.
- 2 Client5**: Shows the Device page for Client5 (WinClient5). The device name is highlighted with a red box.
- 3 Client5**: Shows the "More actions" dropdown menu for Client5. The "Diagnose" option is highlighted with a red box.
- 4 Diagnose**: A confirmation dialog box asking if you want to run the Sophos Diagnostic Utility. The "Run" button is highlighted with a red box.
- 5 Sophos Diagnostic Utility**: Shows the summary of the SDU run. It includes the status (Running), last run time (6 minutes ago), file name (c59251f-[redacted]-08-32-35.zip), and a progress bar indicating the upload status.

SOPHOS

You can also trigger the SDU remotely from Sophos Central. This process runs the SDU on the protected device, the output file is automatically uploaded to Sophos support, without the need to visit the device itself. To run a remote SDU:

1. Click on the device in Sophos Central to open the Device page
2. Click **More Actions**. This will display several actions you can perform remotely from Sophos Central
3. Click **Diagnose**
4. Click **Run**
5. The **Sophos Diagnostic Utility** section at the bottom of the Summary page shows that the SDU is currently running

## [Additional Information]

Sophos Central stores the command to run the Sophos Diagnostic Utility for up to 14 days. Within this time frame if the device is turned on the command will be run once communication with Sophos Central takes place. If the device is turned off for longer than 14 days, the command to run the Sophos Diagnostic Utility will be deleted.

# Sophos Diagnostic Utility - Windows

The Sophos Diagnostic Utility status section displays the:

**Status** - shows the tool is currently Running on the device.

**Last Run** - shows when the command to run the utility was sent to the device.

**File Name** - shows the file name of the diagnostic log created on the device and uploaded to Sophos. The filename consists of the Sophos computer/server ID followed by the date/time stamp.

## Sophos Diagnostic Utility

Status	Running
Last Run	6 minutes ago
File Name	c5925f1f-[REDACTED]-08-32-35.zip

SOPHOS

The Sophos Diagnostic Utility status section on the **Summary** tab of a device record in Sophos Central displays the status of the utility, when it was last run and the name of the last diagnostic log file that was created and uploaded to Sophos. The filename consists of the Sophos computer or server ID followed by a date and time stamp.

## Sophos Diagnostic Utility - Windows

Once the SDU is completed, the status will change to **Not Running**

Sophos Diagnostic Utility	
Status	Not Running
Last Run	34 minutes ago
File Name	<b>bd62443a-19b9-e43f-1927-7ce59cb2e500_2022-06-22-15-41-48.zip</b>

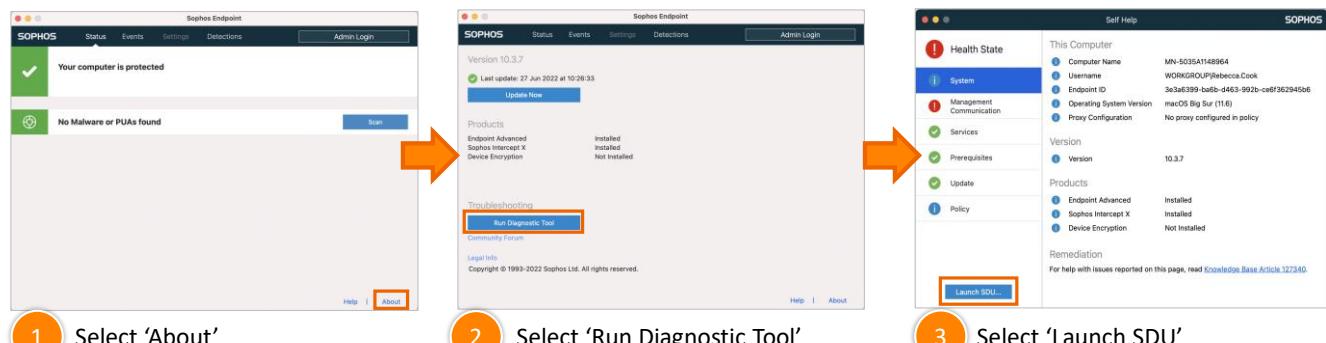
If you open a support ticket with Sophos Support, provide the SDU **File Name** specified at the bottom of the **Summary** page for the device

SOPHOS

On completion the status will change to 'Not Running'. The resulting zip file created as part of this process is uploaded to the sophos.com domain using HTTPS (port 443).

If you are planning to open a support ticket with Sophos, please provide the **File Name** as this will allow technical support to retrieve the file and proceed with an investigation into the reported issue.

# Sophos Diagnostic Utility - MacOS



The SDU can be launched by double-clicking the Sophos Diagnostic Utility application found inside the DMG file

SOPHOS

The Sophos Endpoint Agent on a macOS device includes a diagnostic tool. The SDU can be launched from the diagnostic tool.

Once the SDU has finished, the files are archived and compressed into a file called 'Sophos\_SDU.tgz' and placed on the Desktop.

The SDU can also be launched by double-clicking the Sophos Diagnostic Utility application found inside the DMG file.



Additional information in  
the notes

## SDU for Linux

From a console terminal run the following command

```
/opt/sophos-spl/bin/sophos_diagnose
```

By default the tar.gz file is saved to the directory where the command was run.

To specify the directory add the required file directory to the to the command.

```
/opt/sophos-spl/bin/sophos_diagnose /tmp
```

SOPHOS

To launch an SDU for Linux Servers protected with Sophos Protection for Linux, open a console terminal and run the command shown. This will output a tar.gz file to the current directory where the command was run.

To specify where the diagnostic output file should be created, run the command with the selected directory as the first argument. The tool gathers all logs from the agent, all plugins, and the audit log. Once the SDU has finished, you can locate the archive and send it to Sophos support.

### [Additional Information]

The command to run the SDU is `/opt/sophos-spl/bin/sophos_diagnose`

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 3

What is required to perform an Admin Sign-In on a Sophos Endpoint?

Admin privileges on the device

An administrator command prompt

The tamper protection password

Sophos Central Admin privileges

SOPHOS

## Question 2 of 3

Enter the command required to run the Sophos Diagnostic Utility on a Linux server

\_\_\_\_\_

## Question 3 of 3



Which of the following Endpoint Self Help options displays the characteristics used by Sophos to determine if an executable file is a threat?

Events

File Info

Known Issues

Scan Now

SOPHOS

# Chapter Review

**Admin login** requires entry of the **tamper protection password**, which can be viewed on the Summary page for each endpoint in Sophos Central Admin.

The **Sophos Endpoint Self Help** (ESH) reports on the **status of each component** of the Sophos Endpoint Agent.

The **Sophos Diagnostic Utility (SDU)** exports all relevant endpoint logs and configuration information into an **archive** and allows an administrator to **send them to Sophos support**.

SOPHOS

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

Admin login requires entry of the tamper protection password, which can be viewed on the Summary page for each endpoint in Sophos Central Admin.

The Sophos Endpoint Self Help tool reports on the status of each component of the Sophos Endpoint Agent.

The Sophos Diagnostic Utility exports all relevant endpoint logs and configuration information into an archive and allows an administrator to send them to Sophos support.



# Getting Started with SURF

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE0545: Getting Started with SURF

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 SURF

In this chapter you will learn what the SURF tool is and how it can be used to assist with troubleshooting Sophos Central protected devices.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Understand what Sophos Central is

DURATION      **13 minutes**

SOPHOS

In this chapter you will learn what the SURF tool is and how it can be used to assist with troubleshooting Sophos Central protected devices.

# Sophos Universal Reader and Finder (SURF)

SURF provides an integrated view of all files to aid troubleshooting and resolution of issues

Developed by Sophos support to aid troubleshooting of Sophos products

SURF reads data from a Sophos Diagnostic Utility (SDU) file and creates a local database

Extracts relevant data from the database and displays that data on the SURF dashboard

SOPHOS

The Sophos Universal Reader and Finder, known as SURF, provides an integrated view of all files to aid the troubleshooting and resolution of issues. It is a support tool that has been developed by Sophos Support to aid the support of Sophos products.

The Sophos Diagnostic Utility (SDU) for Sophos Central protected devices, gathers multiple configuration and log files, registry key and process information and much more. These files contain a huge amount of data and can be time consuming to filter through and search.

The SURF tool reads data from an SDU and creates a local database. From the database it extracts the relevant data and displays it on the SURF dashboard. There is a detection engine included in the tool which analyses the log file. The engine can scan logs for known issues and provides links to knowledge base articles if issues are identified. The tool makes use of detection rules which are created by Sophos support and are automatically updated. These rules mean that known issues are identified and known fixes or workarounds are provided.



Additional information in  
the notes

## SURF Requirements

-  The SURF tool
-  Windows 10 or later
-  Only available to Sophos Partners

SOPHOS

The SURF tool is only available to Sophos Partners and can only be used on Windows 10 or later devices.

Please note that you can run an SDU on ANY operating system, however, the SURF tool can only be used on a Windows 10 or later device. You will therefore need to move the gathered SDU log onto a network share, or onto a SURF compatible device to view them.

### [Additional Information]

Download the SURF tool from our Partner Portal: <https://partners.sophos.com/prm/English/c/tech-tools>

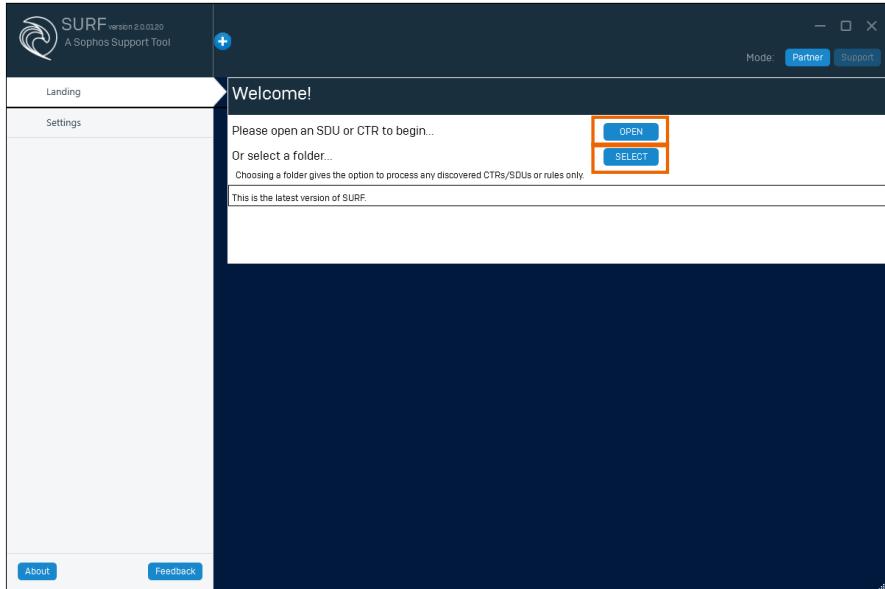
# Download SURF

The screenshot shows the Sophos Partner Portal interface. At the top, there's a blue header bar with the Sophos logo and navigation links like 'ASSET LIBRARY', 'MANAGE SOPHOS CENTRAL', 'GET HELP', and various icons. Below the header, a menu bar includes 'Partner Program', 'Sales', 'Marketing', 'Tech', 'MSP & CSP', and 'Training'. The main content area features a large orange icon of a person holding a gear. To its right, there's a section titled 'SURF – Log Analyzing Tool' with a brief description and three buttons: 'Learn More', 'Download' (which is highlighted with a red box), and 'User Guide'. Below this section, there's another orange icon of a person holding a gear.

To download the SURF tool you must be a Sophos Partner. Log into the Sophos Partner Portal, in the ‘SURF – Log Analyzing Tool’ section, click **Download**.

The SURF tool will be downloaded. Run the installer and once it has finished downloading, follow the prompts to install the tool.

# How SURF Works



SOPHOS

The SURF tool is ready to use. You can select to open an SDU. Once you select **OPEN**, a file explorer window will open allowing you to select the required file.

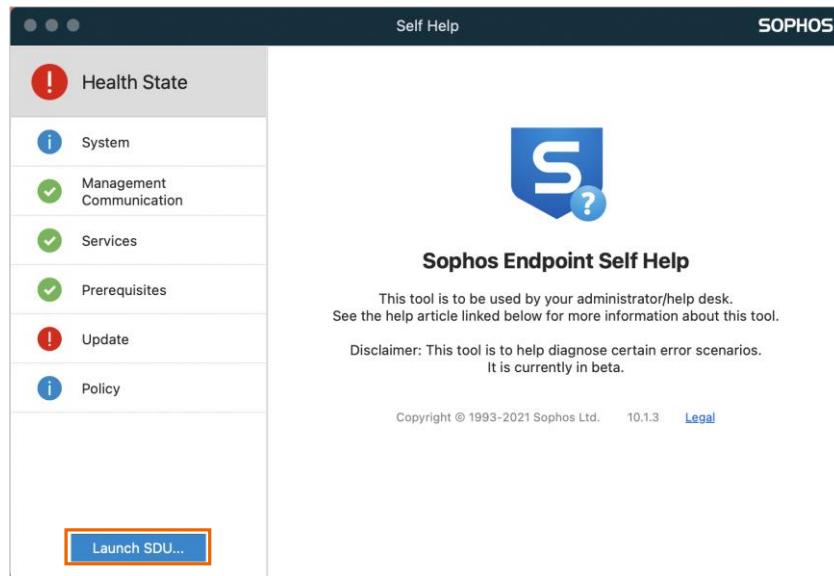
Alternatively, you can select a folder to open. Choosing a folder gives you the option to process any discovered SDU files or rules only. Once you click **SELECT**, choose the file. You can then select to process that file which will look at any rules that are matched in the file.

We will now cover how to generate an SDU file on different operating systems.



Additional information in  
the notes

## Generating an SDU on macOS



To generate an SDU on macOS, open the Sophos Endpoint Agent on the device. Click **About > Run Diagnostic Tool**. Alternatively, you can open the Sophos Endpoint Self Help tool from **Finder > Applications**.

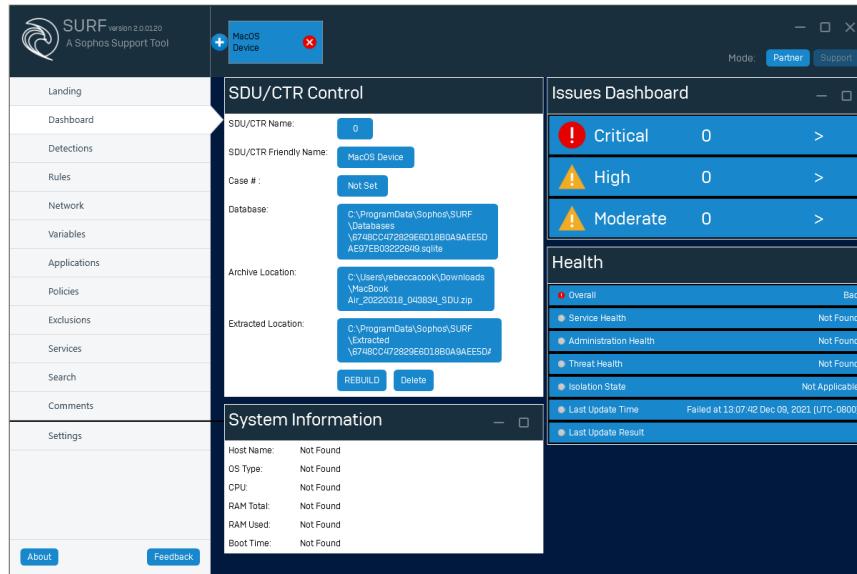
The Endpoint Self Help tool includes the **Launch SDU...** option. Click the button to run the SDU. Click **Run** to start the SDU process. Once it has completed, click **Quit**.

The SDU file created will be saved to the Desktop of the device where it can be submitted to Sophos Support or used with the SURF tool.

### [Additional Information]

For more information on generating SDU logs please see knowledge base article **KB-000033508**.  
<https://support.sophos.com/support/s/article/KB-000033508>

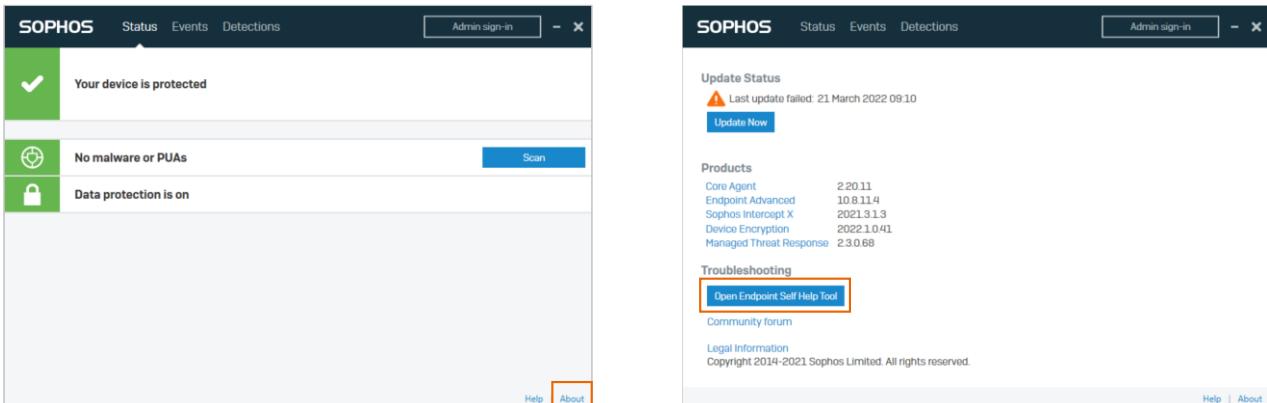
# Loading a MacOS SDU into SURF



SOPHOS

Once you have loaded the macOS SDU into the SURF tool, you will see the dashboard overview and can search the file for specific errors or usernames.

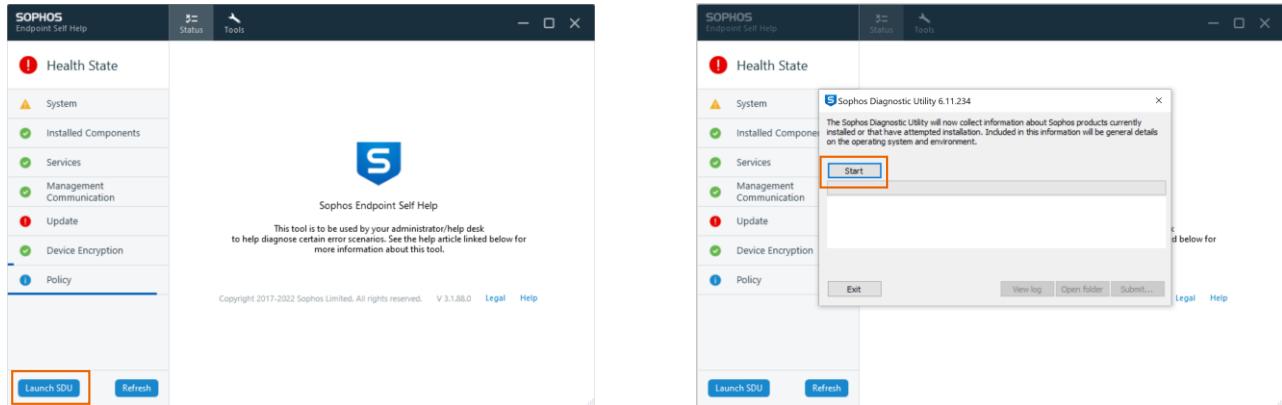
# Generating an SDU on Windows



To run an SDU on a Windows device, open the Sophos Endpoint Agent and click **About**.

Select the option to **Open Endpoint Self Help Tool**.

# Generating an SDU on Windows



SOPHOS

You will see the option at the bottom of the left-hand menu to **Launch SDU**.

Once you have selected this option, click **Start** to start the collection of the log files.



Additional information in  
the notes

# Generating an SDU on Windows

The screenshot shows the SURF tool interface on a Windows system. The main window has a dark theme with blue and white text. On the left, there's a sidebar with various status icons and links like 'Landing', 'Dashboard', 'Detections', etc. The central part of the interface is divided into two main sections: 'SDU/CTR Control' and 'System Information'. The 'SDU/CTR Control' section contains fields for 'SDU/CTR Name' (WINCLIENT1), 'SDU/CTR Friendly Name' (Windows Device), 'Case #' (Not set), 'Database' (C:\ProgramData\Sophos\SURF\Datasatabases\30AFC4A20D0A0A93C8D000CD42836E0D8DE5AC900EE.sqlite), 'Archive Location' (C:\Users\jvivesco\Downloads\WinClient1\_20220321\_094840\_sdudlog.zip), and 'Extracted Location' (C:\ProgramData\Sophos\SURF\Extracted\30AFC4A20D0A0A93C8D000CD42836E0D8DE5AC900EE). It also includes 'REBUILD' and 'Delete' buttons. The 'System Information' section provides details about the host: Host Name (WINCLIENT1), OS Type (Microsoft Windows 10 Pro 10.0.17763 N/A Build 17763 x64-based PC), CPU (Intel® Family 6 Model 166 Stepping 0 GenuineIntel ~1.608 MHz), RAM Total (UTC-00:00) Dublin, Edinburgh, Lisbon, London), RAM Used (4,095 MB), and Boot Time (Boot Time 25/02/2022, 09:40:51). At the bottom, there are 'About' and 'Feedback' buttons. A small note at the top right says 'Mode: Partner Support'. The bottom right corner of the interface has the word 'SOPHOS'.

The tool will collect the logs and provide options of what to do with the log file. In order to use the log file with SURF, select **Open folder** to view the file. The location of the most recent log and all created archives is in the users temporary folder.

Once loaded into the SURF tool, you can view all of the details of the device.

## [Additional Information]

The most recent log and created archives location is: C:\Users\<username>\AppData\Local\Temp\sdudlog.zip



Additional information in  
the notes

# Generating an SDU on Linux

## Sophos Protection for Linux

```
# /opt/sophos-spl/bin/sophos_diagnose
Created tarfile: sspl-diagnose_20220322_095706.tar.gz in directory .
# ls
sspl-diagnose_20220322_095706.tar.gz
#
```

## Sophos Anti-Virus for Linux (legacy)

```
# /opt/sophos-av/bin/savdstatus --diagnose
Creating zip with results at SAV_diagnose_20220322_100352.zip
# ls
SAV_diagnose_20220322_100352.zip
#
```

SOPHOS

To generate an SDU file on a Sophos protected Linux server you will need to run a specific command. The command you run will depend on whether you have deployed Sophos Protection for Linux (SPL) or Sophos Anti-virus for Linux (Legacy).

For an SPL protected server, use the command **sophos\_diagnose**. This will output a file to the current directory where the command was run. To specify where the diagnostic output file should be created, run the command with the selected directory as the first argument. For example, to output the diagnostic log collection to the temp folder, run the command **sophos\_diagnose /tmp**.

For a legacy protected server, run the following command from the console terminal with root privileges, **savdstatus --diagnose**. Please note that if Sophos anti-virus is installed to a non-standard directory, you will need to change the directory path. The files will be archived into the directory where you ran the command from.

## [Additional Information]

The full path for the Sophos diagnose is **/opt/sophos-spl/bin/sophos\_diagnose /tmp**  
The full path for the SAV diagnose is **/opt/sophos-av/bin/savdstatus -diagnose**

# Loading a Linux SDU into SURF

The screenshot shows the SURF software interface. At the top, there are two tabs: 'SAV Diagnose' and 'SPL'. The 'SAV Diagnose' tab is active. In the center, there's a 'SDU/CTR Control' section with fields for 'SDU/CTR Name' (set to 'Not Found'), 'SDU/CTR Friendly Name' (set to 'SPL'), and 'Case #' (set to 'Not Set'). Below these are 'Database' and 'Archive Location' fields, both pointing to 'C:\ProgramData\Sophos\SURF\Datasets\341FA0D59B79AA000AE2370CAF8\4A73B92921CB80.sqlite'. Under 'Extracted Location', it shows 'C:\Users\rebeccacosk\Downloads\`spl-diagnose\_20220322\_095706.tar.gz' and 'C:\ProgramData\Sophos\SURF\Extracted\341FA0D59B79AA000AE2370CAF8'. There are 'REBUILD' and 'Delete' buttons. To the right, there's an 'Issues Dashboard' with sections for Critical (0), High (0), and Moderate (0) issues. Below that is a 'Health' section with various status items like Overall, Service Health, Administration Health, Threat Health, Isolation Status, Last Update Time, and Last Update Result, all marked as 'Not Applicable' or 'Not Found'. At the bottom left are 'About' and 'Feedback' buttons.

SOPHOS

When you load either Linux server log into SURF, the same information will be displayed. You will be able to view an overview of the file along with any variables, policies, and exclusions configured.

# SURF Dashboard

The screenshot shows the SURF dashboard interface. On the left is a sidebar with links: Landing, Dashboard, Detections, Rules, Network, Variables, Applications, Policies, Exclusions, Services, Search, Comments, and Settings. At the bottom of the sidebar are About and Feedback buttons. The main area has tabs at the top: macOS Device (disabled), Windows Device (selected), Firewall Logs (disabled), and Firewall System Snapshot (disabled). The Mode button is set to Partner.

**SDU/CTR Control**

- SDU/CTR Name: WINCLIENT1
- SDU/CTR Friendly Name: Windows Device
- Case #: Not Set
- Database: C:\ProgramData\Sophos\SURF\Datasets\3AFCAA2D90A9A3C6000CDA2836E060B83CACB80EE.sqlite
- Archive Location: C:\Users\rebecapook\Downloads\WinClient1\_20220321\_094729.sdu
- Extracted Location: C:\ProgramData\Sophos\SURF\Extracted\3AFCAA2D90A9A3C6000CDA2836

**System Information**

- Host Name: WINCLIENT1
- OS Type: Microsoft Windows 10 Pro 10.0.17763 N/A Build 17763 x86-based PC
- CPU: Intel® Family 6 Model 166 Stepping 0 GenuineIntel -1608 Mhz
- RAM Total: [UTC+00:00] Dublin, Edinburgh, Lisbon, London
- RAM Used: 4,095 MB
- Boot Time: Boot Time 25/02/2022, 09:40:51

**Issues Dashboard**

Severity	Count	More
Critical	1	>
High	0	>
Moderate	0	>

**Health**

- Overall: Good
- Service Health: Good
- Administration Health: Good
- Threat Health: Good
- Isolation State: Not Isolated

Last Update Time: 2022-03-21T09:12:41 UTC

Last Update Result:

A green callout box points to the Issues Dashboard section with the text "View detected issues".

SOPHOS

Once you have loaded a file into SURF, you can view all of the information contained in the file. It is worth noting that you can open multiple SDU files in SURF. Simply click the plus icon at the top of the tool to add a new file. There is no limit to the amount of files you can open, however, the files will be stacked once they have reached the banner width.

Let's walk through an example file.

On the **Dashboard** tab you will find the main information included in the file, this includes the hostname of the device along with the operating system, and hardware information. The right-hand side of the dashboard displays at-a-glance, any critical, high, or moderate issues that have been detected. It also shows the overall health of the device.

Clicking on any of the issues will display the detection details.

# SURF Detections

The screenshot shows the SURF interface with the 'Detections' tab selected. A prominent red exclamation mark icon indicates a critical detection. The details pane shows the following information:

- A reboot is pending to complete an installation or update.
- 00829fd0-047f-438f-a805-1088822e90d5 Severity: 9
- Line: 0
- KBA: 0000011830

On the right side of the detection card are three buttons: a green checkmark, a blue pencil, and a red X. A callout bubble points to the red X button with the text: "Mark the detection as resolved, not applicable or dismissed".

The **Detections** tab displays any detections found in the file. Detections are displayed by severity and display the log file and knowledge base article information for that detection.

In this example, a reboot is pending on the device. The severity of the detection, the log file, registry key, and process where it was found and the knowledge base article can be seen here. Using the options on the right-hand side you can mark the detection as resolved, not applicable, or dismissed.



# SURF Rules

The screenshot shows the SURF Rules application interface. On the left is a sidebar with navigation links: Landing, Dashboard, Detections, Rules (which is selected), Network, Variables, Applications, Policies, Exclusions, Services, Search, Comments, and Settings. At the bottom of the sidebar are About and Feedback buttons. The main area is titled "Current Rules". It displays a table with four columns: Severity (red), Type (Ep), Description, and Version. There are four rows of data:

Severity	Type	Description	Version
10	Ep	3rd party software cannot be removed due to detection only 70a0f0d7-cbce-4223-8e73-058ab0b109fc	Version: 7
10	Ep	AMSI integration in Microsoft Exchange Server 2016 / 2019 causes performance issues when Sophos Central Server Protection AMSI functionality is enabled d4567070-3bd0-4a65-be02-b9c801a3c69c	Version: 3
10	Ep	Another installation or update in progress. Cannot install Sophos Endpoint while another products is being installed or updated 98cd3a8-0d92-4be4-88ae-13ff2ec024a9	Version: 1
10	Ep	BitLocker Encryption not started due to inserted bootable CD/DVD/ISO 57fbca93-6bd0-409f-959b-d5293b0c1b95	Version: 3
		Email notification not working in Legacy mode(external Email server setting)	

All rules being applied are listed

SOPHOS

Rules are a way for Sophos Support to share knowledge of ongoing issues.

Sophos Support creates a rule, which is configured as .json file, the rule engine intercepts the data. It then reports if any of the rules are matched. If a rule is not fully met, Sophos Support can investigate.

SURF displays a list of the current rules being applied. If a rule has been met, this is displayed on the **Detections** tab. Rules are shared with the Endpoint Self Help tool and are constantly maintained. Rules are archived once an issue is resolved and new rules are introduced when required.

## [Additional Information]

You can also view the rules applied by navigating to C:\ProgramData\Sophos\SURF\Rules all of the .json rule files will be listed here. Please note that these files cannot be edited or overwritten.

# SURF Network

The screenshot shows the SURF Network interface. On the left, a sidebar lists various tabs: Landing, Dashboard, Detections, Rules, Network (which is selected), Variables, Applications, Policies, Exclusions, Services, Search, Comments, Settings, About, and Feedback. The main content area has tabs for Network Interfaces, Routes - IPv4, and Routes - IPv6. The Network Interfaces tab shows one entry: Intel(R) 82574L Gigabit Network Connection, 00-0C-29-FD-F8-89, 172.16.16.70. The Routes - IPv4 and Routes - IPv6 tabs show tables of routes with columns for Interface, Netmask, Destination, Gateway, and Metric. A green callout box points to the Network Interfaces section with the text "View all available interfaces".

Interface	Netmask	Destination	Gateway	Metric
0.0.0	172.16.16.16	172.16.16.70	281	0.0.0
127.0.0	On-link	127.0.0.1	331	255.0.0
127.0.0.1	On-link	127.0.0.1	331	255.255.255.255
127.255.255.255	On-link	127.0.0.1	331	255.255.255.255
172.16.16.0	On-link	172.16.16.70	281	255.255.255.0
172.16.16.70	On-link	172.16.16.70	281	255.255.255.255
172.16.16.255	On-link	172.16.16.70	281	255.255.255.255
224.0.0	On-link	127.0.0.1	331	240.0.0
224.0.0.0	On-link	172.16.16.70	281	240.0.0
255.255.255.255	On-link	127.0.0.1	331	255.255.255.255
255.255.255.255	On-link	172.16.16.70	281	255.255.255.255
1	-1/128	On-link	331	
2	fe80::/64	On-link	281	
1	ff00::/8	On-link	331	
2	ff00::/8	On-link	281	

Interface	Network	Destination	Gateway	Metric
1	-1/128	On-link	331	
2	fe80::/64	On-link	281	
1	ff00::/8	On-link	331	
2	ff00::/8	On-link	281	

The **Network** tab displays all of the available interfaces on the device. It also lists the IPv4 and IPv6 addresses and groups.

SOPHOS

# SURF Variables

The screenshot shows the SURF Variables tool interface. At the top, there's a header with the SURF logo, version 2.0.0.20, and "A Sophos Support Tool". Below the header are tabs for "MacOS Device" (disabled), "Windows Device" (selected), "Firewall Logs" (disabled), and "Firewall System SnapShot" (disabled). A "Mode" dropdown is set to "Partner". On the left, a sidebar menu lists: Landing, Dashboard, Detections, Rules, Network, Variables (selected), Applications, Policies, Exclusions, Services, Search, Comments, and Settings. At the bottom of the sidebar are "About" and "Feedback" buttons. The main content area is titled "Environment Variables" and displays a list of registry keys:

```
1 ALLUSERSPROFILE=C:\ProgramData
2 APPDATA=C:\Users\Sophos\AppData\Roaming
3 CommonProgramFiles=C:\Program Files (x86)\Common Files
4 CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
5 CommonProgramW6432=C:\Program Files\Common Files
6 COMMON_APPDATA=C:\ProgramData
7 COMPUTERNAME=WINCLIENT1
8 ComSpec=C:\Windows\system32\cmd.exe
9 DriveData=C:\Windows\System32\Drivers\DriverData
10 HOMEDRIVE=C:
11 HOMEPATH=\Users\Sophos
12 LOCALAPPDATA=C:\Users\Sophos\AppData\Local
13 LOGONSERVER=\\WINCLIENT1
14 NUMBER_OF_PROCESSORS=2
15 OneDrive=C:\Users\Sophos\OneDrive
16 OS=Windows_NT
17 PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
18 PROCESSOR_ARCHITECTURE=x86
19 PROCESSOR_ARCHITEW6432=AMD64
20 PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 166 Stepping 0, GenuineIntel
21 PROCESSOR_LEVEL=6
22 PROCESSOR_REVISION=a600
23 ProgramData=C:\ProgramData
24 ProgramFiles=C:\Program Files
25 ProgramFiles(x86)=C:\Program Files (x86)
```

A green callout bubble on the right side of the window says "View configuration conflicts on the device".

It is important to note that some tabs will not be displayed for some files. The tabs displayed are dependent on the file type loaded.

The **Variables** tab will be displayed for Windows SDU logs. This tab displays a list of all variables included in the registry under the variable registry key.

# SURF Applications

The screenshot shows the SURF application interface. At the top, there are tabs for 'MacOS Device' (selected), 'Windows Device', 'Firewall Logs', and 'Firewall System SnapShot'. Below the tabs is a navigation sidebar with links like Landing, Dashboard, Detections, Rules, Network, Variables, Applications (selected), Policies, Exclusions, Services, Search, Comments, and Settings. At the bottom of the sidebar are 'About' and 'Feedback' buttons. The main content area is titled 'Applications' and contains a table of installed applications. The table includes columns for the application name, version, and last update. A green callout box points to the 'Sophos Only' filter button at the top of the table. The table lists various applications including Microsoft Update Health Tools, Microsoft Visual C++ 2015-2019 Redistributable (x64), Mozilla Firefox, Mozilla Maintenance Service, Mozilla Thunderbird, Sophos AMSI Protection, Sophos Anti-Virus, Sophos AutoUpdate XG, Sophos Clean, Sophos Diagnostic Utility, Sophos Endpoint Agent, Sophos Endpoint Defense, Sophos Endpoint Firewall, Sophos Endpoint Self Help, Sophos Exploit Prevention, Sophos File Scanner, and Sophos Health.

Application	Version	Last Update
Microsoft Update Health Tools	2.85.0.0	Version: 14.24.28127
Microsoft Visual C++ 2015-2019 Redistributable (x64)	14.24.28127	Version: 14.24.28127
Microsoft Visual C++ 2019 Redistributable (x86)	14.24.28127	Version: 14.24.28127
Microsoft Visual C++ 2019 X64 Additional Runtime	14.24.28127	Version: 14.24.28127
Microsoft Visual C++ 2019 X64 Minimum Runtime	14.24.28127	Version: 14.24.28127
Microsoft Visual C++ 2019 X86 Additional Runtime	14.24.28127	Version: 14.24.28127
Microsoft Visual C++ 2019 X86 Minimum Runtime	14.24.28127	Version: 14.24.28127
Mozilla Firefox (x64 en-GB)	95.0	Version: 95.0
Mozilla Maintenance Service	91.3.2	Version: 91.3.2
Mozilla Thunderbird (x64 en-CA)	91.3.2	Version: 91.3.2
Sophos AMSI Protection	1.8.59	Version: 1.8.59
Sophos Anti-Virus	10.8.11.41	Version: 10.8.11.41
Sophos AutoUpdate XG	6.12.66	Version: 6.12.66
Sophos Clean	3.9.14.1	Version: 3.9.14.1
Sophos Diagnostic Utility	6.11.2.24	Version: 6.11.2.24
Sophos Endpoint Agent	2.4.230.0	Version: 2.4.230.0
Sophos Endpoint Agent	2.20.11	Version: 2.20.11
Sophos Endpoint Defense	3.0.1.878	Version: 3.0.1.878
Sophos Endpoint Firewall	2.0.20.0	Version: 2.0.20.0
Sophos Endpoint Self Help	3.1.88.0	Version: 3.1.88.0
Sophos Exploit Prevention	3.8.3.812	Version: 3.8.3.812
Sophos File Scanner	1.9.16.3	Version: 1.9.16.3
Sophos Health	2.8.130.0	Version: 2.8.130.0

Filter applications list to show only Sophos applications

On the **Applications** tab, a list of all installed applications on the device is displayed. This list can be filtered and you can also use the **Sophos Only** option to display only the Sophos applications that are installed.

You can also search for an application name or version. For example, you could search for v10.1 which will return any application using that version.

# SURF Policies

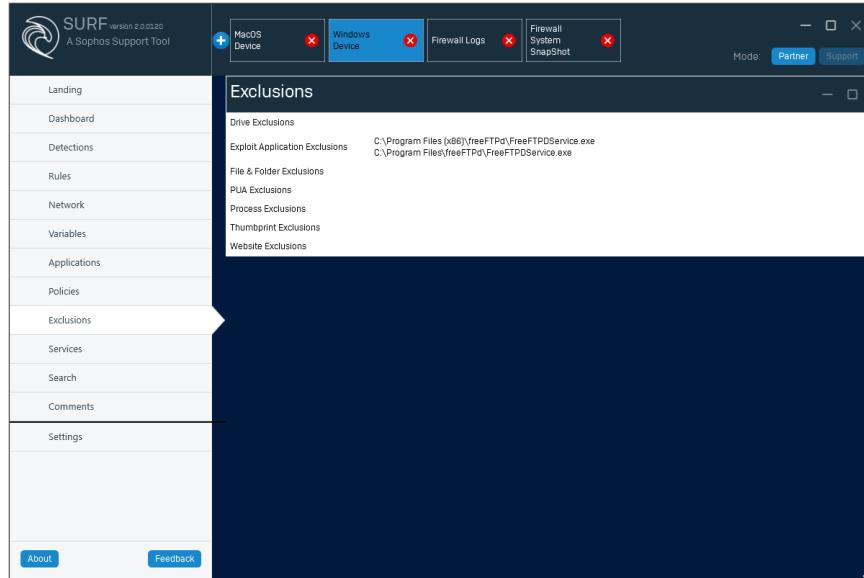
The screenshot shows the SURF Policies interface. On the left is a sidebar with navigation links: Landing, Dashboard, Detections, Rules, Network, Variables, Applications, Policies (which is selected), Exclusions, Services, Search, Comments, and Settings. At the bottom of the sidebar are 'About' and 'Feedback' buttons. The main area is titled 'Policies' and lists various policy items with their current status. A green callout box points to the status column, which uses color coding: green for TRUE, red for OFF, and grey for FALSE.

Policy	Status
Automatic Cleanup	TRUE
Block Access to Malicious Websites	TRUE
Cryptoguard	OFF
Cryptoguard, Remotely Run	OFF
Deep Learning	ON
Detect Malicious Behavior (HIPS)	FALSE
Detect Network Traffic to C2C Servers	TRUE
Detect low-reputation file downloads	ON
Live Protection	OFF
MBR Protection (Wipeguard)	OFF
Mitigate Exploits	ON
Mitigate Exploits - Java	ON
Mitigate Exploits - Media	ON
Mitigate Exploits - Office	ON
Mitigate Exploits - Web	ON
Mitigate Exploits - Web Plugins	ON
Prevent Process Hollowing	OFF
Prevent Untrusted DLL Loading	OFF
Real Time Scanning	TRUE
Safe Browsing	OFF
Scan Downloads in Progress	ON
Tamper Protection	OFF

View the policies that are applied or not

The **Policies** tab is really useful in quickly determining what policies are currently applied and which are not. It uses a colour coded menu which shows when policies are active, denoted in green. Or, when a policy is not applied or switched off, denoted in red.

# SURF Exclusions



View all exclusions applied

The **Exclusions** tab is really useful as it allows you to view all exclusions that have been applied to the device. This is particularly useful to determine that exclusions have been applied correctly. Although you cannot take action through this tab, it does provide a qualitative assessment of all exclusions currently applied.

# SURF Services

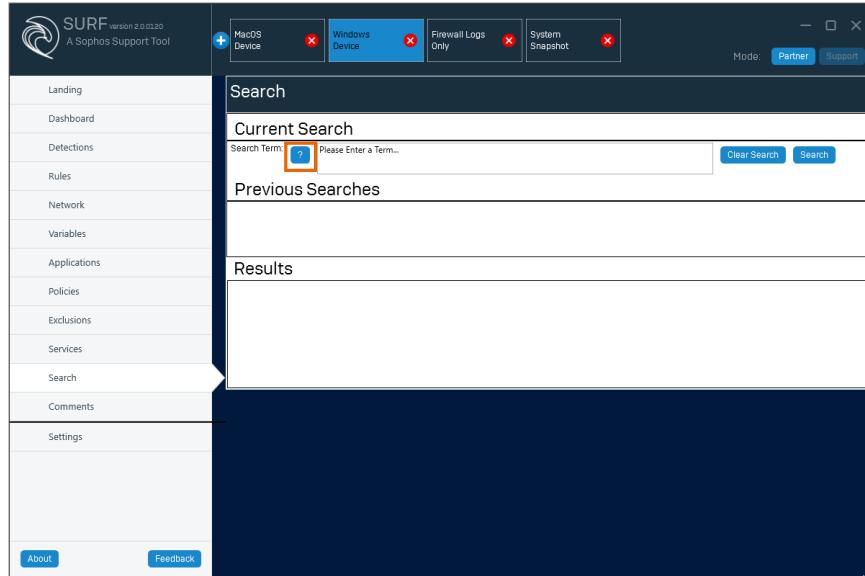
The screenshot shows the SURF Services interface. At the top, there are tabs for 'MacOS Device' (disabled), 'Windows Device' (selected), 'Firewall Logs' (disabled), and 'Firewall System SnapShot' (disabled). Below the tabs is a 'Mode' button with 'Partner' and 'Support' options. The main area is titled 'Services' and contains a table with columns for service name, process ID, and status. The status column uses color coding: red for stopped services and green for running services. A green callout box on the right side points to the table, with the text: 'View all services and the current status (at the time of log collection)'. The bottom of the interface has a sidebar with links like Landing, Dashboard, Detections, Rules, Network, Variables, Applications, Policies, Exclusions, Services, Search, Comments, and Settings. There are also 'About' and 'Feedback' buttons at the bottom.

Service	Process ID	Status
AVCTP service	0	1 STOPPED
ActiveX Installer (AxinstSV)	0	1 STOPPED
AllJoyn Router Service	0	1 STOPPED
App Readiness	0	1 STOPPED
AppX Deployment Service (AppXSVC)	6772	0 RUNNING
Application Identity	0	1 STOPPED
Application Information	18896	4 RUNNING
Application Layer Gateway Service	0	1 STOPPED
Application Management	0	1 STOPPED
AssignedAccessManager Service	0	1 STOPPED
Auto Time Zone Updater	0	1 STOPPED
Background Intelligent Transfer Service	0	1 STOPPED
Background Tasks Infrastructure Service	804	4 RUNNING
Base Filtering Engine	13444	0 RUNNING
BitLocker Drive Encryption Service	0	1 STOPPED
Block Level Backup Engine Service	0	1 STOPPED
Bluetooth Audio Gateway Service	0	1 STOPPED
Bluetooth Support Service	0	1 STOPPED
Bluetooth User Support Service_54dd7a33	0	1 STOPPED
BranchCache	0	1 STOPPED
CNG Key Isolation	692	0 RUNNING
COM+ Event System	2300	4 RUNNING
COM+ System Application	4756	4 RUNNING

Like the applications tab, the **Services** tab is a colour coded list of all services on the device. It displays which services are running and which are stopped.

You can filter the list to show a particular service.

# SURF Search

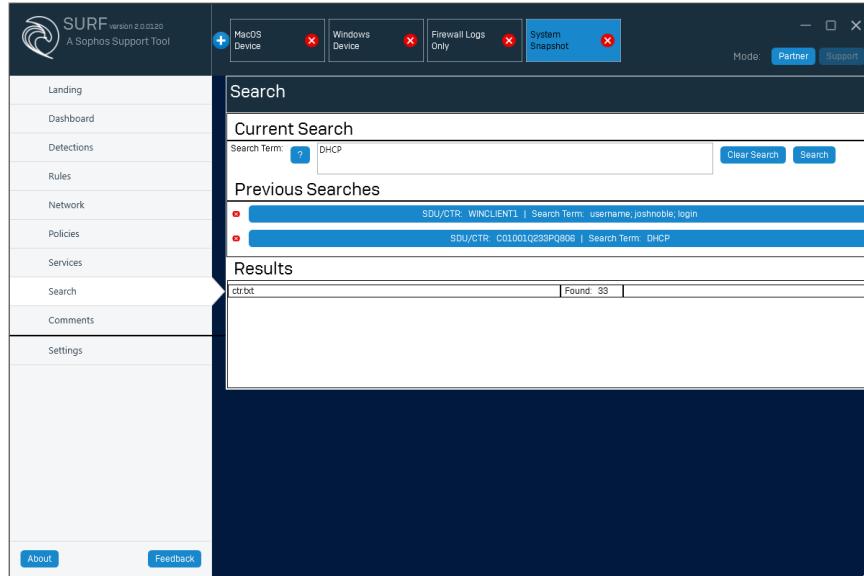


SOPHOS

In the **Search** tab, you can search the loaded log files. Clicking on the search term question mark, you can view the available search options.

In this example, we have searched for the username josh noble and the term login. Each search term will be searched for independently and the results are returned. The results lists the file the term was found in and how many times it was found.

# SURF Search

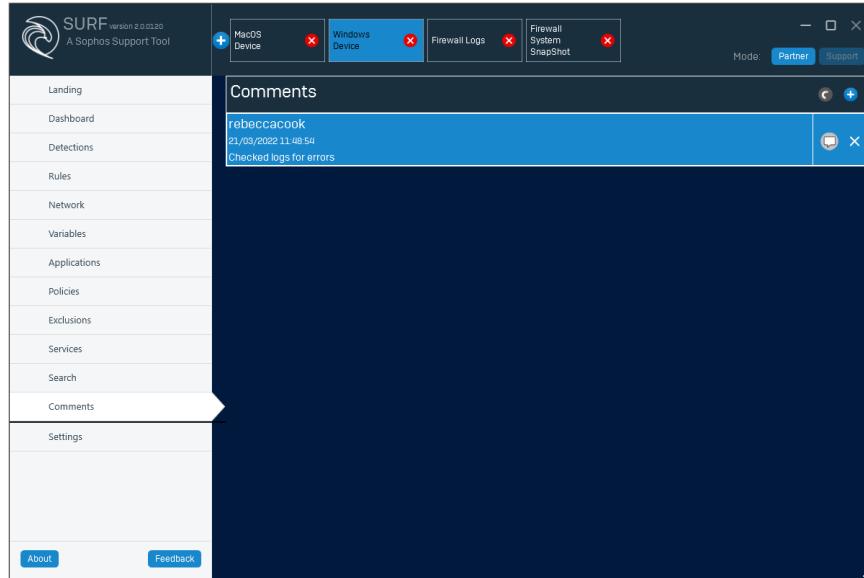


SOPHOS

The search tool can only search for a term within the active archive file, it is not able to search across all loaded archives. The previous searches section lists all searches that have been run against any archive file loaded. This allows you to view all searches made which are listed with the SDU name along with the search term used.

Clicking on a returned search result will display which line of the log the search term was found in. Clicking on this will open that log file to the line where it was found.

# SURF Comments



SOPHOS

The **Comments** tab allows you to add comments. You can create a new comment, edit, or delete an existing comment. Any comments added will appear in linear order.



Additional information in  
the notes

# SURF Settings

The screenshot shows the SURF Settings tab. At the top, there are tabs for macOS Device, Windows Device, Firewall Logs, and Firewall System Snapshot, each with a red 'X' icon. Below these are SDU/CTR Settings with options for Debug Logging (OFF), Consume Logs (OFF), and Analyze on Open (OFF). The main area displays 'Current Databases' with a list of entries, each with a 'Rebuild Database' and 'Delete' button. To the right, there's a 'Feedback' section with radio buttons for General Feedback, Issue Report, or Suggestion, and a text input field for feedback. Buttons for 'Clear Feedback' and 'Submit Feedback' are at the bottom of this section. A green callout box on the right states: 'All feedback submitted is reviewed by the Sophos support team'.

In the **Settings** tab you can view all of the databases that you have opened in the SURF tool. From this tab you can also submit feedback about this tool to Sophos Support.

Select what type of feedback you want to provide, general feedback, issue reporting or provide a suggestion for the tool.

We review all feedback submitted and are always looking to improve this tool.

## [Additional Information]

Please join the Partners-only SURF Community group to raise questions and receive support: <https://community.sophos.com/sophos-partners/surf/>

It is worth noting that the support option in the top right-hand corner is used by Sophos support to field test new features.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 4

Which archive file can be loaded into the SURF tool?

RAR

ISO

SDU

7zip

SOPHOS

## Question 2 of 4

**True or False:** The SURF tool is only available for Sophos Partners.

True

False



## Question 3 of 4

Which operating system can the SURF tool be run on?

MacOS 11.12

Linux Server

Windows Server 2019

Windows 10 or later

SOPHOS



## Question 4 of 4

**True or False:** All tabs are displayed for any SDU file loaded into the SURF tool.

True

False

SOPHOS

# Chapter Review

The SURF tool has been **developed by Sophos Support** to **aid troubleshooting**.

The SURF tool is **only available to Sophos partners** and can only be run on **Windows 10 or later** devices.

The SURF tool **extracts data** from the loaded files and displays it in an **easy-to-read** format.

SOPHOS

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

The SURF tool has been developed by Sophos Support to aid troubleshooting.

The SURF tool is only available to Sophos partners and can only be run on Windows 10 or later devices.

The SURF tool extracts data from the loaded files and displays it in an easy-to-read format.



# Troubleshooting Windows Active Directory Synchronization in Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE1035: Troubleshooting Windows Active 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.

# Troubleshooting Windows Active Directory Synchronization in Sophos Central

In this chapter you will learn how to troubleshoot common Active Directory Synchronization Utility issues.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to add users in Sophos Central
- ✓ How to configure AD Sync Utility

DURATION **12 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot common Active Directory Synchronization Utility issues.

# AD Sync Utility Common Issues



Sophos Central connection



Active Directory connection



Filter configuration

SOPHOS

Issues with the AD Sync Utility tool generally fall into one of the following categories:

- The connection to Sophos Central
- The connection to Active Directory
- Problems relating to filter configuration

We will look at an example of each of these and how to troubleshoot them.

# Sophos Central Connection

SOPHOS

We will start with an example of an issue with the connection from the AD Sync Utility tool to Sophos Central.

# Sophos Central Connection

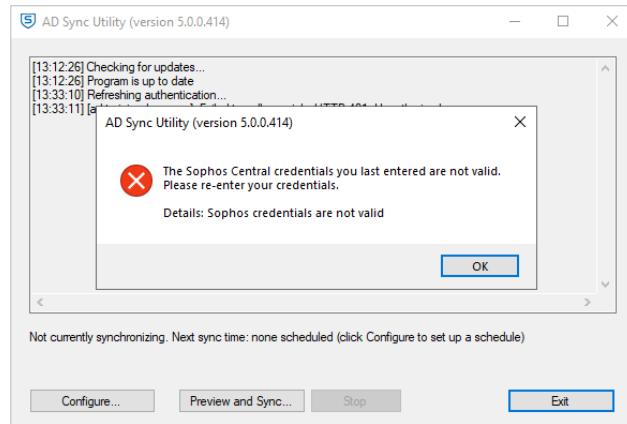


The screenshot shows the Sophos Central interface with the 'People' section selected. The page title is 'People' with the subtitle 'Manage your users'. There are tabs for 'Users' (selected) and 'Groups'. Below are buttons for 'Add', 'Email Setup Link', and 'Delete', along with an 'Export to CSV' link. A search bar is present. The main area displays a table of users with columns: Name, Email, Exchange Login, Last Active, Group Name, and Role. One user, 'Anne Green', is highlighted with a green callout bubble containing the text: 'New users are not being added to Sophos Central'.

Name	Email	Exchange Login	Last Active	Group Name	Role
[Redacted]	[Redacted]	Add Exchange Login		Central Ad...	Super Ad...
[Redacted]	[Redacted]				
Anne Green	[Redacted]				
Jake Murphy	jakemurphy@trainingdemo.xyz	Exchange Login		Admin	
[Redacted]	[Redacted]	Add Exchange Login			
[Redacted]	[Redacted]	Add Exchange Login			

A common symptom for AD Sync Utility issues, whatever the cause, are new users, groups, or devices not being added to Sophos Central.

# Sophos Central Connection



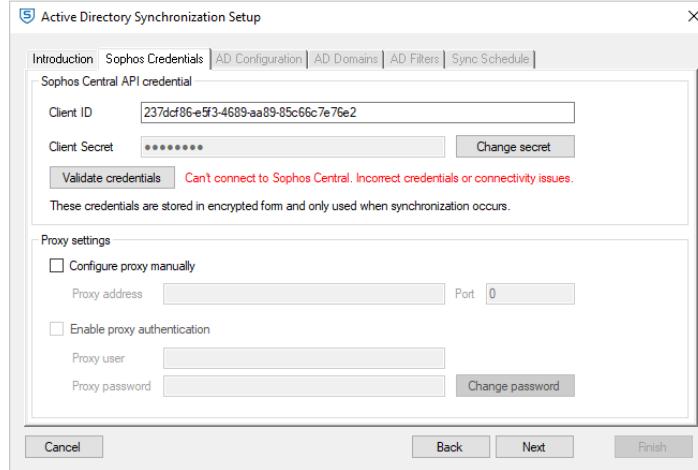
SOPHOS

A good first step is to open the AD Sync Utility tool and select **Preview and Sync...** This will often generate an error that will help you with further troubleshooting.

In this case we can see that there is a problem with the Sophos Central credentials.

Click **Configure...** to review the settings.

# Sophos Central Connection



SOPHOS

AD Sync Utility uses API credentials to connect to Sophos Central, and here you can see the Client ID for the API credentials.

Click **Validate credentials** to check if they are working. Here we can see that AD Sync Utility cannot connect to Sophos Central due to incorrect credentials or connectivity issues.

# Sophos Central Connection



%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs

```
01:28:23.843 PM      Information [Th 14] Configuring secure Sophos Central  
connection  
01:28:25.155 PM      Information [Th 14] HTTP request to  
https://cloud.sophos.com/api/sessions error Unauthorized: HTTP 401: Unauthorized  
01:28:25.201 PM      Error [Th 14] Active Directory synchronization failed.  
Reason: SophosCloudADSyncLib.NeedCloudCredsException: Sophos credentials are not  
valid ---> System.Net.Http.HttpRequestException: HTTP 401: Unauthorized --->  
CommandLib.HttpRequestCommand+HttpStatusException: Exception of type  
'CommandLib.HttpRequestCommand+HttpStatusException' was thrown.  
--- End of inner exception stack trace ---
```

SOPHOS

Let's take a look at what you would see in the log file in this scenario. Here you can see a very clear error message that the credentials are not valid.

# Sophos Central Connection



The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane includes 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (with 'Application', 'Security', 'Setup', 'System', 'Forwarded Events'), 'Applications and Services Log' (with 'Active Directory Web Server', 'DFS Replication', 'Directory Service', 'DNS Server', 'Forefront Identity Manager', 'Hardware Events', 'Internet Explorer', 'Key Management Service', 'Microsoft', 'Microsoft Azure AD Sync', 'Microsoft Azure AD Sync', 'OpenSSH', 'Sophos Cloud AD Sync', and 'Windows PowerShell'), and 'Subscriptions'. The 'Sophos Cloud AD Sync' node is highlighted with a red box. The main pane displays a list of events for 'Sophos Cloud AD Sync' with 241 entries. One specific event is expanded, showing the 'General' and 'Details' tabs. The 'Details' tab contains a large amount of error text:

**Active Directory synchronization failed.**  
Reason:  
SophosCloudADSyncLib.NeedCloudCredsException:  
**Sophos credentials are not valid** --->  
System.Net.Http.HttpRequestException: HTTP 401: Unauthorized --->  
CommandLib.HttpRequestCommand+HttpStatusException  
--- End of inner exception stack trace ---  
at CommandLib.HttpRequestCommand.EnsureSuccessStatusCodeResponseCheck  
at CommandLib.HttpRequestCommand.SyncExImpl(Object runtimeArg)  
at CommandLib.CommandBaseSyncExecute(Object runtimeArg, Command owner)  
at CommandLib.RetryableCommand.SyncExImpl(Object runtimeArg)  
at CommandLib.CommandBaseSyncExecute(Object runtimeArg, Command owner  
at SophosADSync.SophosCloudWebClient.MakeRequest(String address, HttpMethod  
maxRetries, Command context)

Log Name: Sophos Cloud AD Sync  
Source: Sophos AD Sync  
Event ID: 0  
Level: Error  
User: N/A  
Logged: 08/07/2022 13:28:25  
Task Category: (3)  
Keywords: Classic  
Computer: UK-DC01.ad.trainingdemo.xyz

The 'Actions' pane on the right lists options: 'Open Saved Log...', 'Create Custom View...', 'Import Custom View...', 'Clear Log...', 'Filter Current Log...', and 'Properties'.

In addition to the log file, AD Sync Utility logs to the Windows Event Viewer in **Applications and Services Logs > Sophos Cloud AD Sync**. Here you can see a very similar error to what we saw in the log file.

# Sophos Central Connection



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 navigation items: Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected), Third-party Connectors, Protect Device, and Account Health. Below that is 'MY PRODUCTS' with options for Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, and Email Security. The main content area is titled 'API Credentials Management' under 'Settings / API Credentials Management'. It has tabs for 'Credentials' (selected) and 'Roles'. A note says 'Note: You may create up to 10 credentials.' There's a table with one row: NAME: API, CREDENTIAL ID: b9651df6 (redacted), ROLE: Service Principal Super Admin, CREATED ON: Aug 26, 2021, LAST USED ON: Aug 26, 2021, EXPIRES ON: Aug 25, 2024. A green callout box on the left says 'Check if API credentials have expired or been deleted'. On the right, there's a modal window titled 'Active Directory Synchronization Setup' with tabs for Introduction, Sophos Credentials, AD Configuration, AD Domains, AD Filters, and Sync Schedule. The 'Sophos Central API credential' tab is selected. It shows 'Client ID: 237dcf86' (highlighted with an orange border) and 'Client Secret: \*\*\*\*\*'. There's a 'Change secret' button and a 'Validate credentials' button. A note below says 'These credentials are stored in encrypted form and only used when synchronization occurs.'

From the errors we have seen we can be fairly certain that this is an issue with the API credentials, so the next place to check is Sophos Central in **Global Settings > API Credentials Management**.

Here you should check that the API credentials with the client ID found in AD Sync Utility are present, have not expired, and have the correct role (Service Principal Directory Sync).

Here we can see that the API credentials have been removed, however, you would need to create a new set of API credentials as the client secret is only shown once when the API is first created.

# Sophos Central Connection



The screenshot shows the Sophos Central API Credentials Management page. On the left, there's a sidebar with 'Global Settings' selected. The main area displays a table of credentials, with one row for 'Active Directory Sync' highlighted by an orange border. This row corresponds to the 'Active Directory Synchronization Setup' modal window, which is overlaid on the main page. The modal contains fields for 'Client ID' (18e80d2d) and 'Client Secret' (redacted), and a 'Validate credentials' button with the message 'Credentials are correct!'. Other tabs in the modal include 'Introduction', 'Sophos Credentials', 'AD Configuration', 'AD Domains', 'AD Filters', and 'Sync Schedule'. At the bottom of the modal, it says 'These credentials are stored in encrypted form and only used when synchronization occurs.' Below the modal, there are 'Proxy settings' options.

NAME	CREDENTIAL ID	ROLE	CREATED ON	LAST USED ON	EXPIRES ON
API	b9651df6- <span style="background-color: #cccccc; color: black;">XXXXXXXXXX</span>	Service Principal Super Admin	Aug 26, 2021	Aug 26, 2021	Aug 25, 2024
Active Directory Sync	18e80d2d- <span style="background-color: #cccccc; color: black;">XXXXXXXXXX</span>	Service Principal Directory Sync	Jul 08, 2022	Jul 08, 2022	Jul 07, 2025

In this scenario, we have created new API credentials for the AD Sync Utility, added them, and checked they are valid.

# Sophos Central Connection



The screenshot shows the Sophos Central 'People' management interface. On the left, a sidebar lists various product categories like Endpoint Protection, Server Protection, and Email Security. The 'People' section is selected and highlighted in blue. The main area is titled 'People: Manage your users' and contains tabs for 'Users' and 'Groups'. Under 'Users', there are buttons for 'Add', 'Email Setup Link', and 'Delete'. A dropdown menu shows 'All users'. On the right, there's a search bar and a 'Export to CSV' button. The main table lists users with columns for Name, Email, Exchange Login, Last Active, and Group Name. One row is highlighted with a red box, showing a user named Anne Green with the status 'agree' under 'Last Active' and 'Marketing (TRAINING)' under 'Group Name'. Other users listed include Fred Rogers, Jake Murphy, Jane Doe, and Jo Brown.

Name	Email	Last Active	Group Name
Anne Green		agree	Marketing (TRAINING)
Fred Rogers		frogers	Support (TRAINING)
Jake Murphy	jakemurphy@trainingdemo.xyz	Add Exchange Login	
Jane Doe		jdoe	Sales (TRAINING)
Jo Brown		jbrown	HR (TRAINING)

Once the AD Sync Utility performs its next synchronization with Sophos Central you will see the missing users added. This would be the same for groups and devices.

# Active Directory Connection

SOPHOS

We will now look at two examples related to the connection from AD Sync Utility to Active Directory.

# Active Directory Connection: Scenario 1

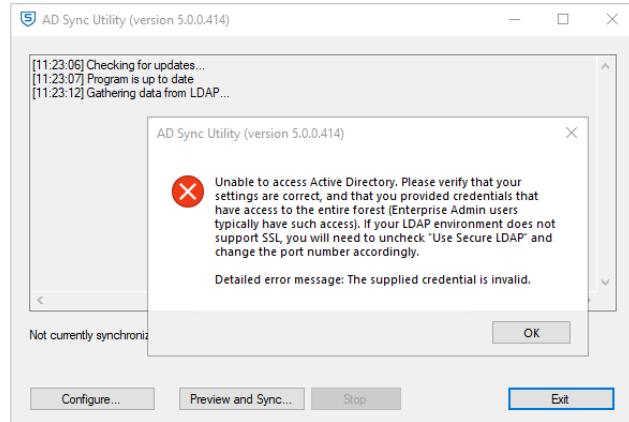


The screenshot shows the Sophos Central interface with the 'People' section selected. The page title is 'People' with the subtitle 'Manage your users'. There are tabs for 'Users' (selected) and 'Groups'. Below are buttons for 'Add', 'Email Setup Link', and 'Delete', along with a 'Search' bar. A table lists users with columns: Name, Email, Exchange Login, Last Active, Group Name, and Role. One user, Anne Green, is highlighted with a green callout box containing the text: 'New users are not being added to Sophos Central'.

Name	Email	Exchange Login	Last Active	Group Name	Role
Anne Green	anne.green@trainingdemo.xyz	Add Exchange Login	Central Ad...	Super Ad...	
Jake Murphy	jake.murphy@trainingdemo.xyz	Exchange Login	Admin		
		Add Exchange Login			
	ztna@trainingdemo.xyz	Add Exchange Login	Super Ad...		

We will continue with the same symptom of new users not being added to Sophos Central.

# Active Directory Connection: Scenario 1



SOPHOS

As with the previous scenario we will start by initiating a manual **Preview and Sync...** in AD Sync Utility to try and generate an error for more information.

Here the error is indicating an issue with the user credentials provided for AD Sync Utility to read the domain.

# Active Directory Connection: Scenario 1



%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs

```
11:23:12.222 AM      Information [Th 14] Configuring secure Active Directory connection through LDAP
11:23:12.222 AM      Information [Th 14] Checking to see if we have stored credentials for LDAP.
11:23:12.222 AM      Information [Th 14] Using: C:\ProgramData\Sophos\Sophos Cloud AD Sync\LDAPCredentials.dat
11:23:12.222 AM      Information [Th 14] LDAP credentials were restored from a file and decrypted successfully.
11:23:12.238 AM      Information [Th 14] Creating LDAP connection to host UK-DC01.ad.trainingdemo.xyz
11:23:12.300 AM      Error [Th 14] Active Directory synchronization failed.
Reason: SophosCloudADSyncLib.NeedADCredsException: The supplied credential is invalid. ---> System.DirectoryServices.Protocols.LdapException: The supplied credential is invalid.
```

SOPHOS

Let's have a quick look in the log file. The error we find here is also indicating an issue with the supplied credentials.

# Active Directory Connection: Scenario 1



The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with the 'Sophos Cloud AD Sync' log selected. The main pane shows a list of events under 'Sophos Cloud AD Sync'. One event is highlighted, showing an 'Error' level entry from 11/07/2022 11:23:12. The details pane below shows the event's properties, including the error message: 'Active Directory synchronization failed. Reason: SophosCloudADSyncLib.NeedADCredsException: The supplied credential is invalid.' A tooltip is overlaid on the error message, highlighting the phrase 'The supplied credential is invalid.' in orange.

Level	Date and Time	Source
Error	11/07/2022 11:23:12	Sophos AD Sync
Information	11/07/2022 11:23:11	Sophos AD Sync
Information	11/07/2022 11:23:11	Sophos AD Sync
Information	11/07/2022 11:23:11	Sophos AD Sync

Event 0, Sophos AD Sync

General Details

Active Directory synchronization failed. Reason: SophosCloudADSyncLib.NeedADCredsException: The supplied credential is invalid.

Reason:

SophosCloudADSyncLib.NeedADCredsException: **The supplied credential is invalid.**

System.DirectoryServices.Protocols.LdapException: **The supplied credential is invalid.**

Log Name: Sophos Cloud AD Sync  
Source: Sophos AD Sync  
Event ID: 0  
Level: Error  
User: N/A

Logged: 11/07/2022 11:23:12  
Task Category: (3)  
Keywords: Classic  
Computer: UK-DC01.ad.trainingdemo.wz

Actions

- Sophos Cloud AD Sync
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties

Here is what you would see if you checked the Windows Event Viewer logs.

# Active Directory Connection: Scenario 1



The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view of the domain structure is visible, including 'ad.trainingdemo.xyz' and various organizational units like 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Training Demo', and 'Users'. In the center, a list of users is shown with columns for 'Name', 'Type', and 'Description'. A context menu is open over a user account named 'STAS'. The 'Reset Password...' option is highlighted with a cursor. To the right, a 'Reset Password' dialog box is displayed, asking for a new password ('New password:' and 'Confirm password:') and providing checkboxes for 'User must change password at next logon' and 'Unlock the user's account'. Buttons for 'OK' and 'Cancel' are at the bottom.

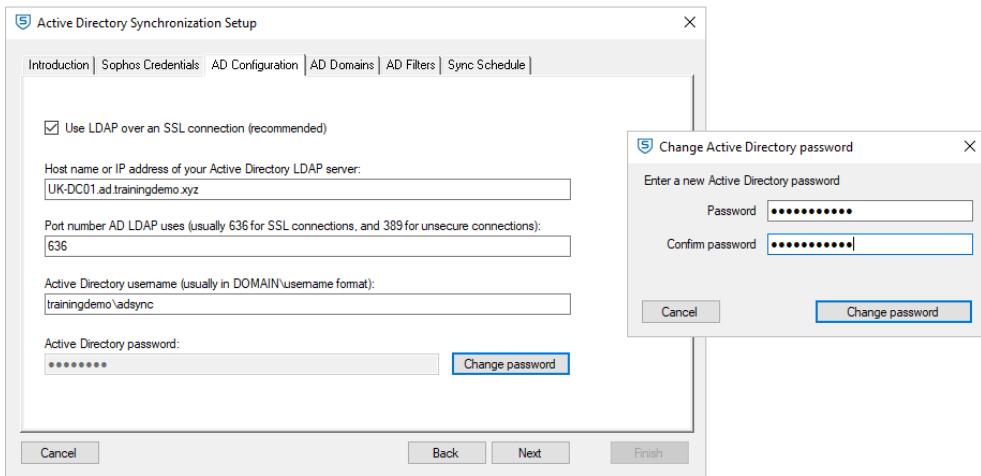
Optionally set the password to never expire for the user

SOPHOS

There are a couple of common causes for this error, usually the password on the user account has expired or been changed. In either case, it is usually advisable to reset the password.

As long as you are using a strong password, you may also want to set the password to never expire for this user account.

# Active Directory Connection: Scenario 1



SOPHOS

Once you have reset the password in Active Directory, you will need to update the password in the AD Sync Utility.

# Active Directory Connection: Scenario 1

3

The screenshot shows the Sophos Central interface with the 'People' section selected. The main table lists users with their names, emails, and synchronization status. A red box highlights the rows for Anne Green, Fred Rogers, Jake Murphy, Jane Doe, and Jo Brown, which are missing from the sync process.

Name	Email	Last Active	Group Name
Anne Green		agree	Marketing (TRAINING)
Fred Rogers		frogers	Support (TRAINING)
Jake Murphy	jakemurphy@trainingdemo.xyz	Add Exchange Login	
Jane Doe		jdoe	Sales (TRAINING)
Jo Brown		jbrown	HR (TRAINING)
		Add Exchange Login	

Once the AD Sync Utility performs its next synchronization with Sophos Central you will see the missing users added.

# Active Directory Connection: Scenario 2

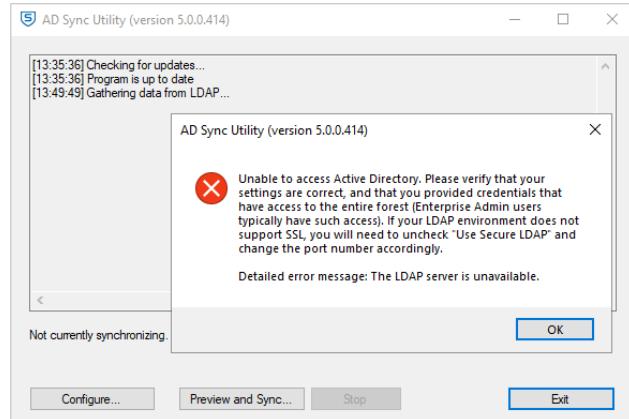


The screenshot shows the Sophos Central interface with the 'People' section selected. The page title is 'People' with the subtitle 'Manage your users'. There are tabs for 'Users' (selected) and 'Groups'. Below are buttons for 'Add', 'Email Setup Link', and 'Delete', along with a 'Search' bar. A green callout box with the text 'New users are not being added to Sophos Central' is overlaid on the right side of the user list table. The table columns include Name, Email, Exchange Login, Last Active, Group Name, and Role. The data rows show several users, including Anne Green, Jake Murphy, and ztna@trainingdemo.xyz.

Name	Email	Exchange Login	Last Active	Group Name	Role
Anne Green	jakemurphy@trainingdemo.xyz	Add Exchange Login		Central Ad...	Super Ad...
Jake Murphy		Exchange Login			Admin
		Add Exchange Login			
	ztna@trainingdemo.xyz	Add Exchange Login			Super Ad...

In this second scenario, users are not being added to Sophos Central.

# Active Directory Connection: Scenario 2



SOPHOS

The first step is always to try and get more information by performing a manual synchronization.

Here the error is indicating that the AD Sync Utility is unable to connect to the domain controller. The message 'The LDAP server is unavailable' suggests that this is a network issue instead of a credentials issue.

## Active Directory Connection: Scenario 2



%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs

```
01:49:49.417 PM      Information [Th 17] Configuring secure Active Directory connection through LDAP
01:49:49.417 PM      Information [Th 17] Checking to see if we have stored credentials for LDAP.
01:49:49.417 PM      Information [Th 17] Using: C:\ProgramData\Sophos\Sophos Cloud AD Sync\LDAPCredentials.dat
01:49:49.417 PM      Information [Th 17] LDAP credentials were restored from a file and decrypted successfully.
01:49:49.417 PM      Information [Th 17] Creating LDAP connection to host UK-DC01.ad.trainingdemo.xyz
01:50:10.543 PM      Error [Th 17] Active Directory synchronization failed.
Reason: SophosCloudADSyncLib.NeedADCredsException: The LDAP server is unavailable. ---> System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable.
```

SOPHOS

We can see the same 'The LDAP server is unavailable' error in the log file.

## Active Directory Connection: Scenario 2



The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists categories like Event Viewer (Local), Custom Views, Windows Logs, Applications and Services Log, and Subscriptions. Under Applications and Services Log, there's a folder for Sophos Cloud AD Sync. The main pane displays a list of events for 'Sophos Cloud AD Sync' with a count of 64 events. One specific event is selected, showing its details. The 'General' tab of the event details window contains the following error message:

```
Active Directory synchronization failed. Reason: SophosCloudADSyncLib.NeedADCredsException: The LDAP server is unavailable.
System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable.
at System.DirectoryServices.Protocols.LdapConnection.Connect()
at System.DirectoryServices.Protocols.LdapConnection.BindHelper(NetworkCredential newCred)
at SophosCloudADSyncLib.LdapSearchCommand.Bind(SecureString userName, SecureString pa
--- End of inner exception stack trace ---
at SophosCloudADSyncLib.LdapSearchCommand.Bind(SecureString userName, SecureString pa
at SophosCloudADSyncLib.LdapSearchCommand..ctor(String host, Int32 port, String ldapUserN
Boolean initSearchBases, HashSet`1 dnsTolgnore, HashSet`1 dnsTolclude, Int32 timeoutInSecond
at SophosADSync.GetChangesCmd.SyncExImpl(Object runtimeArg)
at CommandLib.Command.BaseSyncExecute(Object runtimeArg, Command owner)
at SophosADSync.ADSyncCommand.GetLDAPData()
at SophosADSync.ADSyncCommand.SyncExImpl(Object runtimeArg)
```

The 'Details' tab shows the following log information:

Log Name:	Sophos Cloud AD Sync
Source:	Sophos AD Sync
Event ID:	0
Logged:	11/07/2022 13:50:10
Task Category:	(3)

A large blue callout box highlights the error message from the event details window.

Here is the error you would see in the Event Viewer for this scenario.

## Active Directory Connection: Scenario 2



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jsmith> Test-NetConnection -ComputerName uk-dc01.ad.trainingdemo.xyz -Port 636
WARNING: TCP connect to (172.16.16.10 : 636) failed

ComputerName      : uk-dc01.ad.trainingdemo.xyz
RemoteAddress     : 172.16.16.10
RemotePort        : 636
InterfaceAlias    : Ethernet0
SourceAddress     : 172.16.16.20
PingSucceeded     : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded   : False

PS C:\Users\jsmith>
```

SOPHOS

As the error indicates an issue connecting to the domain, we can use the `Test-NetConnection` command in PowerShell. This should be run on the device that has the AD Sync Utility tool installed.

In the example shown here we are using port 636, which is used for secure LDAP connections. This is recommended. If you are not using a secure LDAP connection the port would be 389. If you are unsure, you can check your configuration in the AD Sync Utility.

Here you can see that the connection failed.

# Active Directory Connection: Scenario 2



The screenshot shows the Sophos Firewall interface for editing a firewall rule. The left sidebar has sections for MONITOR & ANALYZE (Control center, Current activities, Reports, Zero-day protection, Diagnostics), PROJECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection), and CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services). The SYSTEM section at the bottom includes Sophos Central and Firewall.

The main area is titled "Edit firewall rule" and shows "Destination and services". It lists "Destination zones \*": LAN and "Destination networks \*": Any. Under "Services \*", it lists NTP, RDP, SAMBA, SIP, SIP-MSN messenger, SSH, and ldap. A dropdown menu shows "All types" with checkboxes for Any, LDAP (checked), and LDAPS (checked). A green button at the bottom right says "Apply 2 selected items".

Assuming that the domain controller is running, you may find that there is something like a firewall on the route to the domain controller that is blocking the connection.

Consider if there have been any network changes recently that may have caused this.

Here we can see that a firewall rule is missing the LDAP and secure LDAP services.

## Active Directory Connection: Scenario 2



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jsmith> Test-NetConnection -ComputerName uk-dc01.ad.trainingdemo.xyz -Port 636

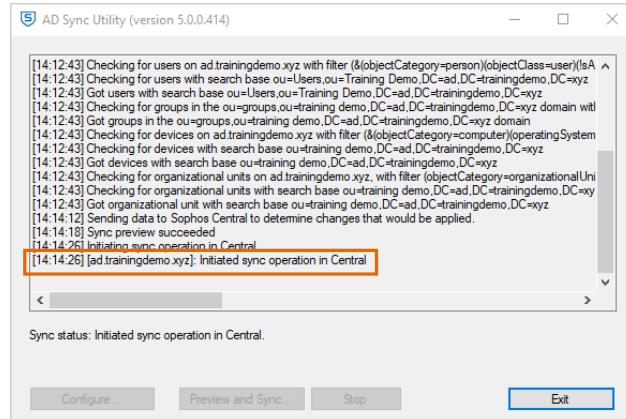
ComputerName      : uk-dc01.ad.trainingdemo.xyz
RemoteAddress    : 172.16.16.10
RemotePort       : 636
InterfaceAlias   : Ethernet0
SourceAddress    : 172.16.16.20
TcpTestSucceeded : True

PS C:\Users\jsmith> -
```

SOPHOS

After adding the services to the firewall rule, the `Test-NetConnection` command shows that the domain controller is accessible again.

# Active Directory Connection: Scenario 2



SOPHOS

Initiating a manual synchronization in the AD Sync Utility we can see that it is successful.

# Active Directory Connection: Scenario 2



The screenshot shows the Sophos Central interface with the 'People' section selected. A table lists users with their names, emails, exchange logins, last active times, and group names. A red box highlights the rows for Anne Green, Fred Rogers, Jake Murphy, Jane Doe, and Jo Brown, indicating they have been synchronized. The table has columns for Name, Email, Exchange Login, Last Active, and Group Name.

Name	Email	Exchange Login	Last Active	Group Name
Anne Green		agreeen		Marketing (TRAINING)
Fred Rogers		frogers		Support (TRAINING)
Jake Murphy	jakemurphy@trainingdemo.xyz	Add Exchange Login		
Jane Doe		jdoe		Sales (TRAINING)
Jo Brown		jbrown		HR (TRAINING)
		Add Exchange Login		

Once the synchronization is complete you will see the missing users added.

# Filter Configuration

SOPHOS

The last type of issue is for filter configuration, and we will look at two examples.

# Filter Configuration: Scenario 1



The screenshot shows the Sophos Central 'People' management interface. On the left, a sidebar lists various product categories like Endpoint Protection, Server Protection, and Email Security. The 'People' section is selected. The main area is titled 'People: Manage your users' and contains tabs for 'Users' and 'Groups'. Below these are buttons for 'Add', 'Email Setup Link', and 'Delete'. A dropdown menu shows 'All users' and a search bar with placeholder 'Search'. A green callout box points to the 'Add Exchange Login' button next to a user entry for 'John Smith'. The user table lists several entries, each with columns for Name, Email, Exchange Login, Last Active, and Group Name. A note at the bottom states '1 - 7 of 7 users/0 selected'.

Name	Email	Exchange Login	Last Active	Group Name
John Smith		jsmith	Jul 11, 2022 1:14 PM	Sales (TRAIL)
[Redacted]				Central Adm
[Redacted]				Central Adm
Jake Murphy	jakemurphy@trainingdemo			
[Redacted]				Add Exchange Login
[Redacted]	ztna@trainingdemo.xyz			Add Exchange Login
[Redacted]				Add Exchange Login

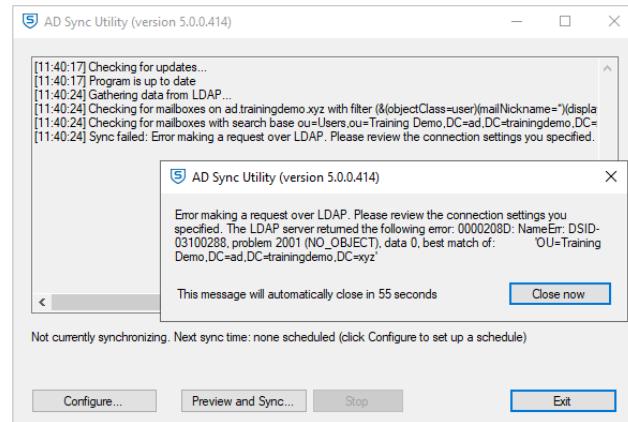
1 - 7 of 7 users/0 selected

Last updated: Jul 12, 2022, 9:59 AM

Users are missing from Sophos Central

In this scenario, users are not being added to Sophos Central.

# Filter Configuration: Scenario 1



SOPHOS

Manually starting a synchronization in the AD Sync Utility, we see the message 'Error making a request over LDAP. Please review the connection settings you specified'. This indicates a configuration error.

## Filter Configuration: Scenario 1



%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs

```
11:40:24.978 AM      Information [Th 38] Checking for mailboxes with search base
ou=Users,ou=Training Demo,DC=ad,DC=trainingdemo,DC=xyz
11:40:24.978 AM      Information [Th 38] Searching LDAP under
ou=Users,ou=Training Demo,DC=ad,DC=trainingdemo,DC=xyz for
(&(objectClass=user)(mailNickname=*)(displayName=*)(!cn=HealthMailbox*)(proxyAdd
resses=*)(msExchDelegateListLink=*)(userAccountControl:1.2.840.113556.1.4.803:=2
)(|(|(homeMTA=*)(homeMDB=*)(msExchHomeServerName=*))(&(objectClass=contact)(targ
etAddress=*)))).
11:40:24.978 AM      Error [Th 38] Active Directory synchronization failed.
Reason: SophosCloudADSyncLib.DisplayableException: Error making a request over
LDAP. Please review the connection settings you specified. The LDAP server
returned the following error: 0000208D: NameErr: DSID-03100288, problem 2001
(NO_OBJECT), data 0, best match of:      'OU=Training
Demo,DC=ad,DC=trainingdemo,DC=xyz'
```

SOPHOS

You will see the same error in the log file.

# Filter Configuration: Scenario 1



The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane lists various logs like Custom Views, Windows Logs, Applications and Services Log, Forefront Identity Manager, and Microsoft logs. The main pane displays a list of events under the 'Sophos Cloud AD Sync' log, with a total of 352 events. One specific event is selected, which is an Error event with ID 0. The event details show the following message:  
Active Directory synchronization failed. Reason: SophosCloudADSyncLib.DisplayableException: Error making a request over LDAP. Please review the connection settings you specified. The LDAP server returned problem 2001 (NO\_OBJECT), data 0, best match of:  
'OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz'  
---> System.DirectoryServices.Protocols.DirectoryOperationException: The object at System.DirectoryServices.Protocols.LdapConnection.ConstructResponse(Int32 resultType, TimeSpan requestTimeOut, Boolean exceptionOnTimeOut)  
at System.DirectoryServices.Protocols.LdapConnection.SendRequest(DirectoryRe...  
The event also includes the following metadata:  
Log Name: Sophos Cloud AD Sync  
Source: Sophos AD Sync  
Event ID: 0  
Level: Error  
User: N/A  
OpCode:  
More Information: [Event Log Online Help](#)  
The right pane contains an 'Actions' menu with options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., and Filter Current Log... . A tooltip box is overlaid on the right side of the event details, containing the error message text.

And in the Event Viewer.

# Filter Configuration: Scenario 1



The screenshot shows two windows side-by-side. On the left is the 'Define Filters for TRAININGDEMO' window in the AD Sync Utility. It has tabs for 'Users', 'User Groups', 'Devices', 'Organizational Units', and 'Public Folders'. Under 'Search bases (all items below will be searched when discovering users):', the value 'ou=Users,ou=Training Demo,DC=ad,DC=trainingdemo,DC=xyz' is entered and highlighted with a red box. Below this, under 'Additional LDAP filters to be applied when discovering Active Directory users to sync. Any filters you specify below will be in addition to the following defaults:', there is a checkbox for 'Exclude disabled user accounts (userAccountControl:1.2.840.113556.1.4.803:=2)' which is checked. A second red box highlights the LDAP filter '(memberof=cn=uk\_users,ou=groups,ou=training demo,dc=ad,dc=trainingdemo,dc=xyz)'. At the bottom is a 'Reset User Filters to Defaults' button. On the right is the 'Active Directory Users and Computers' snap-in. The left pane shows the navigation tree with nodes like 'Saved Queries', 'ad.trainingdemo.xyz', 'Training Demo', 'Groups', and 'Demo Users'. The right pane lists objects by name, type, and description. The 'Demo Users' node in the tree is also highlighted with a red box.

SOPHOS

In the AD Sync Utility tool configuration, check that the search bases for each of the types of objects being synchronized are correct and valid.

In this scenario, the search base does not match the Active Directory. This may happen if an organization unit is renamed or moved.

You can choose whether to rename the OU or update the search base to be correct.

# Filter Configuration: Scenario 1

3

The screenshot shows the Sophos Central 'People' management interface. On the left, a sidebar lists various product categories like Endpoint Protection, Server Protection, and Email Security. The 'People' section is selected and highlighted in blue. The main area is titled 'People: Manage your users' and contains tabs for 'Users' and 'Groups'. Below these are buttons for 'Add', 'Email Setup Link', and 'Delete'. A dropdown menu shows 'All users' and a search bar with a placeholder 'Search'. The main table lists users with columns for Name, Email, Exchange Login, Last Active, and Group Name. An orange box highlights the rows for Anne Green, Fred Rogers, Jake Murphy, Jane Doe, and Jo Brown, all of whom have their 'Exchange Login' status set to 'agree'. Other users listed include 'Central Admin' and 'Support (TRAIL)'. At the bottom right of the table, there is a link 'Add Exchange Login'.

Name	Email	Exchange Login	Last Active	Group Name
Central Admin	[REDACTED]	Add Exchange Login		Central Admin
Central Admin	[REDACTED]	Add Exchange Login		Central Admin
Anne Green	[REDACTED]	agree		Marketing (TRAIL)
Fred Rogers	[REDACTED]	frogers		Support (TRAIL)
Jake Murphy	jakemurphy@trainingdemo.xyz	Add Exchange Login		
Jane Doe	[REDACTED]	jdoe		Sales (TRAIL)
Jo Brown	[REDACTED]	jbrown		HR (TRAINING)
	[REDACTED]	Add Exchange Login		

Once the AD Sync Utility performs its next synchronization with Sophos Central you will see the missing users added.

# Filter Configuration: Scenario 2



The screenshot shows the Sophos Central interface with the 'People' section selected. The main area displays a list of users with columns for Name, Email, Exchange Login, Last Active, and Group Name. A green callout box with the text 'Users are missing from Sophos Central' points to the list. The left sidebar includes sections for Dashboard, Alerts, Threat Analysis Center, Logs & Reports, Devices, Global Settings, Third-party Connectors, Protect Devices, Account Health Check, and MY PRODUCTS (Endpoint Protection, Server Protection, Mobile, Encryption, Wireless, Email Security).

Name	Email	Exchange Login	Last Active	Group Name
John Smith	jsmith		Jul 11, 2022 1:14 PM	Sales (TRAIL)
Jake Murphy	jakemurphy@trainingdemo			
	ztna@trainingdemo.xyz	Add Exchange Login		Central Adm
		Add Exchange Login		Central Adm

In this second scenario, users are not being added to Sophos Central.

## Filter Configuration: Scenario 2



Pending Changes

Users to Add (0) Users to Delete (0) Users to Modify (0) Groups to Add (0) Groups to Delete (0) Groups to Modify (0) Devices to Add (0) Devices to Delete (0) Devices to Modify (0) Organizational Units to Add (0) Organizational Units to Delete (0)

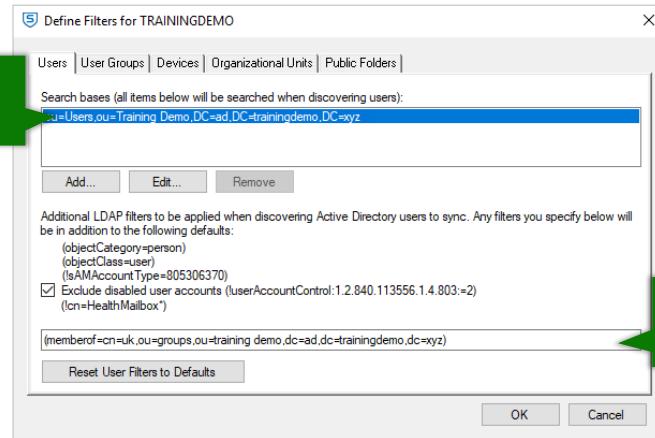
No users will be added.

Approve Changes and Continue Reject Changes and Stop

SOPHOS

When you try to do a manual synchronization, it works without any errors; however, it is not showing the missing users that should be added to Sophos Central.

# Filter Configuration: Scenario 2



SOPHOS

You will need to check the configuration, both the search bases and the LDAP filters.

## Filter Configuration: Scenario 2



The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the tree view shows various organizational units (OUs) under 'ad.trainingdemo.xyz'. A specific OU, 'Training Demo', is expanded, and its 'Users' container is selected, highlighted with a red box. On the right, the 'Properties' window for this OU is open, specifically the 'General' tab. In the 'Search bases' field, the value 'ou=Users,ou=Training Demo,dc=ad,dc=trainingdemo,dc=xyz' is entered and highlighted with a red box. Below this, in the 'Attributes' list, the 'distinguishedName' attribute is set to 'OU=UK Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz', also highlighted with a red box. The bottom of the window contains standard 'OK', 'Cancel', 'Apply', and 'Help' buttons.

When considering search bases, you may find that the current set of search bases is incomplete. Here we can see that there is a single search base, but the users are being created in two locations in Active Directory.

There are a couple of ways you can update the configuration to work in this scenario, as you could use a broader search base, or add the other OU as an additional search base.

## Filter Configuration: Scenario 2



Name	Type	Description
Finance	Security Group...	
HR	Security Group...	
IT	Security Group...	
Marketing	Security Group...	
Sales	Security Group...	
Support	Security Group...	
Training	Security Group...	
<b>UK Users</b>	Security Group...	
US	Security group...	
ZTNA_ALL	Security Group...	

SOPHOS

Another possibility is an error with your LDAP filter. Assuming that it had been working when AD Sync Utility was initially installed, it may be that something has been moved or renamed in Active Directory so that it no longer matches.

In the example shown here, the 'UK' group has been renamed to 'UK Users' and the filter needs to be updated to reflect this.

## Filter Configuration: Scenario 2



Pending Changes

Users to Add (5) Users to Delete (0) Users to Modify (0) Groups to Add (0) Groups to Delete (0) Groups to Modify (7) Devices to Add (0) Devices to Delete (0) Devices to Modify (0) Organizational Units to Add (0) Organizational Units to De [ ]

The following 5 users will be added to Sophos Central.

Name	Email	Distinguished Name
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
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
Sara Baker		CN=Sara Baker,OU=Training,OU=Users,OU=Training Demo,DC=ad,DC=trainingdemo,DC=xyz

Approve Changes and Continue Reject Changes and Stop

SOPHOS

With the configuration updated, a manual synchronization will show the missing users that need to be added to Sophos Central.

# Filter Configuration: Scenario 2

3

The screenshot shows the Sophos Central interface with the 'People' section selected. A green box highlights the list of users under the 'Central Admin' group. The users listed are Anne Green, Fred Rogers, Jake Murphy, Jane Doe, and Jo Brown. Each user has a status indicator (green for Jake Murphy, yellow for the others) and a 'Last Active' timestamp.

Name	Last Active	Group Name
Anne Green	agree	Marketing (TRAINING)
Fred Rogers	frogers	Support (TRAINING)
Jake Murphy	jakemurphy@trainingdemo.xyz	Add Exchange Login
Jane Doe	jdoe	Sales (TRAINING)
Jo Brown	jbrown	HR (TRAINING)

Once the synchronization is complete you will see the missing users added.

## Filter Behaviour



Changing a group filter has no effect on which users will be discovered and added to Sophos Central.



Changing a user filter has no effect on which groups will be discovered and added to Sophos Central.



AD Sync will delete Sophos Central users and groups that are no longer present in search results (except admins).



Changing a filter could result in the deletion of many users and groups from Sophos Central.

SOPHOS

Let's review how the LDAP filters work.

Changing a group filter has no effect on which users will be discovered and added to Sophos Central, and changing a user filter has no effect on which groups will be discovered and added to Sophos Central.

AD Sync Utility will delete Sophos Central users and groups that are no longer present in search results, **except for users configured with administrator roles**.

Changing a filter could result in the deletion of many users and groups from Sophos Central.

# Symptoms of Synchronization Problems

New users, groups, and devices not being added

Existing users, groups, and devices disappearing

Policies not being applied as expected

SOPHOS

Throughout this chapter we have used the same symptom so that we can focus on the troubleshooting process; however, there are a few symptoms you might notice.

We focused on new users not being added, but it could also be groups or devices.

In the case of misconfigured filters, you could notice that existing users, groups, or devices have been removed from Sophos Central.

You might notice that policies are not being applied as expected. A little further digging might reveal that this is due to some groups no longer being synchronized.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 3

What is the recommended first step when troubleshooting AD Sync Utility issues?

Check the API credentials

Test the connection to the domain controller

Initiate a manual synchronization

Review the filter configuration

SOPHOS



## Question 2 of 3

**True or False:** All issues will cause an error when you initiate a manual synchronization.

True

False

SOPHOS



## Question 3 of 3

What PowerShell command can you use to test the connection to the domain controller from the computer with AD Sync Utility installed? Enter the name of the command only with no additional parameters.

SOPHOS

# Chapter Review

The first troubleshooting step is to initiate a **manual synchronization** to see if there is an error that can provide more information. You can also check the **log files** and the **event viewer** for details of errors that have occurred.

AD Sync Utility uses **API credentials** to connect to Sophos Central. If these **expire**, are **deleted**, or have the wrong **role** you will need to create new API credentials. AD Sync Utility uses a **domain user** to **read** the domain, if the **password** has **expired** or **changed** you will need to reset it.

Issues with **filter configuration** do not always show an error during synchronization. Issues can be caused by changes made in Active Directory. Review both the **search bases** and the **LDAP filter** configuration.

SOPHOS

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

The first troubleshooting step is to initiate a manual synchronization to see if there is an error that can provide more information. You can also check the log files and the event viewer for details of errors that have occurred.

AD Sync Utility uses API credentials to connect to Sophos Central. If these expire, are deleted, or have the wrong role you will need to create new API credentials. AD Sync Utility uses a domain user to read the domain, if the password has expired or changed you will need to reset it.

Issues with filter configuration do not always show an error during synchronization. Issues can be caused by changes made in Active Directory. Review both the search bases and the LDAP filter configuration.



# Advanced Directory Synchronization in Sophos Central

Sophos Central Endpoint & Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE1025: Advanced 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.

# Advanced Directory Synchronization in Sophos Central

In this chapter you will learn how to customize directory synchronization using filters.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Be able to install AD Sync Utility for Windows Active Directory synchronization
- ✓ Be able to configure Azure AD for synchronization

DURATION      **11 minutes**

SOPHOS

In this chapter you will learn how to customize directory synchronization using filters.



Additional information in  
the notes

# Windows Active Directory Synchronization



Uses API credentials with the  
**Service Principal Directory Sync** role



The **user** connecting to Active Directory only  
needs **read** access



AD Sync Utility can synchronize for **multiple domains** in a forest  
**Unrelated domains** require **separate** installations of AD Sync Utility



We recommend scheduling synchronization **daily**

SOPHOS

Windows Active Directory synchronization is achieved using the AD Sync Utility, which uses API credentials with the service principle directory sync role to connect to your Sophos Central account. The user that you configure AD Sync Utility to use for Active Directory access only needs to have read access to the directory, and this is included in the default user permissions for all Active Directory users.

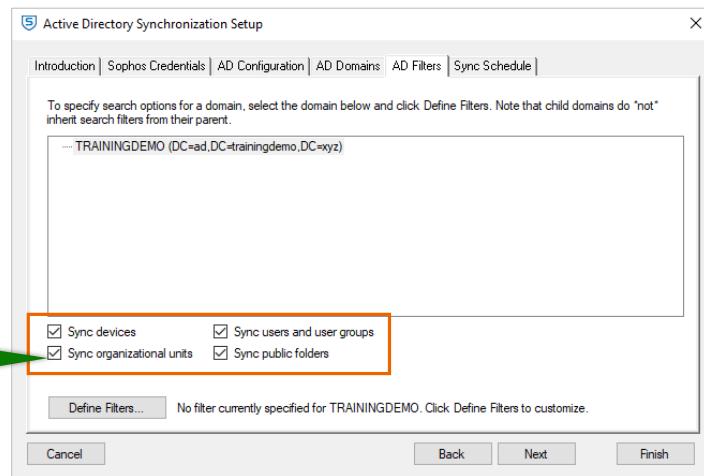
The AD Sync Utility can synchronize users for multiple domains in a forest; however, for unrelated domains you will require separate installations of AD Sync Utility.

We recommend that AD Sync Utility is configured to synchronize users daily.

## [Additional Information]

Default permissions for a user in Active Directory: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions>

# Windows Activity Directory Sync Options



SOPHOS

AD Sync Utility can synchronize five types of object from Active Directory:

- Users
- User groups
- Devices
- Organization units, which are imported as device groups in Sophos Central
- Public folders

To maintain the link between the association between the organization units and devices you should have both enabled when synchronizing devices.

# Windows Active Directory Synchronization

The screenshot shows the Sophos Central interface with the 'Active Directory Config' page open. The left sidebar 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, Mobile, Encryption, Wireless, Email Security, and Firewall Management. The main content area displays the 'Active Directory Config' settings. It shows the 'Directory type' as 'Active directory', 'Status' as 'Synchronized successfully Nov 24, 2022 5:15 PM', and provides a summary of synchronized objects: 11 Users (4), User groups (58), Devices (7), Device groups (2), Public folders (0), Shared mailboxes (0). It also lists the 'Domain' as 'ad.trainingdemo.xyz', 'Client hostname' as 'WinServer1', and 'Client version' as '5.0.2.71'. Action buttons include 'Turn off', 'Download installer', 'Synchronize', and 'Purge data'. The 'Name' field is set to 'AD\_AD.TRAININGDEMO.XYZ' and the 'Description' field is 'AD\_AD.TRAININGDEMO.XYZ'.

Once you have installed and configured AD Sync Utility with the basic settings you can see the users and groups that it is synchronizing. By default, AD Sync Utility will synchronize all users and groups in the domain.

# Device Groups

The screenshot shows the Sophos Central interface for managing server groups. The left sidebar is dark-themed with white text, showing the navigation menu:

- SOPHOS
- Server Protection
- ANALYZE
  - Dashboard
  - Logs & Reports
- MANAGE PROTECTION
  - Servers** (highlighted)
  - Policies
  - Settings
  - Protect Devices
- MORE PRODUCTS
  - Free Trials

The main content area has a light background and displays the "Server Protection - Server Groups" section. At the top, there are tabs: Servers, Unmanaged servers, and Server Groups (which is selected). Below the tabs are buttons for Add Server Group, Move, and Delete.

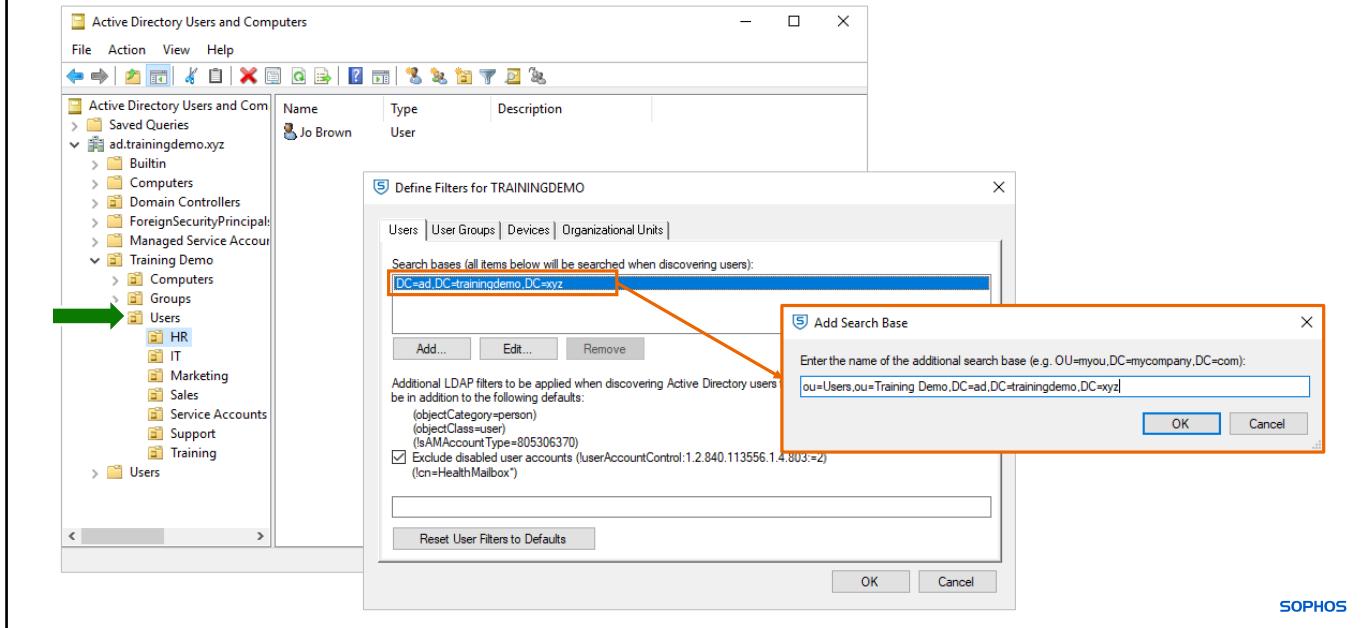
A search bar labeled "Search" is located at the top right. The main list shows the following organization units:

Name (Nested Groups)	Servers	Description
Azure VMs	0	A...
Domain Controllers (OU=Domain Controllers,DC=AD,DC=TRAININGDEMO,DC=XYZ) (1)	1	
Linux Servers	0	
Member Servers 1	0	
New York Office	1	
Reading Office	4	

At the bottom of the list, it says "1 - 8 of 8 top level groups / 0 selected". There are navigation arrows and a page number indicator (1). On the far right, it says "Last updated: Nov 24, 2022, 5:18 PM" and has a refresh icon.

Here you can see organization units that have been imported into Sophos Central. These will be available as both server groups and computer groups.

# Configuring Search Bases

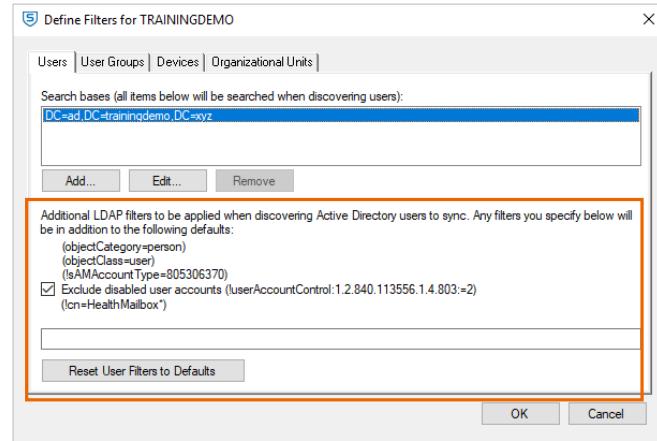


For each of the five object types that you choose to synchronize you can configure a search base. This is the location in Active Directory that AD Sync Utility will synchronize from.

You can define the search base separately for each of the object types, and you can configure multiple search bases.

Here you can see that we are changing the search base for users to be a specific OU, or organization unit, in the domain.

# LDAP Filters



SOPHOS

In addition to defining the search bases, you can configure LDAP filters to further control what is synchronized from Active Directory.

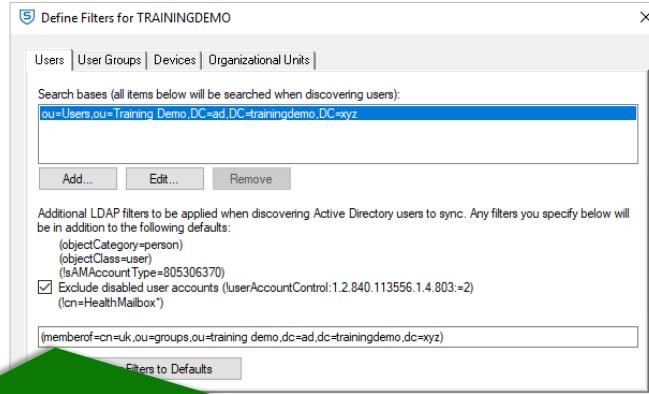
You can see that the default LDAP filters that are applied are shown, and you can optionally choose whether to exclude disabled user accounts. The synchronization of disabled user accounts is important if you use shared mailboxes on Microsoft Exchange, because these shared mailboxes are maintained as disabled user accounts.

Note that LDAP filters are not available for organization units.



Additional information in  
the notes

## LDAP Filters



(memberof=cn=uk,ou=groups,ou=training  
demo,dc=ad,dc=trainingdemo,dc=xyz)

SOPHOS

You can enter your own LDAP filters, which will be applied in addition to the default filters shown. LDAP filters are applied to all search bases for that object type.

In the example shown here we have added an LDAP filter that checks whether users are a member of a specific group. When you write your LDAP filter it should be contained in a set of brackets like the example shown here.

### [Additional Information]

AD Sync Utility filter documentation: <https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithActiveDirectory/ADSyncFilters/index.html>



Additional information in  
the notes

## LDAP Filters

Define Filters for TRAININGDEMO

Search bases (all items below will be searched when discovering users):  
ou=Users,ou=Training Demo,DC=ad,DC=trainingdemo,DC=xyz

Add... Edit... Remove

Additional LDAP filters to be applied when discovering Active Directory users to sync. Any filter(s) entered here will be in addition to the following defaults:  
(objectCategory=person)  
(objectClass=user)  
(isAMAccountType=805306370)  
 Exclude disabled user accounts (userAccountControl:1.2.840.113556.1.4.803:=2)  
(cn=HealthMailbox\*)

(memberof=cn=uk,ou=groups,ou=training demo,dc=ad,dc=trainingdemo,dc=xyz) | (memberof=cn=us,ou=groups,ou=training demo,dc=ad,dc=trainingdemo,dc=xyz)

Filters to Defaults

### Operators

& AND, all conditions must be met  
| OR, any of the conditions must be met  
! NOT, the clause must evaluate to false

( (memberof=cn=uk,ou=groups,ou=training demo,dc=ad,dc=trainingdemo,dc=xyz) | (memberof=cn=us,ou=groups,ou=training demo,dc=ad,dc=trainingdemo,dc=xyz) )

SOPHOS

You can join multiple LDAP filters together using the 'AND' and 'OR' operators.

In the example shown here we are checking for the membership of either the UK or US group by using the 'OR' operator between the two LDAP filters. Notice that each LDAP filter is enclosed in brackets, and the whole string including the 'OR' operator is also enclosed in brackets.

Please note that search bases and filters are defined separately for each domain that you have selected in AD Sync Utility.

### [Additional Information]

More information about the userAccountControl values that can be used is available here:

<https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

### Operator      Meaning

&	AND, all conditions must be met
	OR, any of the conditions must be met
!	NOT, the clause must evaluate to False

# Purge Data

The screenshot shows the Sophos Central interface. On the left sidebar, under 'Global Settings', the 'Active Directory Config' section is selected. The main content area displays the 'Active Directory Config' page with the following details:

Directory type	Active directory	Domain	ad.trainingdemo.xyz
Status	Synchronized successfully Nov 24, 2022 5:15 PM Synchronized 1 Users (4), User groups (58), Devices (7), Device groups (2), Public folders (0), Shared mailboxes (0)	Client hostname	WinServer1
		Client version	5.0.2.71

Below the table are two buttons: 'Synchronize' (blue) and 'Purge data'. To the right of the table, there are three buttons: 'Turn off' (highlighted with a red box), 'Download installer', and a help icon.

You can delete your synchronized Windows Active Directory data using the **Purge data** option. You must **Turn off** the synchronization before you can purge the data.

Please note that managed devices and their associated users or administrators will not be deleted even if they came from Active Directory.

# Purge Data

The screenshot shows the Sophos Central interface. On the left, the 'Global Settings' section is selected under 'Sophos Central'. In the center, the 'Active Directory Config' page is displayed, showing a domain entry for 'ad.trainingdemo.xyz' with a status of 'WinServer1' and version '5.0.2.71'. A 'Purge data' modal window is open over the main content. The modal title is 'Purge data' and it asks 'Purge data for directory AD\_AD.TRAININGDEMO.XYZ ?'. It includes a warning message: 'Purging data resets all your groups, users and associated policies.' and 'If you plan to switch directory type, follow the steps in KBA article'. Below the warning, there's a section titled 'Select the data type you want to purge' with three options: 'All' (selected), 'Users and user groups' (unchecked), and 'Devices and device groups' (unchecked). A note states 'This also purges the data for public folders and mailboxes'. At the bottom of the modal, there are 'Cancel' and 'Purge data' buttons.

Before removing your data, make sure that you don't have any copies of AD Sync Utility set to synchronize the same data, otherwise your data will reappear.

Select the type of data you want to delete. If you select 'All', this will remove any shared mailboxes and public folders.

You must acknowledge that you understand that purging the data cannot be undone by ticking the check box.

To complete the process, click **Purge data**. Clicking this button is confirmation that you want to purge the data.

# AD Sync Utility Logs

```
2022-06-24 - Notepad
File Edit Format View Help
10:31:24.635 AM Information [Th 10] Got public folders with search base DC=ad,DC=trainingdemo,DC=xyz
10:31:24.635 AM Information [Th 10] Checking for users on ad.trainingdemo.xyz with filter (&(objectCategory=person)(objectClass=user)(!sAMAcc
10:31:24.635 AM Information [Th 10] Checking for users with search base DC=ad,DC=trainingdemo,DC=xyz
10:31:24.635 AM Information [Th 10] Searching LDAP under DC=ad,DC=trainingdemo,DC=xyz for (&(objectCategory=person)(objectClass=user)(!sAMAcc
10:31:24.650 AM Information [Th 10] Page:1 contains 15 response entries
10:31:24.650 AM Information [Th 10] Last page detected in LDAP result.
10:31:24.650 AM Information [Th 10] The result set was not paged.
10:31:24.650 AM Information [Th 10] Search returned 15 records.
10:31:24.650 AM Information [Th 10] Got users with search base DC=ad,DC=trainingdemo,DC=xyz
10:31:24.650 AM Information [Th 10] Checking for groups in the DC=ad,DC=trainingdemo,DC=xyz domain with filter (&(objectCategory=group))
10:31:24.650 AM Information [Th 10] Searching LDAP under DC=ad,DC=trainingdemo,DC=xyz for (&(objectCategory=group)).
10:31:24.650 AM Information [Th 10] Page:1 contains 69 response entries
10:31:24.650 AM Information [Th 10] Last page detected in LDAP result.
10:31:24.650 AM Information [Th 10] The result set was not paged.
10:31:24.650 AM Information [Th 10] Search returned 69 records.
10:31:24.650 AM Information [Th 10] Got groups in the DC=ad,DC=trainingdemo,DC=xyz domain
10:31:24.671 AM Information [Th 10] Get all AD entries finished
10:31:24.962 AM Information [Th 10] 15 users
10:31:24.962 AM Information [Th 10] 0 mailboxes
10:31:24.962 AM Information [Th 10] 69 groups
10:31:24.962 AM Information [Th 10] 0 public folders
10:31:24.962 AM Information [Th 10] 84 total records
10:31:24.993 AM Information [Th 10] Sending data to Sophos Central to determine changes that would be applied.
10:31:24.993 AM Information [Th 10] SubmitPreviewSyncData start
10:31:25.009 AM Information [Th 10] Requesting to create a preview sync session with the following payload: {"clientHost":{"hostName":"UK-DCE
10:31:25.009 AM Information [Th 10] The preview sync session creation response: {"createdAt":"2022-06-24T09:31:24.918Z","errors":null,"id":"c
10:31:25.305 AM Information [Th 10] Uploading LDAP data for preview sync
10:31:25.352 AM Information [Th 10] Sync: Compressed JSON from: 35824 bytes, to: 7336 bytes.
10:31:25.681 AM Information [Th 10] SubmitPreviewSyncData finished
10:31:30.771 AM Information [Th 10] Sync preview succeeded
10:33:35.840 AM Information [Th 17] Request received to abort the current sync
10:33:35.840 AM Information [Th 10] Aborted operation.
```

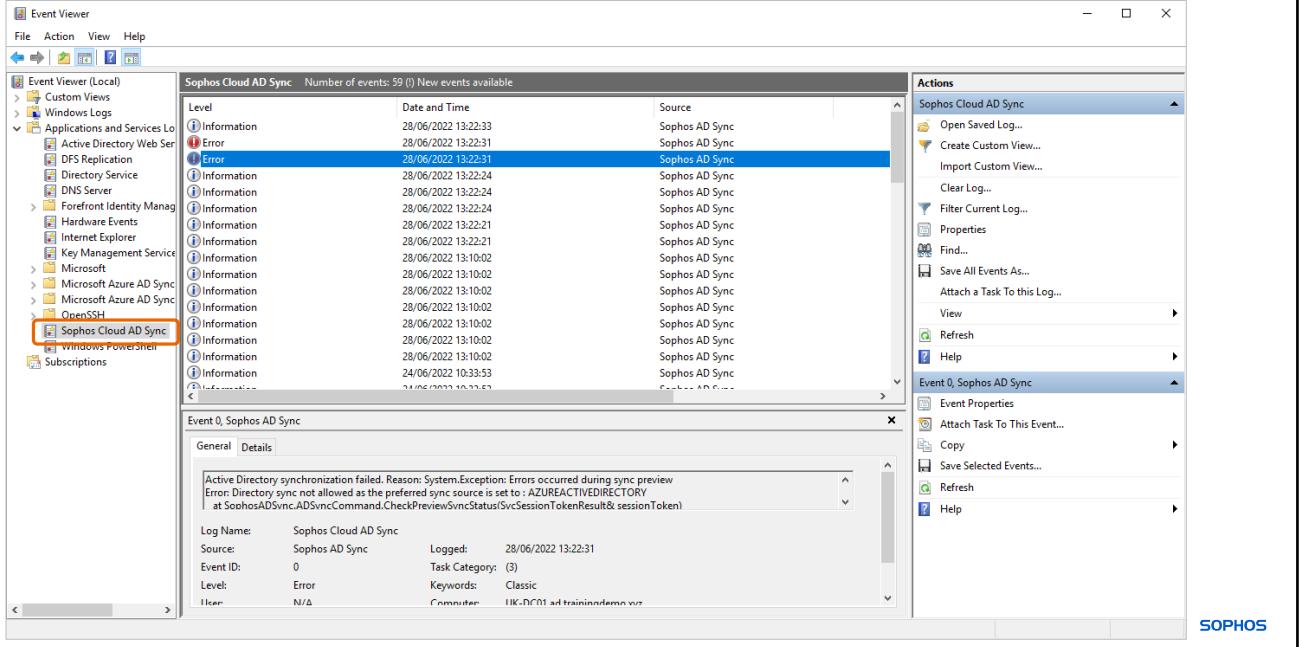
%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs\

SOPHOS

The logs for Windows Active Directory synchronization are located on the device AD Sync Utility is installed on and can be found in folder shown here.

In the logs you can find all the searches the AD Sync Utility is performing to find the users and groups.

# AD Sync Utility Logs



In addition to the log files, the AD Sync Utility also logs to the Windows Event Viewer.

Select **Applications and Services Logs > Sophos Cloud AD Sync** in the left-hand panel to see only events from the AD Sync Utility.

The logging here is less detailed than in the log files, but provides a quick way to spot any errors.

# Azure Active Directory Synchronization



Azure Active Directory can be synchronized in Sophos Central



Sophos Central uses an app registration to access the Azure API



The app registration requires a secret for authentication



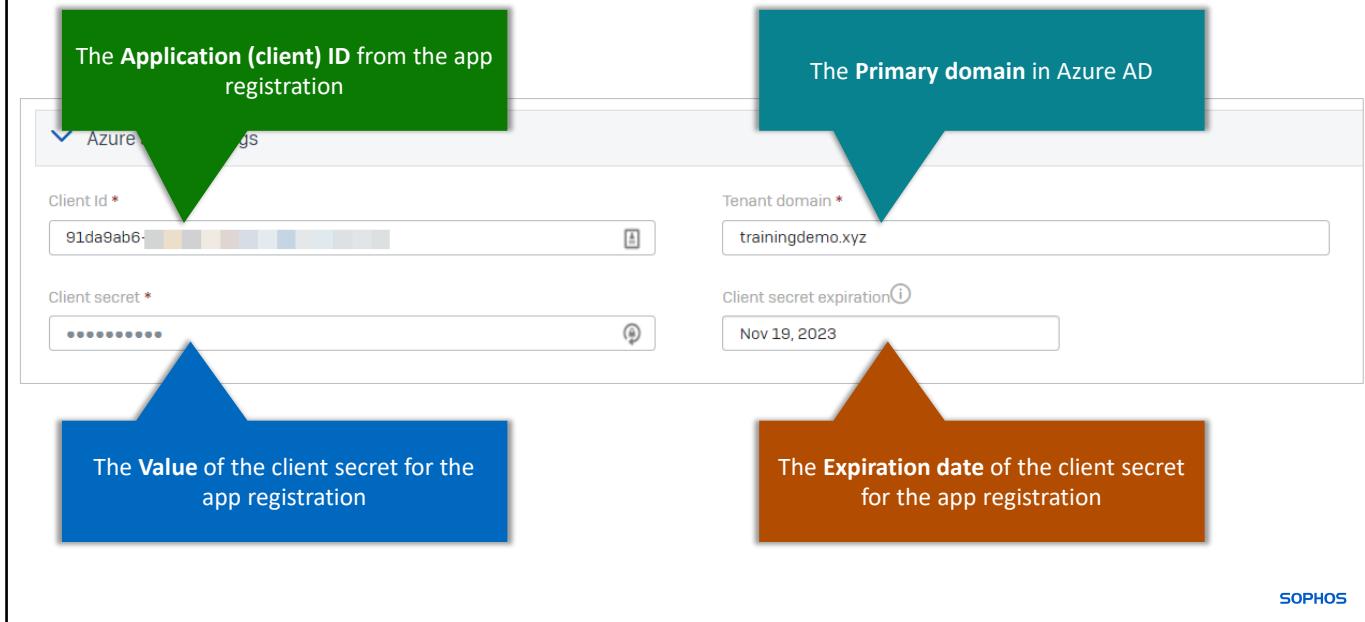
The app registration requires the **Microsoft Graph Directory.Read.All** application API permission

SOPHOS

For Sophos Central to use the Azure Active Directory you must create an app registration in Azure. The app registration will need a secret that Sophos Central will use to authenticate its requests. Within the app registration you need to grant the API permission to Microsoft Graph Directory.Read.All. This should be an application permission and not a delegated permission.

Sophos Central will synchronize users from Azure Active Directory every 6 hours.

# Azure Active Directory Synchronization



To configure Azure AD synchronization in Sophos Central you need the following four pieces of information. The 'Client ID' which is also known as the 'Application ID' that can be found in the app registration in Azure.

The 'Tenant domain' for Azure Active Directory, this is also known as the primary domain in Azure AD.

The 'Client secret' that can be found in the app registration in Azure.

Finally, you will need the client secret expiration date. This is the date the client secret for the app registration will expire.

# Simulation: Azure AD Synchronization



In this simulation you will configure Azure AD synchronization in Sophos Central.

**LAUNCH SIMULATION**

**CONTINUE**

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



Additional information in  
the notes

# Azure Active Directory Users & Groups Filter

The screenshot shows the Sophos Central interface. On the left, there's a sidebar with various navigation options like Overview, Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is currently selected), Third-party Connectors, Protect Devices, and Account Health Check. Below these are sections for MY PRODUCTS: Endpoint Protection, Server Protection, Mobile, and Encryption. In the center, under Global Settings, the 'Directory service' tab is selected. It shows basic sync settings: Type (Azure AD Sync), Auto sync (Every 6 hours), Sync End (Jun 28, 2022 10:43:25 AM), and Status (Successfully synced users and groups). A summary table indicates 14 Users and 9 User Groups. Below this, there are links for 'Setup Azure Application', 'Azure Sync Settings', and a expanded 'Users & Groups Filter' section. The 'All users and groups' option is selected. Other filter modes include 'Add users by group ID', 'Add users by group filter', and 'Add users by user filter'. At the bottom right are 'Sync now', 'Test connection', 'Change directory service?', 'Cancel', 'Save & Sync', and 'Save' buttons.

Here you can see we have Azure AD Sync configured, and we are synchronizing all users and groups. You can see that we currently have 14 users and 9 groups synchronized.

If you are working with a large directory you are likely to want to control which users and groups are synchronized. To do this there are three other filter modes that can be selected.

## [Additional Information]

Azure Active Directory filter documentation: <https://docs.sophos.com/central/Customer/help/en-us/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithAzureAD/AzureADFilters/index.html>

# Add Users by Group ID

The screenshot shows the Sophos Central Admin interface with the 'Global Settings' menu selected. The main content area displays the 'Add Users by Group ID' configuration. At the top right are 'Cancel', 'Save & Sync', and 'Save' buttons. Below them is a 'Setup Azure Application' section with a link to 'Azure Sync Settings'. Under 'Users & Groups Filter', the 'Add users by group ID' option is selected, indicating it will sync all users from selected groups. A table summary shows 7 users and 2 user groups successfully synced. In the 'Groups by ID' section, two group IDs are listed: '6E455700-' and 'C81A731E', each with an 'X' button to remove it.

Type	Azure AD Sync	Users	7
Auto sync	Every 6 hours	User Groups	2
Sync End	Jun 28, 2022 10:46:39 AM		
Status	Successfully synced users and groups		

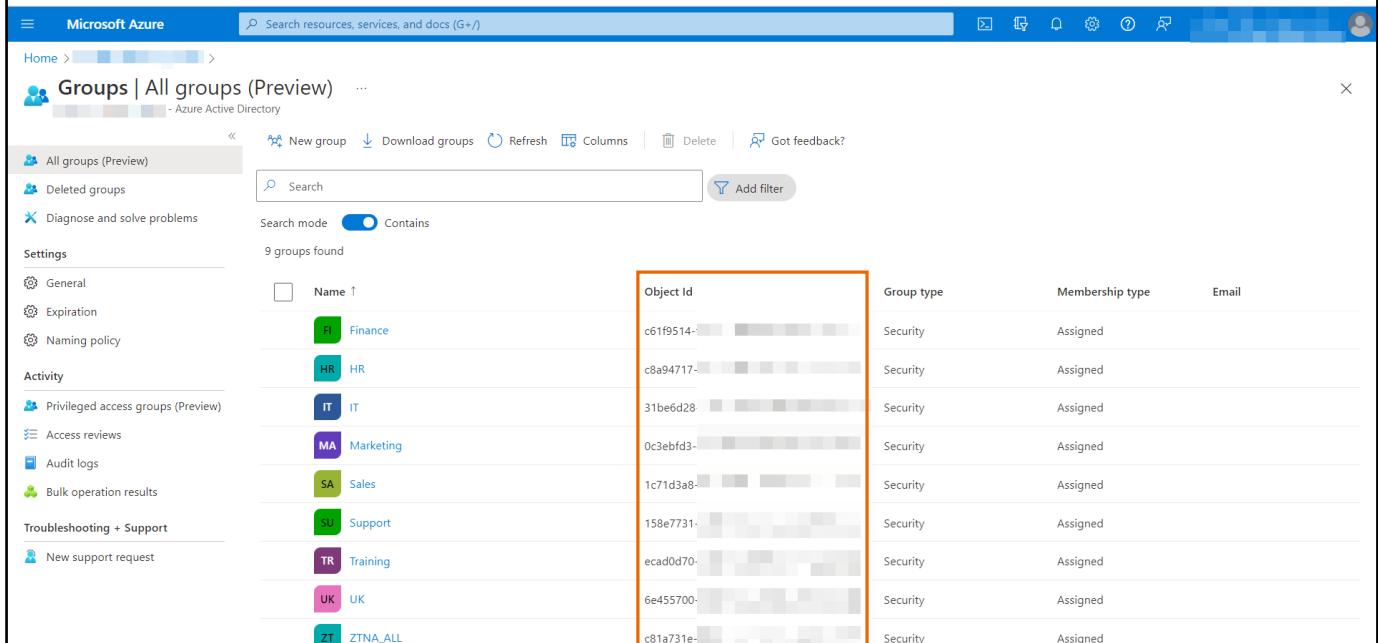
We will start with 'Add users by group ID'.

This is the simplest filter mode, where you add group IDs and only those groups and the users in them are synchronized to Sophos Central.

When you modify the filter settings you will need to first test the connection, then save and synchronize for the changes to take affect.

Here you can see that we are now synchronizing 7 users and 2 groups. The other users and groups that were previously synchronized have been removed from Sophos Central.

# Add Users by Group ID



The screenshot shows the Microsoft Azure Groups page. The left sidebar includes links for Home, Groups (Preview), All groups (Preview), Deleted groups, Diagnose and solve problems, Settings (General, Expiration, Naming policy), Activity (Privileged access groups, Access reviews, Audit logs, Bulk operation results), and Troubleshooting + Support (New support request). The main content area displays a table of groups. A search bar at the top allows filtering by name or object ID. The table columns are Name, Object Id, Group type, Membership type, and Email. Nine groups are listed, each with a unique color-coded icon and name: Finance (green), HR (blue), IT (dark blue), Marketing (purple), Sales (light green), Support (yellow), Training (orange), UK (pink), and ZTNA\_ALL (teal). The 'Object Id' column for these groups is highlighted with a red border.

Name	Object Id	Group type	Membership type	Email
Finance	c61f9514-[REDACTED]	Security	Assigned	
HR	c8a94717-[REDACTED]	Security	Assigned	
IT	31be6d28-[REDACTED]	Security	Assigned	
Marketing	0c3ebfd3-[REDACTED]	Security	Assigned	
Sales	1c71d3a8-[REDACTED]	Security	Assigned	
Support	158e7731-[REDACTED]	Security	Assigned	
Training	ecad0d70-[REDACTED]	Security	Assigned	
UK	6e455700-[REDACTED]	Security	Assigned	
ZTNA_ALL	c81a731e-[REDACTED]	Security	Assigned	

You can find the object IDs for your groups in Azure AD.

# Add Users by Group Filter

The screenshot shows the Sophos Central Admin interface. On the left sidebar, under 'Global Settings', the 'Azure Sync Settings' tab is selected. In the main content area, under 'Users & Groups Filter', there are four filter options:

- All users and groups
- Add users by group ID
- Add users by group filter** (selected)
- Add users by user filter

A table summary is shown on the right:

Type	Azure AD Sync	Users	7
Auto sync	Every 6 hours	User Groups	3
Sync End	Jun 28, 2022 4:10:50 PM		
Status	Successfully synced users and groups		

Below the filters, a complex logic builder titled 'Add groups by matching' is displayed. It shows two nested conditions: 'any' or 'all'. The first 'any' condition has a single condition: 'Display name starts with S'. The second 'any' condition has a single condition: 'Display name starts with U'. There are 'Add condition' and 'Add group' buttons at the top right of the builder.

The next filter is 'Add users by group filter'.

In this mode you create a filter that selects the groups based on criteria. Then only these groups and the users in them are synchronized.

The matching criteria for the group can be configured into quite complex expressions using and, or logic.

You can create a simple filter by matching on either all or any conditions that you select, or you can create more complex filters by creating groups of conditions, each of which can either require any or all the conditions to match.

Group matching conditions include but is not limited to: Azure AD sync enable, Display name, Email, Security enabled, and Object ID. Depending on the condition you select the matching data will change.

Here you can see we are now synchronizing 7 users and 3 groups.

# Add Users by User Filter

The screenshot shows the Sophos Central Global Settings interface under the 'Azure Sync Settings' section. On the left, there's a sidebar with various product categories like Endpoint Protection, Server Protection, and Email Security. The main area displays a 'Users & Groups Filter' configuration. Under 'Add users by matching', there are two filter expressions: one for France and one for the United Kingdom, both set to 'Member' user type. To the right, a table summarizes the sync results:

Type	Azure AD Sync	Users	3
Auto sync	Every 6 hours	User Groups	9
Sync End	Jun 28, 2022 4:36:23 PM		
Status	Successfully synced users and groups		

The last filter type is 'Add users by user filter'.

This filter mode operates in a very similar way to the previous example in the way that you construct the filter expressions. This filter type will synchronize all the matching users and any groups they are a member of.

User matching conditions include but is not limited to: Country, Given name, Surname, Account enabled, User type, Email, and Department.

Here you can see we are now synchronizing 3 users and 9 groups.

# Changing Filter Type

The screenshot shows the Sophos Central Admin interface. On the left, there's a sidebar with various navigation options like Overview, Dashboard, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected), Third-party Connectors, Protect Devices, Account Health Check, and sections for MY PRODUCTS (Endpoint Protection, Server Protection, Mobile, Encryption). The main area shows a 'Setup Azure Application' configuration screen with tabs for 'Azure Sync Settings' and 'Users & Groups Filter'. A 'Confirmation' dialog box is overlaid on the screen, containing the message: 'By changing the filter type you will lose all the existing filter criteria. Do you want to proceed?'. There are 'Cancel' and 'Yes' buttons at the bottom of the dialog. In the background, under the 'Users & Groups Filter' tab, there are four filter options: 'All users and groups', 'Add users by group ID', 'Add users by group filter' (which is selected), and 'Add users by user filter'. Below this, there's a 'Groups by ID' section with a table showing two entries: 'Group ID' 2 with object ID '6E455700-' and 'Group ID' 1 with object ID 'C81A731E-i'.

You can change the filter type, however, when you change the filter type, all of your existing filter criteria settings are lost.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 4

**True or False:** A single installation of AD Sync Utility can synchronize multiple domains that are in the same forest.

True

False

SOPHOS

## Question 2 of 4

Which LDAP operator would you use when you want two LDAP filters to be true?

&

!

|

@



## Question 3 of 4

What API permission do you need to grant to the app registration in Azure for Central to be able to synchronize?

Directory.Audit

User.Read

Directory.Read.All

User.Enumerate

SOPHOS



## Question 4 of 4

What filter modes can you select for Azure AD Sync?

Users by group ID

Users by user type

Users by group name

Users by group filter

Users by user filter

Users by group type

SOPHOS

# Chapter Review

AD Sync Utility can synchronize **users**, **groups**, **devices**, **organization units**, and **public folders** from Windows Active Directory. You can define one or more **search bases** and **LDAP filters** to manage what is synchronized.

The logs for AD Sync Utility can be found in **%ProgramData%\Sophos\Sophos Cloud AD Sync\Logs\** and in the event log in **Applications and Services Logs > Sophos Cloud AD Sync**.

Azure AD Sync has three filter modes: **users by group id**, **users by group filter**, and **users by user filter**. You can change the filter mode, but you will lose any existing filter criteria.

SOPHOS

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

AD Sync Utility can synchronize users, groups, devices, organization units, and public folders from Windows Active Directory. You can define one or more search bases and LDAP filters to manage what is synchronized.

The logs for AD Sync Utility can be found in the Sophos Cloud AD Sync Logs folder and in the Windows event log in Applications and Services Logs.

Azure AD Sync has three filter modes: users by group id, users by group filter, and users by user filter. You can change the filter mode, but you will lose any existing filter criteria.



# Troubleshooting Automated Deployment on Windows

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE1540: Troubleshooting Automated Deployment on Windows

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.

# Troubleshooting Automated Deployment on Windows

In this chapter you will learn how to troubleshoot common issues with automating the deployment of the Sophos Central endpoint agent on Windows.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Be able to install the Sophos Central endpoint agent on Windows

DURATION      **10 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot common issues with automating the deployment of the Sophos Central endpoint agent on Windows.



Additional information in  
the notes

## Installer Options

Don't display interface  
during installation

--quiet

Define proxy  
configuration

--noproxydetection  
--proxyaddress=<custom proxy address>  
--proxyusername=<custom proxy username>  
--proxypassword=<custom proxy password>

Specify products to  
install

--products=<comma or semi-colon separated list of products>  
Options: antivirus, intercept, mdr, xdr, deviceEncryption, all

Specify Message Relays

--messagerelays=<comma-separated message relay list>  
Format: hostname:port,ip-address:port

SOPHOS

When automating deployment of the Sophos Central Endpoint Agent you can make use of the installer options. We will look at some of the key options briefly here. You can prevent the installer being displayed during installation; this will be used in every automated deployment.

If a proxy is required to access the Internet, this can be configured on the command line. Note that a proxy URL without protocol will use HTTPS.

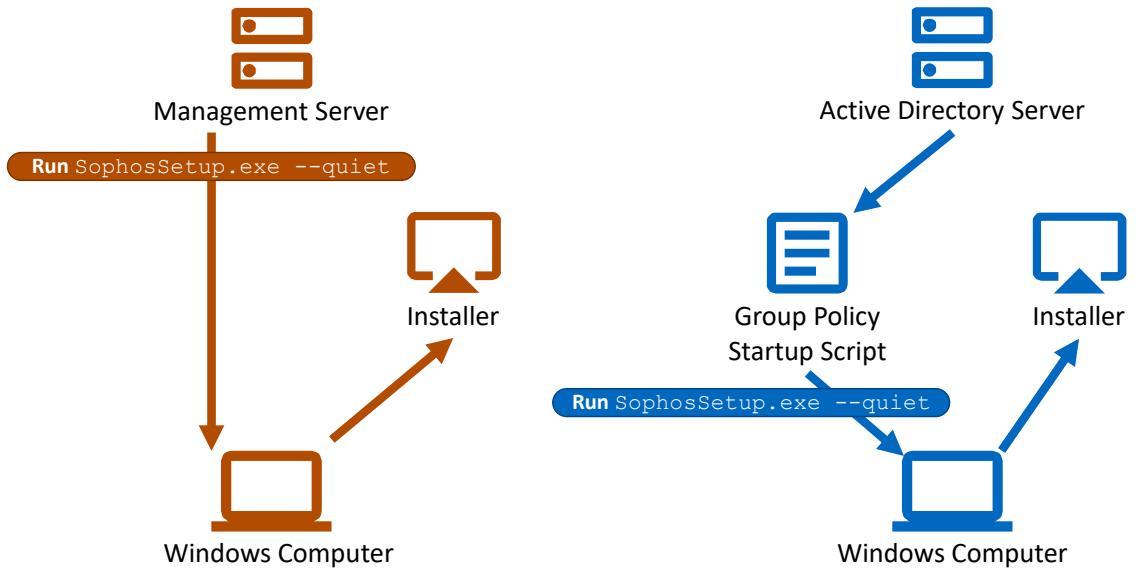
You can control which products are installed, antivirus, intercept, mdr, xdr, deviceEncryption, or all.

If you are using Message Relays, these can be passed to the installer on the command line. This is a comma-separated list and can use either the hostname or IP address along with the Message Relay port. Please note there is no command line option regarding installation from an update cache. The installer will automatically assess connectivity to any update caches set up in the Central account and install from them if appropriate.

### [Additional Information]

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

# Automating Deployment



Automating deployment can be completed by either calling the installer directly with any options you want, which is what you would do if you were using Microsoft Endpoint Configuration Manager, or by using a script to call the installer with the required options, which is what you would do if you were using Active Directory Group Policy.



## Example Deployment Script

```
Untitled - Notepad
File Edit Format View Help

@echo off
SET MCS_ENDPOINT=Sophos\Management Communications
System\Endpoint\McsClient.exe
IF "%PROCESSOR_ARCHITECTURE%" == "x86" GOTO X86_PROG
IF NOT EXIST "%ProgramFiles(x86)%\%MCS_ENDPOINT%" GOTO INSTALL
exit /b 0

:X86_PROG
IF NOT EXIST "%ProgramFiles%\%MCS_ENDPOINT%" GOTO INSTALL
exit /b 0

:INSTALL
pushd \\servername\share
SophosSetup.exe --quiet
Popd
```

Let's look at an example deployment script that you would use with Active Directory Group Policy. The script firstly checks to see if the Sophos Agent is already installed, it starts this process by storing the location of the MCS service executable.

The path to the installation folder depends on whether it is a 32 or 64-bit operating system, so the script checks for the file depending on the processor architecture. If the Sophos Agent is already installed the script will exit, otherwise it starts the installation. The path to the installer will need to be modified for your environment.

The script must be saved as a 'bat' file to be used.

### [Additional Information]

Automate the software deployment to devices **KB-000035049**.

<https://support.sophos.com/support/s/article/KB-000035049>

# Testing the Script



```
Untitled - Notepad
File Edit Format View Help

REM @echo off
SET MCS_ENDPOINT=Sophos\Management Communications
SET SMC=Endpoint\McsClient.exe
IF "%PROCESSOR_ARCHITECTURE%" == "x86" GOTO X86_PROG
%MCS_ENDPOINT% GOTO INSTALL

Use 'REM' to comment out the '@echo off' line so you can see each command as it is executed

:X86_PROG
IF NOT EXIST "%ProgramFiles%\%MCS_ENDPOINT%" GOTO INSTALL
exit /b 0

:INSTALL
pushd \\servername\share
SophosSetup.exe --quiet
Popd

Ln 1, Col 1      100%   Windows (CR/LF)   UTF-8
```

SOPHOS

Installation scripts should be tested before they are deployed.

When testing, it is useful to comment out the '@echo off' line with 'REM'. This means that each command will be displayed as it is run, making it much easier to identify any problems with the script.

## Testing the Script

```
C:\>Script\InstallSophos.bat  
C:\>REM @echo off  
C:\>SET MCS_ENDPOINT=Sophos\Management Communications System\Endpoint\McsClient.exe  
C:\>IF "AMD64" == "x86" GOTO X86_PROG  
C:\>IF NOT EXIST "C:\Program Files (x86)\Sophos\Management Communications System\Endpoint\McsClient.exe" GOTO INSTALL  
C:\>pushd \\servername\share  
The network path was not found.  
C:\>SophosSetup.exe --quiet  
'SophosSetup.exe' is not recognized as an internal or external command,  
operable program or batch file.  
C:\>Popd
```

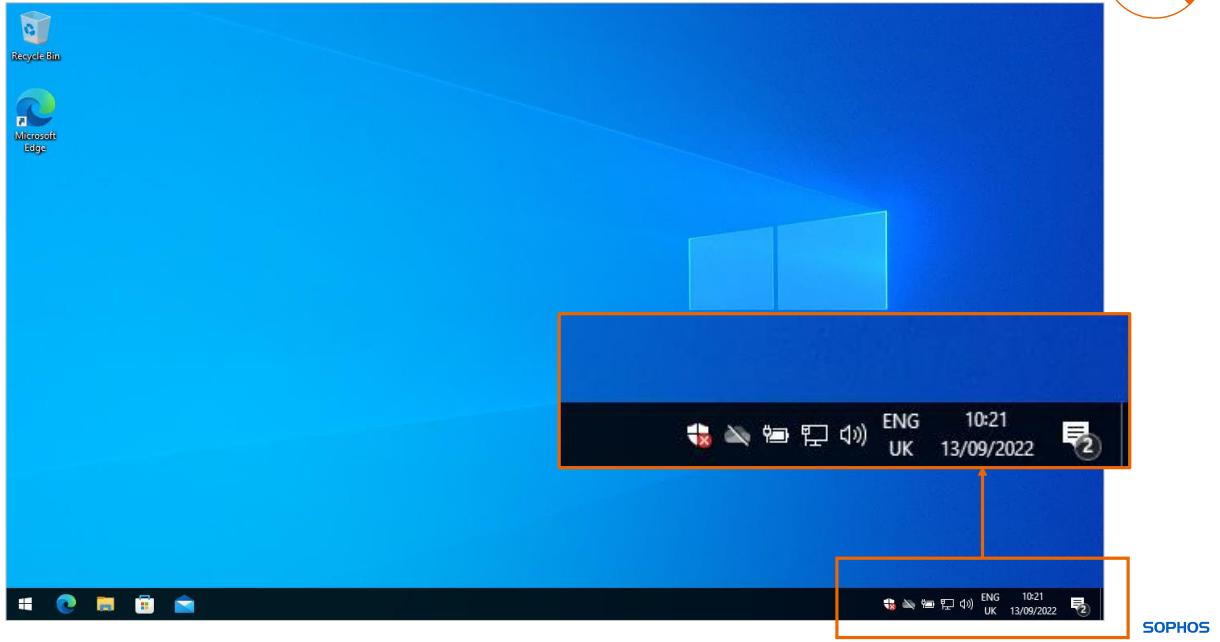
SOPHOS

To test the script, run it on a target device using a command prompt run with administrator rights.

Here you can see that the script has failed because the path to the share where the installer is kept has been misconfigured.

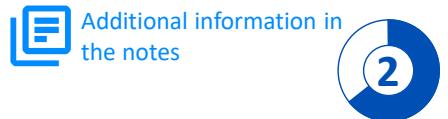
# Sophos Not Installing: Scenario 1

1



We will now look at some common issues scripting deployment with Active Directory Group Policy.

Most likely what you will notice is that Sophos is not installed onto the devices. You might notice that they are not appearing in Sophos Central, or that the Sophos shield icon is not appearing in the system tray.



# Sophos Not Installing: Scenario 1



```
C:\Users\Administrator>gpresult /r /scope computer /s winclient1  
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0  
© Microsoft Corporation. All rights reserved.
```

Created on 13/09/2022 at 02:16:13

RSOP data for on WINCLIENT1 : Logging Mod

```
OS Configuration: Member Workst  
OS Version: 10.0.19043  
Site Name: Default-First  
Roaming Profile:  
Local Profile:  
Connected over a slow link?: No
```

COMPUTER SETTINGS

```
Last time Group Policy was applied: 13  
Group Policy was applied from: UK  
Group Policy slow link threshold: 50  
Domain Name: TR  
Domain Type: Wi
```

## Applied Group Policy Objects

### Default Domain Policy

The following GPOs were not applied because they were filtered out

```
Local Group Policy  
Filtering: Not Applied (Empty)
```

The computer is a part of the following security groups

```
BUILTIN\Administrators  
Everyone  
BUILTIN\Users  
NT AUTHORITY\NETWORK  
NT AUTHORITY\Authenticated Users  
This Organization  
WINCLIENT1$  
Domain Computers  
Authentication authority asserted identity  
System Mandatory Level
```

SOPHOS

The first step will be to determine if the device is applying the group policy with the installation script. To do this you can use the gpresult command.

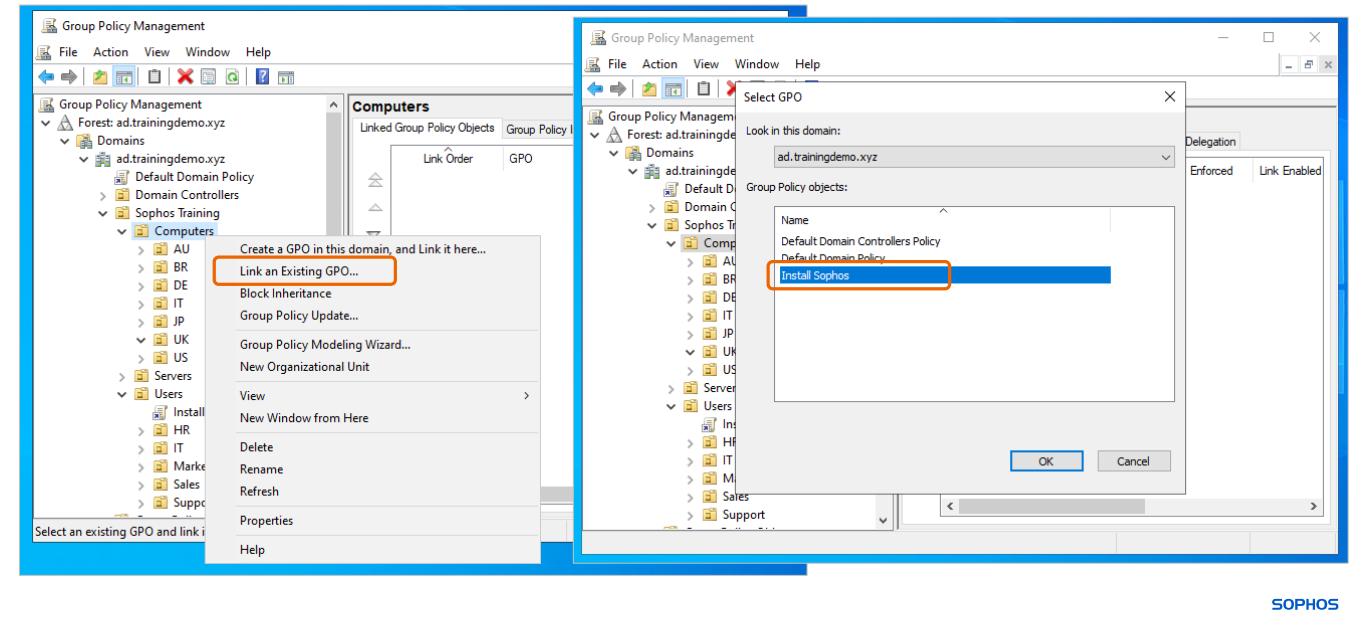
You want to set the scope to computer and specify the device that you want to check the group policy result on. Please note that the gpresult command must be run with administrator rights.

In the output you can see the group policy objects that are applied to the computer. In this case the group policy for installing Sophos is missing.

## [Additional Information]

The syntax for gpresult is: gpresult /r /scope computer /s <device>

# Sophos Not Installing: Scenario 1



To apply the group policy to a set of computers, you want to link to the group policy object in the organization unit using the Group Policy Management tool.

The group policy will apply to all devices in that organizational unit and all child organizational units.

## Sophos Not Installing: Scenario 1

3

Refresh the group policy on the target device

```
C:\Windows\system32>gpupdate
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

```
C:\Windows\system32>
```

SOPHOS

Before you can check whether the group policy is now being applied you will need to refresh the group policy on the target device using the gpupdate command.

# Sophos Not Installing: Scenario 1

3

```
C:\Users\Administrator>gpresult /r /scope computer /s winclient1

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on 13/09/2022 at 02:16:13

RSOP data for on WINCLIENT1 : Logging Mod
-----
OS Configuration: Member Workst
OS Version: 10.0.19043
Site Name: Default-First
Roaming Profile:
Local Profile:
Connected over a slow link?: No

COMPUTER SETTINGS
-----
Last time Group Policy was applied: 13
Group Policy was applied from: UK
Group Policy slow link threshold: 50
Domain Name: TR
Domain Type: Wi

Applied Group Policy Objects
-----
Install Sophos
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
WINCLIENT1$
Domain Computers
Authentication authority asserted identity
System Mandatory Level
```

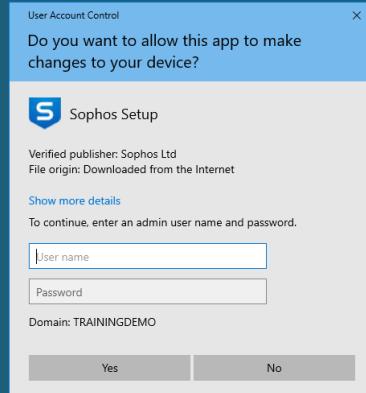
SOPHOS

You can then run the gpresult command again.

This can be run on the endpoint but does require an administrator command prompt. If you are running it on the device, you do not need to specify the system as it will default to itself.

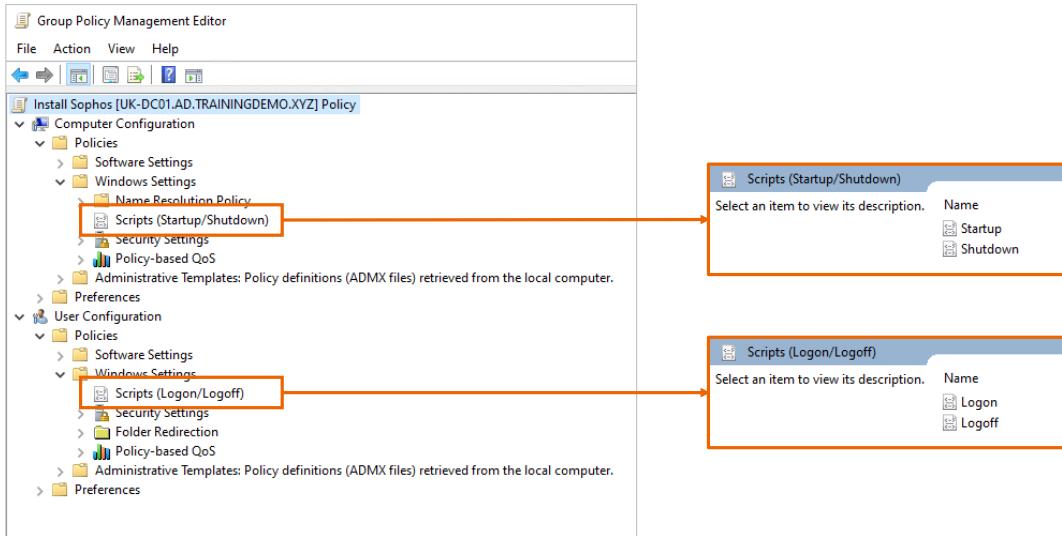
Here you can see that the group policy is now applied to this device.

# User Prompted for Administrator Authentication



In this scenario, users are prompted to login as an administrator to install Sophos.

# User Prompted for Administrator Authentication



SOPHOS

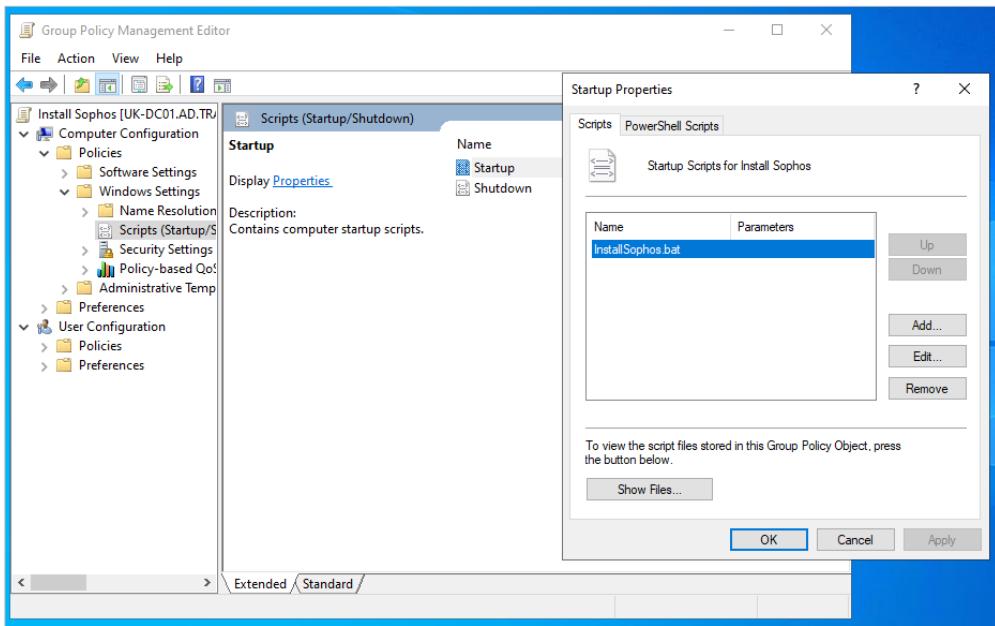
The Sophos installation requires administrator rights to run, and so should be run as a computer startup script.

If the installation is run from a user logon script it will run with that user's permissions. Unless all users have administrator rights, they will be prompted to login as an administrator to start the installation.

The startup and shutdown scripts are found in the **Computer Configuration** section of the policy and run with system privileges.

The logon and logoff scripts are found in the **User Configuration** section of the policy. These are run as the user that logs into the computer.

# User Prompted for Administrator Authentication



SOPHOS

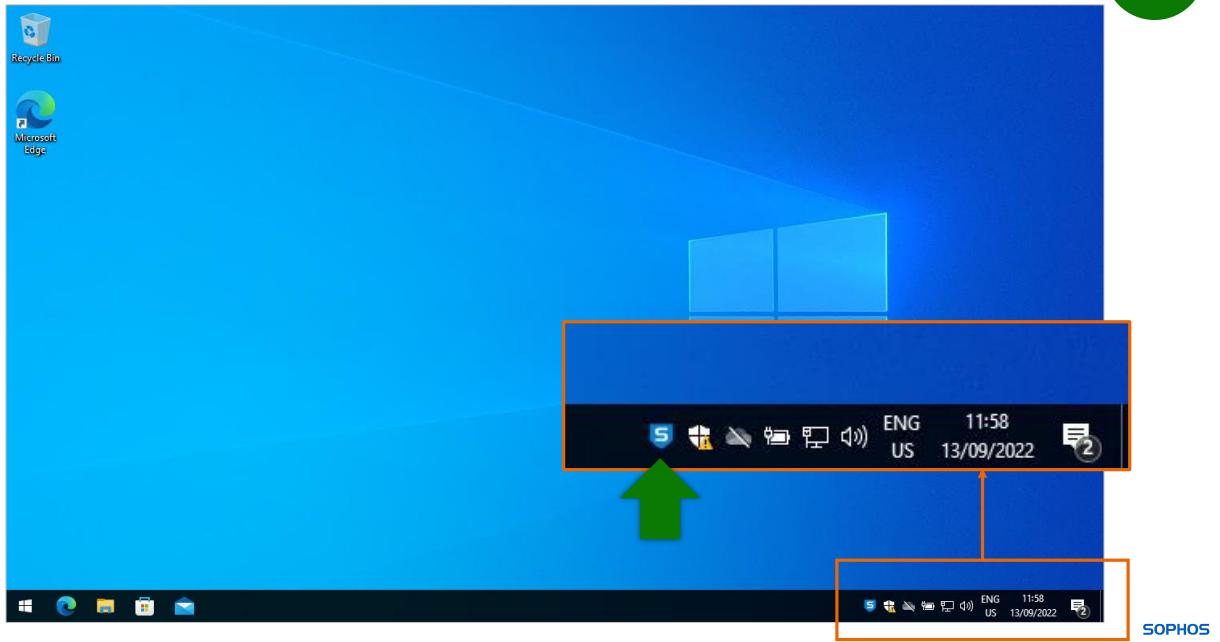
To correct this, add the installation script to the **Computer Configuration Startup scripts**.

First, use the **Show Files...** button to open the script directory and copy the installation script into the folder.

Then, click **Add** and select the script file.

## User Prompted for Administrator Authentication

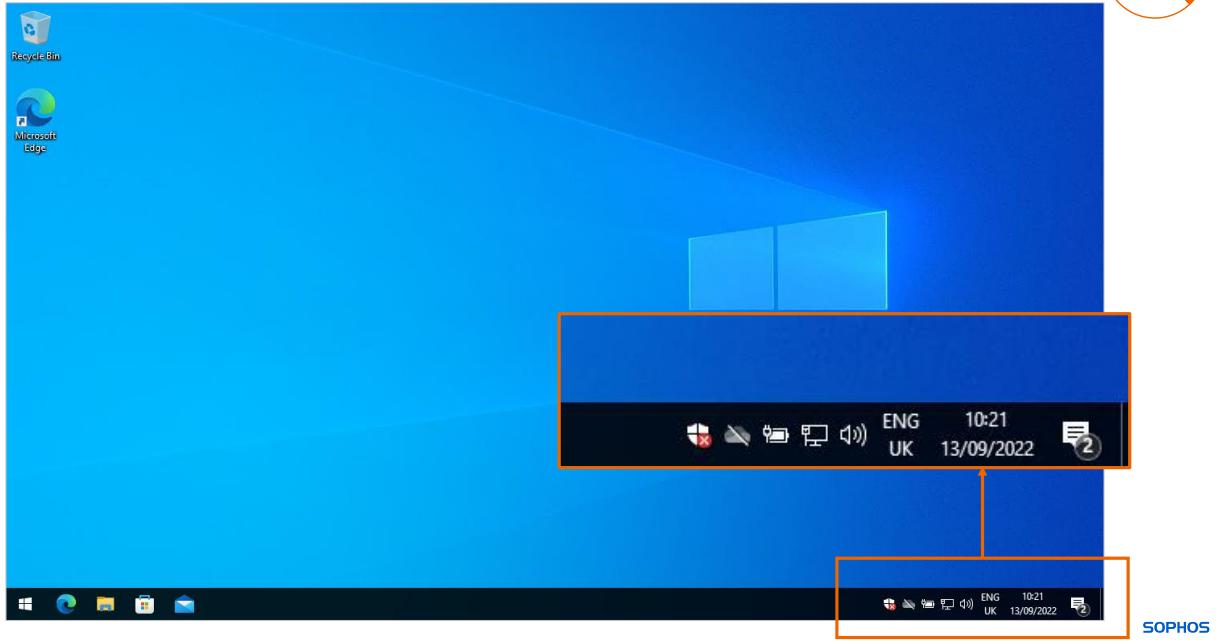
3



When the computer is restarted Sophos will install in the background and you will see the icon in the system tray, and the device will appear in the Sophos Central dashboard.

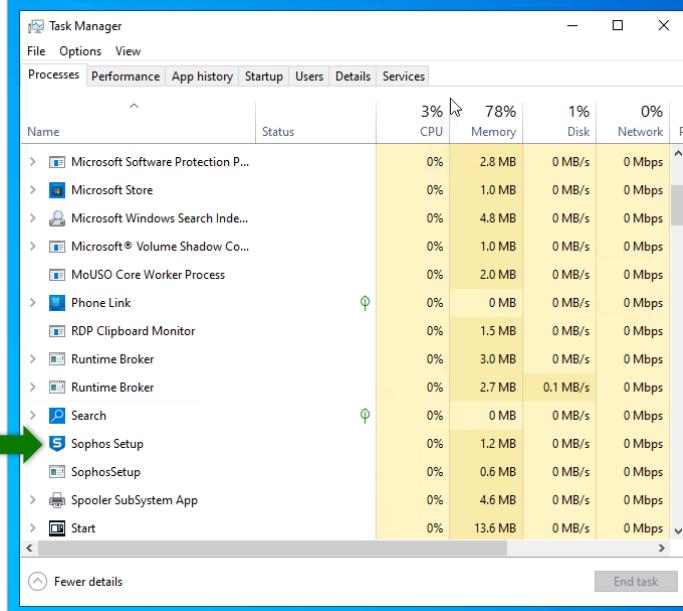
## Sophos Not Installing: Scenario 2

1



In this scenario, the group policy is applied to the computer and the installations script is being run as a computer startup script, but Sophos is still not being installed.

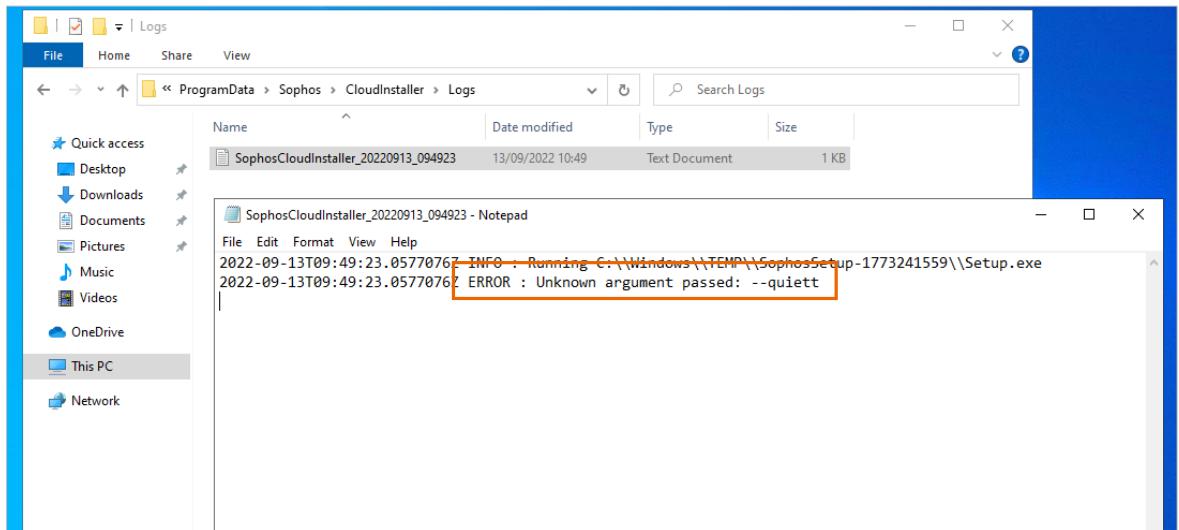
## Sophos Not Installing: Scenario 2



SOPHOS

If you look at the processes on the target device you will see that Sophos Setup is running in the background, but it is not doing anything.

# Sophos Not Installing: Scenario 2



SOPHOS

As the installer is running you can check the log file. This is located in Program Data\Sophos\CloudInstaller\Logs.

Looking at the most recent log file we can see the error 'unknown argument passed'. This indicates that the quiet option has a typo.

As the Sophos setup has not received a valid quiet option, it is running in interactive mode; however, it is running as system and so is not visible to the user and cannot be interacted with.

## Sophos Not Installing: Scenario 2



```
SophosCloudInstaller_20220913_095630 - Notepad
File Edit Format View Help
2022-09-13T09:56:30.7068095Z INFO : Running C:\Windows\TEMP\SophosSetup-969405461\Setup.exe
2022-09-13T09:56:30.7068095Z INFO : Stage 1 command-line options:
2022-09-13T09:56:30.7068095Z INFO :
2022-09-13T09:56:30.7068095Z INFO : Quiet mode on: 0
2022-09-13T09:56:30.7068095Z INFO : Automatic Proxy detection disabled: 0
2022-09-13T09:56:30.7224278Z INFO : No feedback mode on: 0
2022-09-13T09:56:30.7224278Z INFO : Dump feedback enabled: 0
2022-09-13T09:56:30.7224278Z INFO : Bypass competitor removal: 0
2022-09-13T09:56:30.7224278Z INFO : Using CRT catalog file path: --
2022-09-13T09:56:30.7380516Z INFO : Only register endpoint with Central: 0
2022-09-13T09:56:30.7380516Z INFO : Log messages between endpoint and Central: 0
2022-09-13T09:56:30.7380516Z INFO : Log command-line passed to executables: 0
2022-09-13T09:56:30.7380516Z INFO : Using custom server that hosts the installer stage2 filename: --
2022-09-13T09:56:30.7380516Z INFO : Using cloud group: --
2022-09-13T09:56:30.7380516Z INFO : Overriding computer name: --
2022-09-13T09:56:30.7380516Z INFO : Overriding computer description: --
2022-09-13T09:56:30.7380516Z INFO : Overriding domain name: --
2022-09-13T09:56:30.7380516Z INFO : Language will be set to: --
2022-09-13T09:56:30.7380516Z INFO : Using message relays: --
2022-09-13T09:56:30.7380516Z INFO : Proxy address: --
2022-09-13T09:56:30.7380516Z INFO : Proxy user name: --
2022-09-13T09:56:30.7380516Z INFO : Using custom customer token: --
2022-09-13T09:56:30.7380516Z INFO : Using specified products: --
2022-09-13T09:56:30.7380516Z INFO : Using certificates from the program data folder: A
<                                         Ln 1, Col 1   100% Windows (CRLF)   UTF-8 ..
```

SOPHOS

You would also get the same behaviour if the quiet option is omitted entirely; however, the log file would get a lot further.

At the top of the log file you can see the command-line options that Sophos setup has received, and in this log file there is no quiet option.

## Sophos Not Installing: Scenario 2



```
Untitled - Notepad
File Edit Format View Help

@echo off
SET MCS_ENDPOINT=Sophos\Management Communications
System\Endpoint\McsClient.exe
IF "%PROCESSOR_ARCHITECTURE%" == "x86" GOTO X86_PROG
IF NOT EXIST "%ProgramFiles(x86)%\%MCS_ENDPOINT%" GOTO INSTALL
exit /b 0

:X86_PROG
IF NOT EXIST "%ProgramFiles%\%MCS_ENDPOINT%" GOTO INSTALL
exit /b 0

:INSTALL
pushd \\servername\share
SophosSetup.exe --quiet
Popd

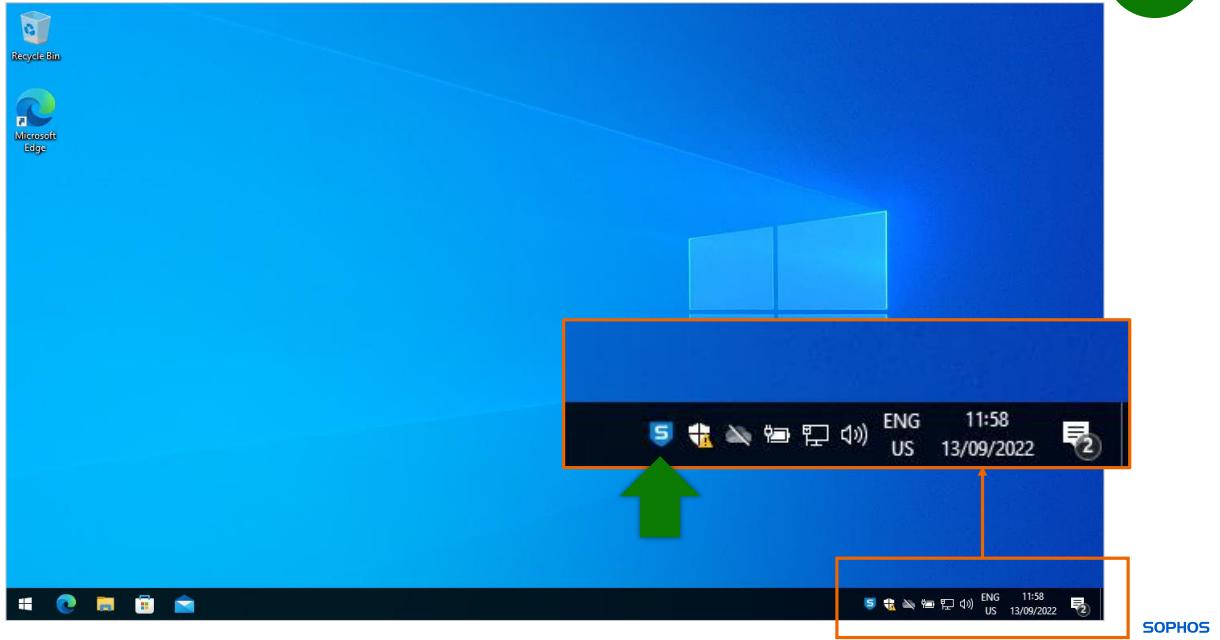
Ln 1, Col 1      100%   Windows (CR/LF)   UTF-8
```

SOPHOS

To resolve this, either add the missing quiet option or correct the typo.

## Sophos Not Installing: Scenario 2

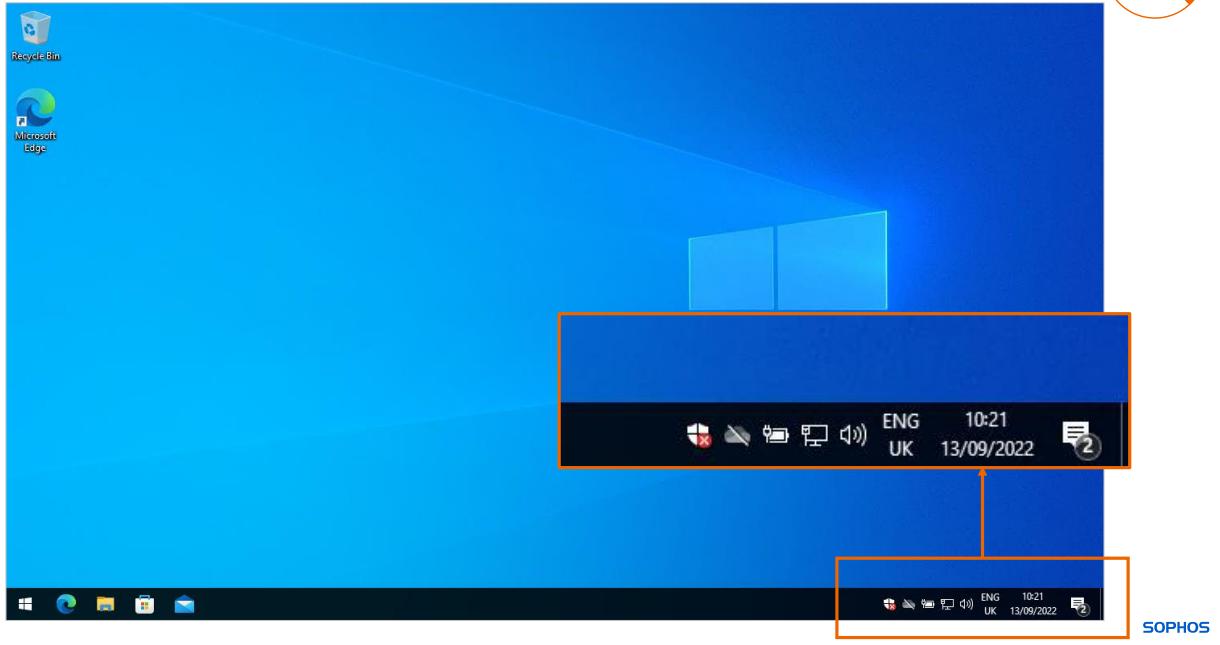
3



The next time the computer restarts the script will run in the background and Sophos will be installed.

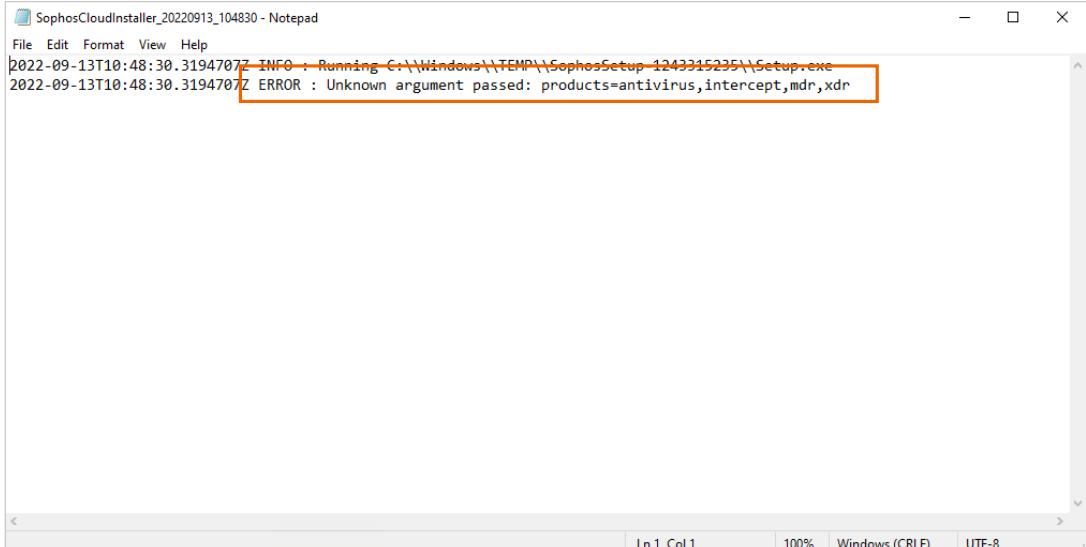
## Sophos Not Installing: Scenario 3

1



In this scenario, the Sophos Endpoint Agent is not installing; however, there is no setup process running in the background.

## Sophos Not Installing: Scenario 3



The screenshot shows a Notepad window titled "SophosCloudInstaller\_20220913\_104830 - Notepad". The window contains the following text:

```
File Edit Format View Help
2022-09-13T10:48:30.3194707Z INFO : Running C:\\Windows\\\\TEMP\\\\SophosSetup_1243315235\\\\Setup.exe
2022-09-13T10:48:30.3194707Z ERROR : Unknown argument passed: products=antivirus,intercept,mdr,xdr
```

The last line of the log, which contains the error message, is highlighted with a red rectangular box.

SOPHOS

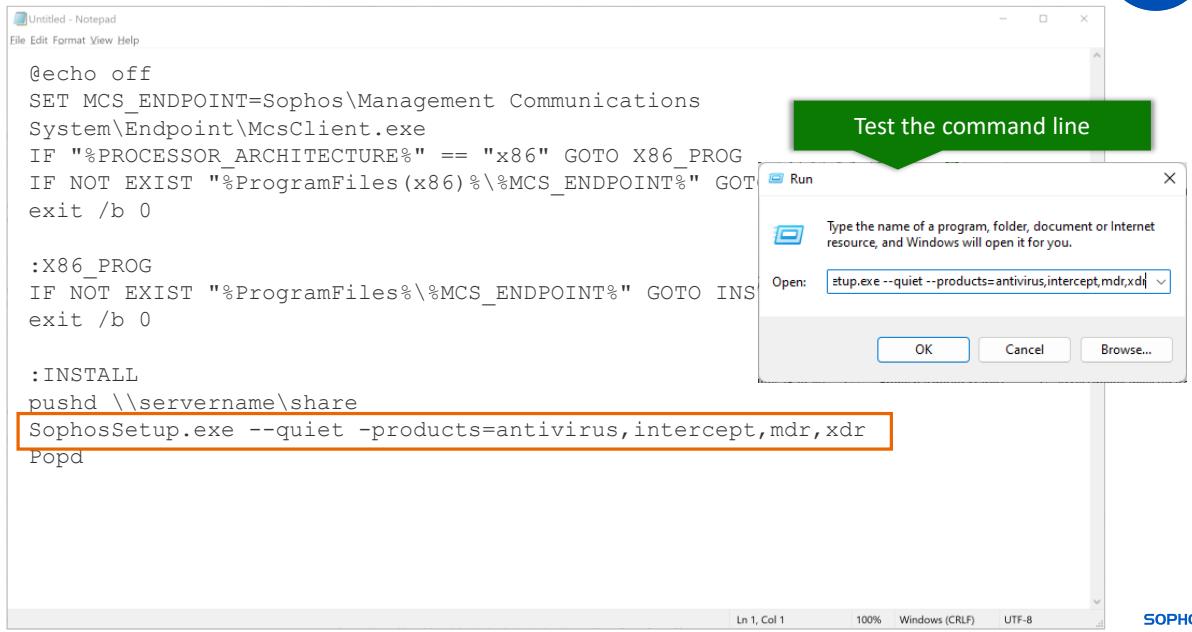
The first step is to check the installer log.

Here we can see the error 'unknown argument passed' and the option that the installer does not recognise.

At first look this appears okay, so the next step will be to look at the script.

## Sophos Not Installing (Scenario 3)

2



Untitled - Notepad

```
@echo off
SET MCS_ENDPOINT=Sophos\Management Communications
System\Endpoint\McsClient.exe
IF "%PROCESSOR_ARCHITECTURE%" == "x86" GOTO X86_PROG
IF NOT EXIST "%ProgramFiles(x86)%\%MCS_ENDPOINT%" GOTO INS
exit /b 0

:X86_PROG
IF NOT EXIST "%ProgramFiles%\%MCS_ENDPOINT%" GOTO INS
exit /b 0

:INSTALL
pushd \\servername\share
SophosSetup.exe --quiet -products=antivirus,intercept,mdr,xdr
Popd
```

Run

Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: `setup.exe --quiet --products=antivirus,intercept,mdr,xdr`

OK Cancel Browse...

In 1, Col 1 100% Windows (CR/LF) UTF-8

SOPHOS

On closer inspection we can see that the products option is missing a hyphen.

Correct the command, then run it as an administrator to test that it works correctly.

# Common Command Line Errors



## Example

## Correct Command

### Missing hyphen

SophosSetup.exe -quiet

SophosSetup.exe --quiet

### Additional space

SophosSetup.exe -- quiet  
SophosSetup.exe --products= intercept  
SophosSetup.exe --products=intercept, xdr

SophosSetup.exe --quiet  
SophosSetup.exe --products=intercept  
SophosSetup.exe --products=intercept,xdr

### Typo

SophosSetup.exe -queit

SophosSetup.exe -quiet

### Missing option

SophosSetup.exe

SophosSetup.exe --quiet

SOPHOS

There are a few common mistakes with command line options.

Missing a hyphen, which makes the option invalid.

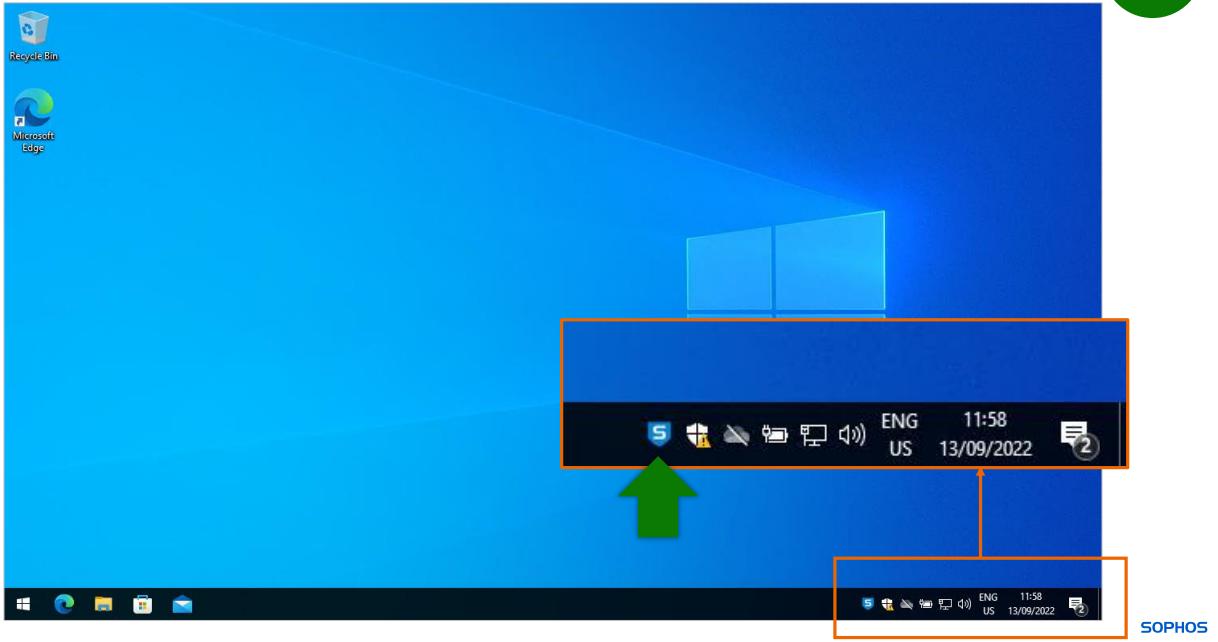
Adding an additional space. This could be in various places, after the hyphens, after the equals, or maybe in comma-separated lists.

General typos.

Missing a required option. We looked at missing the quiet option, but missing proxy settings could also cause the installation to fail.

## Sophos Not Installing: Scenario 3

3



With the script corrected, the next time the computer restarts the script will run in the background and Sophos will be installed.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 5

Sophos Setup is running in the background but not doing anything. What is the most likely cause?

Incorrect proxy settings

Insufficient user permissions

Group Policy is not applied

Missing quiet option

SOPHOS

## Question 2 of 5



You are prompted to login as an administrator to install Sophos. What is the most likely cause?

The script is running as a user logon script

The quiet option has not been used

The script is running as a computer startup script

The group policy is not applied to the computer

SOPHOS

## Question 3 of 5

What command can you use to view the group policies that are applied to a computer?

\_\_\_\_\_



## Question 4 of 5

What command can you use to refresh the group policies on a computer?

SOPHOS



## Question 5 of 5

Here is an incorrect command:

```
SophosSetup.exe -quiet --products=antivirus, intercept,mdr,xdr  
Correct the command and enter it below.
```

SOPHOS

# Chapter Review

When deploying through Active Directory Group Policies, the deployment script must be added to the **computer startup** script so that it runs with sufficient privileges. If it runs as a user logon script it will run as the logged in user and only be able to install if the user is an administrator.

You can use the **gpresult** command to **check what group policies are applied** to a device. The **gpupdate** command can be used to **refresh the group policies** on a device.

Incorrect installer options will cause the installation to end early. If the **quiet** option is missing or incorrect the installer will remain running in the background waiting for user input. You can see the installer options in the cloud installer log file in **ProgramData\Sophos\CloudInstaller\Logs**.

SOPHOS

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

When deploying through Active Directory Group Policies, the deployment script must be added to the computer startup script so that it runs with sufficient privileges. If it runs as a user logon script it will run as the logged in user and only be able to install if the user is an administrator.

You can use the gpresult command to check what group policies are applied to a device. The gpupdate command can be used to refresh the group policies on a device.

Incorrect installer options will cause the installation to end early. If the quiet option is missing or incorrect the installer will remain running in the background waiting for user input. You can see the installer options in the cloud installer log file in ProgramData\Sophos\CloudInstaller\Logs.



# Troubleshooting Central Manual Deployment on Windows

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE1535: Troubleshooting Central Manual Deployment on Windows

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.

# Troubleshooting Central Manual Deployment on Windows

In this chapter you will learn how to troubleshoot installation of the Sophos Central Endpoint Agent on Windows devices.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to install the Sophos Central Endpoint Agent on Windows devices

DURATION      **17 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot installation of the Sophos Central Endpoint Agent on Windows devices.



Additional information in  
the notes

# Installation Requirements

Sophos Installer

Supported OS and minimum resource requirements (KB-000035144)

Internet connection to Sophos Central

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

SOPHOS

To install the Sophos Endpoint Agent on Windows devices, download the installer from Sophos Central. The target device must meet the minimum operating system and resource requirements.

The device will also need an Internet connection to Sophos Central. The domains and ports required for successful connection can be found in the Sophos Central online documentation.

## [Additional Information]

System Minimum Requirements: <https://support.sophos.com/support/s/article/KB-00003514>

# Activity: Review Domains and Ports



Read the documentation that outlines the domains and ports used by Sophos Central.

**OPEN ACTIVITY**

**CONTINUE**

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

SOPHOS

Please complete this activity.

Click **OPEN ACTIVITY** to start. Once you have finished, click **CONTINUE**.

## [Additional Information]

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

# Installation Process

Stage 1  
**Thin** Installer

Downloads and runs the Stage 2 Installer

Stage 2  
**Full** Installer

Register Endpoint  
Download AutoUpdate Policy  
Download Software  
Decode Downloaded Files  
Moved Downloaded Data to AutoUpdate Cache  
Install Software

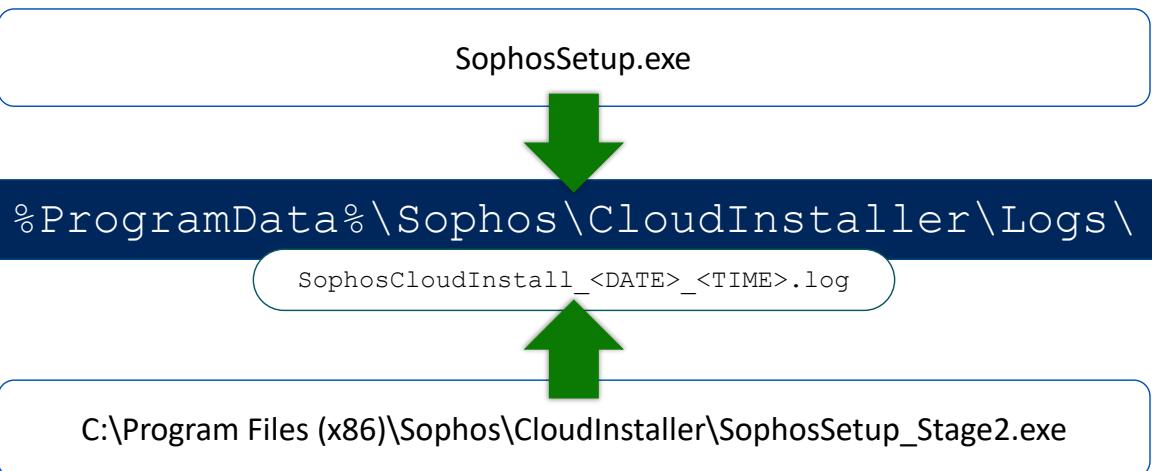
SOPHOS

The Windows installation process is completed using two installers. Firstly, the thin installer which is downloaded from Sophos Central. When run, the thin installer will download and run the stage 2 installer.

The stage 2, or full installer will:

- Register the endpoint with Sophos Central. As this is done before the rest of the installation, if there is a problem the device will appear in the Sophos Central but show that the protection is not installed
- Download the AutoUpdate policy, which defines the software packages that need to be installed
- The installer will download the software and decode the downloaded files
- The files are moved the AutoUpdate Cache folder
- Finally, the installers for each package are called

## SophosSetup.exe Installer Logging



SOPHOS

The main log file for the installation is the SophosCloudInstall log located in ProgramData\Sophos\CloudInstaller\Logs.

Both the thin installer and the full stage 2 installer will log to this file.

## SophosSetup.exe Installer Logging

```
2022-09-13T10:53:54.6707071Z INFO : Running C:\\Windows\\\\TEMP\\\\SophosSetup-1698582668\\\\Setup.exe
2022-09-13T10:53:54.6707071Z INFO : Stage 1 command-line options:
2022-09-13T10:53:54.6707071Z INFO : ---
2022-09-13T10:53:54.6707071Z INFO : Quiet mode on: 1
2022-09-13T10:53:54.6707071Z INFO : Automatic Proxy detection disabled: 0
2022-09-13T10:53:54.6707071Z INFO : No feedback mode on: 0
2022-09-13T10:53:54.6707071Z INFO : Dump feedback enabled: 0
2022-09-13T10:53:54.6707071Z INFO : Bypass competitor removal: 0
2022-09-13T10:53:54.6707071Z INFO : Using CRT catalog file path: --
2022-09-13T10:53:54.6707071Z INFO : Only register endpoint with Central: 0
2022-09-13T10:53:54.6707071Z INFO : Log messages between endpoint and Central: 0
2022-09-13T10:53:54.6707071Z INFO : Log command-line passed to executables: 0
2022-09-13T10:53:54.6707071Z INFO : Using custom server that hosts the installer stage2 filename: --
2022-09-13T10:53:54.6707071Z INFO : Using cloud group: --
2022-09-13T10:53:54.6707071Z INFO : Overriding computer name: --
2022-09-13T10:53:54.6707071Z INFO : Overriding computer description: --
2022-09-13T10:53:54.6707071Z INFO : Overriding domain name: --
2022-09-13T10:53:54.6707071Z INFO : Language will be set to: --
2022-09-13T10:53:54.6707071Z INFO : Using message relays: --
2022-09-13T10:53:54.6707071Z INFO : Proxy address: --
2022-09-13T10:53:54.6707071Z INFO : Proxy user name: --
2022-09-13T10:53:54.6707071Z INFO : Using custom customer token: --
2022-09-13T10:53:54.6707071Z INFO : Using specified products: antivirus,intercept,mdr,xdr
2022-09-13T10:53:54.6707071Z INFO : Using certificates from the program data folder: 0
```

Command line options passed to SophosSetup.exe

SOPHOS

Let's look at some of the key parts of the SophosCloudInstall log file.

At the top of the log, you can see the command line options that were passed to SophosSetup.exe. This is useful for determining if there are any formatting or typo errors in the parameters, especially where the installation is being launched by a script or other management tool.

## SophosSetup.exe Installer Logging

```
2022-09-13T10:53:54.7957059Z INFO : Sending HTTP 'POST' request to: api/download/stage2-
details/c7cbc8c3-daa5-4087-8a37-2ef4548b24fe
2022-09-13T10:53:54.8112838Z INFO : Opening connection to dze-api-amzn-eu-west-
upe.p.hmr.sophos.com
2022-09-13T10:53:56.6562960Z INFO : Parsing message received for Stage 2 filename:
'{"downloads_server":"downloads.sophos.com","telemetry_server":"t1.sophosupd.com","mcs_server":"mcs2-
cloudstation-eu-west-1.prod.hydra.sophos.com","stage2_filename":"stage2-1.15.63.0-
38c36c7059d0574f25588ef6571438fccedc0269d8f0ccbba5b3ea9761d2f0689.tar.gz"}'
2022-09-13T10:53:56.6562960Z INFO : Sending HTTP 'GET' request to:
full/central/windows/business/installer/stage2-1.15.63.0-
38c36c7059d0574f25588ef6571438fccedc0269d8f0ccbba5b3ea9761d2f0689.tar.gz
2022-09-13T10:53:59.1752238Z INFO : Response status code: 200
2022-09-13T10:53:59.1752238Z INFO : Response data size: 3191170
2022-09-13T10:53:59.1752238Z INFO : Extracting files:
2022-09-13T10:54:01.6678273Z INFO : Stage 2 command-line options:
```

Get stage2 installer details

Downloading the stage2 installer

Extract the stage2 installer

Command line options passed to the stage2 installer

SOPHOS

Next you will see logging for getting the stage 2 installer. The thin installer makes a request to Sophos Central to get the latest version of the installer, then it extracts and runs it.

You will see the command line options being passed on to the full stage 2 installer when it is executed.

## Software Installation Logs

```
2022-09-13T10:54:02.1535572Z INFO : Sending HTTP 'POST' request to:  
sophos/management/ep/install/register
```

Register device

```
2022-09-13T10:54:02.4596817Z INFO : Retrieved endpoint id: 8a1b6601-22e8-4468-3a64-456c2271f905
```

```
2022-09-13T10:54:03.4702621Z INFO : Sending HTTP 'GET' request to:
```

```
sophos/management/ep/install/flags/endpoint/8a1b6601-22e8-4468-3a64-456c2271f905
```

```
2022-09-13T10:54:03.4729852Z INFO : Request content size: 0
```

```
2022-09-13T10:54:03.6046422Z INFO : Attempt to retrieve policy.
```

```
2022-09-13T10:54:03.6046422Z INFO : Sending HTTP 'GET' request to:
```

```
sophos/management/ep/install/commands/applications/APPSPROXY;ALC/endpoint/8a1b6601-22e8-4468-3a64-  
456c2271f905
```

Download AutoUpdate policy

```
2022-09-13T10:54:03.6517352Z INFO : Successfully retrieved policy with  
policyId='588fada9a1f621b18d0a517266422e911e25d225369d9c7300bdb0826b541d59'.
```

```
2022-09-13T10:54:03.9350257Z INFO : Updating subscription created with id: Base, rigidname:  
WindowsCloudNextGen, baseversion: 11, tag: RECOMMENDED, fixedversion:
```

```
2022-09-13T10:54:04.0753121Z INFO : Command 'Register' completed with success with reboot code '0' and  
error message ''.
```

SOPHOS

The first thing the full stage 2 installer does is to register the endpoint. You will see log entries for the request that result in an endpoint ID being retrieved. The endpoint ID is generated based on the computer name during registration. If a computer is re-protected it should be assigned the same unique endpoint ID.

Using the endpoint ID, the installer will download the AutoUpdate policy that will contain the information required to download the software.

This section ends with log entries for updating the subscription and the register command completing.

# Software Installation Logs

```
2022-09-13T10:54:04.452249ZZ INFO : Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy:  
<direct; no proxy>  
2022-09-13T10:54:04.577259ZZ INFO : 200 from  
https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat with proxy: <direct; no  
proxy> (peer address 92.122.119.82)  
2022-09-13T10:54:04.577259ZZ INFO : Syncing from: https://sdds3.sophosupd.com  
2022-09-13T10:54:04.577259ZZ INFO : Syncing suite sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat  
2022-09-13T10:54:04.592902ZZ INFO : GET  
https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat: 200 (11398  
bytes)

2022-09-13T10:54:13.6760139ZZ INFO : WindowsCloudNextGen: downloaded suite:  
sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat, version: 2022.2.1.9.0, display version:  
2022.2.1.9

2022-09-13T10:54:13.6760139ZZ INFO : Extracting packages.  
2022-09-13T10:54:13.7854391ZZ INFO : Extracting package DataSetA_2022.9.12.23.  
2022-09-13T10:54:13.7854391ZZ INFO : Decoding  
C:\\\\ProgramData\\\\Sophos\\\\CloudInstaller\\\\AutoUpdatePreparation\\\\Cache\\\\decoded\\\\sse64\\\\2022081502.ide  
2022-09-13T10:54:13.8166445ZZ INFO : Decoding  
C:\\\\ProgramData\\\\Sophos\\\\CloudInstaller\\\\AutoUpdatePreparation\\\\Cache\\\\decoded\\\\sse64\\\\2022081701.ide
```

Downloading software

Decoding software

SOPHOS

There will be a long section of the log that shows entries downloading the software and then extracting and decoding the files.

# Software Installation Logs

```
2022-09-13T10:55:14.0896759Z INFO : Install sequence for components is: CRTSETUP UNINSTALLER64 SED64  
MCS SSE64 SFS64 SHS UI64 AMSI64 SME64 ESH64 LIVETERMINAL64 EFW64 LiveQuery64 | Installing software  
2022-09-13T10:55:14.1052697Z INFO : Checking  
manifest:C:\\\\ProgramData\\\\Sophos\\\\AutoUpdate\\\\Cache\\\\decoded\\\\crt\\\\manifest.dat  
2022-09-13T10:55:14.1533792Z INFO : Checking  
manifest:C:\\\\ProgramData\\\\Sophos\\\\AutoUpdate\\\\Cache\\\\decoded\\\\crt\\\\crt\\\\manifest.dat  
2022-09-13T10:55:16.1238975Z INFO : Installing Component: crt  
2022-09-13T10:55:16.1238975Z INFO : setupDll='setup.dll'; setupExe='su-setup32.exe'.  
2022-09-13T10:55:16.496Z [ 7300: 7380] I Successfully established interface IProductSetup2.  
2022-09-13T10:55:18.948Z [ 7300: 7380] I Reboot state: 0  
2022-09-13T10:55:18.949Z [ 7300: 7380] I Successfully installed product 2B5BCA43-F85C-4C43-8C6B-  
30E7A5794439 0.1.25.  
2022-09-13T10:55:18.9612730Z INFO : Installed crt: 0 (reboot code: 0)  
2022-09-13T10:55:18.9612730Z INFO : Checking  
manifest:C:\\\\ProgramData\\\\Sophos\\\\AutoUpdate\\\\Cache\\\\decoded\\\\uninstaller64\\\\manifest.dat  
2022-09-13T10:55:19.2893948Z INFO : Installing Component: uninstaller64  
2022-09-13T10:55:19.2893948Z INFO : setupDll='setup.dll'; setupExe='su-setup32.exe'.  
2022-09-13T10:55:19.482Z [ 2152: 5700] W IProductSetup2 threw exception Could not create instance.  
2022-09-13T10:55:19.483Z [ 2152: 5700] I Successfully established interface IProductSetup.  
2022-09-13T10:55:19.591Z [ 2152: 5700] I Reboot state: 0  
2022-09-13T10:55:19.592Z [ 2152: 5700] I Successfully installed product 243DECCD-8080-410D-A45F-  
77F2182715EE 1.14.9.9.  
2022-09-13T10:55:19.6019551Z INFO : Installed uninstaller64: 0 (reboot code: 0)  
2022-09-13T10:55:19.6019551Z INFO :
```

SOPHOS

The final part of the log file shows the installation of the software. First you will see the install sequence, that shows the order the packages will be installed. For each package you will then see the installation being started and the result.

The installer can only see the result of the installation for each package. If it fails, the installer will try the installation two further times before continuing to install the other packages. As the installer can only see the result, to get more detail you will need to check the separate log file for the components installation.

# Component Log Files

## Run as USER

User's temp directory: %TEMP%

If %TEMP% resolves to a numbered folder the logs will be in the parent directory

E.g.,  
C:\Users\LucyFox\AppData\Local\Temp\2  
Would be:  
C:\Users\LucyFox\AppData\Local\Temp

## Run as SYSTEM

C:\Windows\Temp

SOPHOS

The log files for each of the component packages can be found in the temp directory. Where this is located will depend on how the installation was started.

If it is a manual installation the log files will be in the user's temp directory. Please note that if the temp environment variable resolves to a numbered folder, the logs will be stored in that folder's parent.

If the installation is being run by a management tool or being started with group policy, it may be running as the SYSTEM user. In this case the component log files will be stored in Windows\Temp.

## Component Log Files

Component	Log Type (MSI/Sophos)	Log Name
Competitor Removal Tool (CRT)	Sophos Sophos	CRT Install Log <Date> <Time>.txt avremove.log
Live Response	Sophos Sophos	Sophos Live Terminal Install Log <Date> <Time>.txt Sophos LiveQuery Install Log <Date> <Time>.txt
Sophos AMSI Protection	Sophos	Sophos AMSI Protection Install Log <Date> <Time>.txt
Sophos AutoUpdate (SAU)	MSI	Sophos AutoUpdate <Ver> Setup Log <Date> <Time>.txt
Sophos Clean	Sophos	Sophos Clean Install Log <Date> <Time>.txt
Sophos Diagnostic Utility (SDU)	Sophos	Sophos SDU <Ver> Install Log <Date> <Time>.txt
Sophos Endpoint Agent (Sophos Endpoint Uninstaller)	Sophos	Sophos Endpoint Agent Setup <Ver> <Date> <Time>.txt
Sophos Endpoint Defense (SED)	Sophos	Sophos Endpoint Defense Setup <Ver> <Date> <Time>.txt
Sophos Endpoint Firewall Management (efw64)	Sophos	Sophos Endpoint Firewall <Ver> Install Log <Date> <Time>.txt

SOPHOS

Here you can see the log files for each of the components that are installed. Most of the log files are Sophos logs, however, some are MSI logs. We will look at why this is important shortly.

Review the logs, then click **Continue** to proceed.

## Component Log Files

Component	Log Type (MSI/Sophos)	Log Name
Sophos Endpoint Self Help	MSI	Sophos Endpoint Self Help Install Log <Date> <Time>.txt
Sophos File Scanner (SFS)	Sophos	Sophos File Scanner Install Log <Date> <Time>.txt
Sophos Health (SHS)	Sophos	Sophos Health <Ver> Install Log <Date> <Time>.txt
Sophos HitmanPro Alert (HMPA)	Sophos	Sophos HitmanPro Alert Initial Install Log <Date> <Time>.txt
Sophos Machine Learning Engine (ML)	Sophos	Sophos ML Engine Install Log <Date> <Time>.txt
	Sophos	Sophos ML Engine Validator Log <Date> <Time>.txt
Sophos Management Communications System (MCS)	Sophos	Sophos Management Communications System Install Log <Date> <Time>.txt
Sophos Network Threat Protection (NTP/SNTP)	Sophos	Sophos Network Threat Protection Install Log <Date> <Time>.txt
Sophos Standalone Engine (SSE)	Sophos	Sophos Standalone Engine Install Log <Date> <Time>.txt
		Sophos Standalone Engine Validator Log <Date> <Time>.txt
Sophos UI	Sophos	Sophos UI Install Log <Date> <Time>.txt

SOPHOS

Review the logs, then click **Continue** to proceed.

## Sophos Log Files

Search for...

fail

error

SOPHOS

We mentioned that there are two types of log, Sophos logs and MSI logs.

Sophos logs are from installers that do not use the Windows MSI installer. If you have an installation problem with one of these components you need to search the log file for the word fail, or error, to try and find the relevant entries to troubleshoot further.

## MSI Log Files

```
== Verbose logging started: 13/09/2022 11:56:25 Build type: SHIP UNICODE 5.00.10011.00 Calling process: C:\Program Files (x86)\Sophos\CloudInstaller\su-setup32.exe ===
MSI (c) (88:64) [11:56:25:257]: Cloaking enabled.
MSI (c) (88:64) [11:56:25:257]: Attempting to enable all disabled privileges before calling Install on Server
MSI (c) (88:64) [11:56:25:257]: End dialog not enabled
MSI (c) (88:64) [11:56:25:272]: Original package ==>
C:\ProgramData\Sophos\AutoUpdate\Cache\decoded\sau\Sophos AutoUpdate.msi
MSI (c) (88:64) [11:56:25:272]: Package we're running from ==>
C:\ProgramData\Sophos\AutoUpdate\Cache\decoded\sau\Sophos AutoUpdate.msi
MSI (c) (88:64) [11:56:25:272]: Machine policy value 'DisableUserInstalls' is 0
MSI (c) (88:64) [11:56:25:272]: APPCOMPAT: Compatibility mode property overrides found.
MSI (c) (88:64) [11:56:25:272]: APPCOMPAT: looking for appcompat database entry with ProductCode '{FA203C29-393F-4247-A69D-6C93E6D685EB}'.
MSI (c) (88:64) [11:56:25:272]: APPCOMPAT: no matching ProductCode found in database.
MSI (c) (88:64) [11:56:25:288]: MSCOREE not loaded loading copy from system32
MSI (c) (88:64) [11:56:25:319]: APPCOMPAT: looking for appcompat database entry with ProductCode '{FA203C29-393F-4247-A69D-6C93E6D685EB}'.
MSI (c) (88:64) [11:56:25:319]: APPCOMPAT: no matching ProductCode found in database.
MSI (c) (88:64) [11:56:25:319]: Transform are not secure.
MSI (c) (88:64) [11:56:25:335]: Note: 1: 2205 2: 3: Control
MSI (c) (88:64) [11:56:25:335]: PROPERTY CHANGE: Adding MsiLogFileLocation property. Its value is 'C:\Windows\TEMP\Sophos AutoUpdate 6.13.1014 Install Log 2022-09-13 10-56-25Z.txt'.
MSI (c) (88:64) [11:56:25:335]: No Command Line.
```

SOPHOS

Here is an example of an MSI log file. You can immediately see that it is an MSI log because the lines start with 'MSI'.



Additional information in  
the notes

# MSI Error Codes

Error Code	Codes Returned by MsiExec and Function Calls	Return Values	Description
ERROR_FUNCTION_NOT_CALLED	1626	0	A function could not be executed
ERROR_SUCCESS	0	1	An action completed successfully
ERROR_INSTALL_USEREXIT	1602	2	A user cancelled installation
ERROR_INSTALL_FAILURE	1603	3	A fatal error
ERROR_INSTALL_SUSPEND	1604	4	Installed suspended, incomplete
ERROR_SUCCESS	0	5	The action completed successfully
ERROR_INVALID_HANDLE_STATE	1609	6	The handle is in an invalid state
ERROR_INVALID_DATA	1626	7	The data is invalid
ERROR_INSTALL_ALREADY_RUNNING	1618	8	Another installation is in progress

Search MSI logs for '**return value 3**'

SOPHOS

When you are working with MSI log files you need to look for MSI error codes. You can see some of them here.

The one that is generally most useful is the fatal error MSI error code 1603, which logs a return value of 3. You can search for this in the MSI log to identify the relevant log entries to be able to troubleshoot further. When searching the logs, it's often useful to start at the bottom of the log and search upwards.

## [Additional Information]

<https://docs.microsoft.com/en-us/windows/win32/msi/error-codes>



Additional information in  
the notes

# Competitor Removal Tool (CRT)

Removes third-party security software to prevent conflicts

Performs a standard uninstall

CRT checks the uninstall section of the registry

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall  
HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

CRT logs to avremove.log in %TEMP% or C:\Windows\Temp

Products can be submitted to Sophos when not detected or removed by the CRT

SOPHOS

The CRT, or Competitor Removal Tool, is the component that will check for, and remove third-party security software to prevent conflicts.

The CRT will initiate a standard uninstall of the software using the information from the uninstall section of the registry. The registry locations are shown here. If the software has features that prevent an uninstall, like Sophos does with tamper protection, then the uninstall will most likely fail.

The CRT logs to avremove.log in the temp folder, and this will show any detected products and the result of trying to remove them. If the CRT is not detecting a product, or is unable to remove a product, it can be submitted to Sophos to be added.

For cases where the product's uninstallation is protected you may need to contact the vendor for instructions on how to remove it.

## [Additional Information]

The two registry locations CRT checks are:

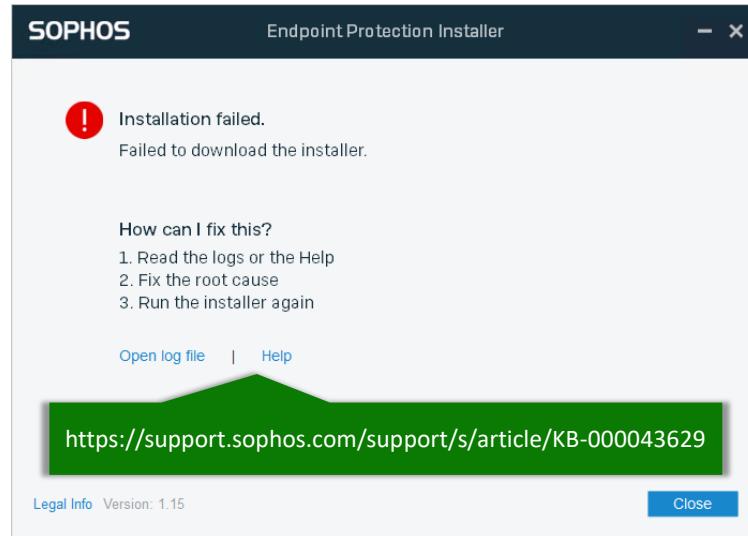
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\



Additional information in  
the notes



## Download Failed: Scenario 1



SOPHOS

Let's look at some examples of common installation issues and how to troubleshoot them.

The first issue is where the thin installer is unable to download the full stage 2 installer from Sophos Central.

The error screen provides a link to a knowledgebase article on getting started with log file locations and errors. There is also a link to open the SophosCloudInstaller log file.

### [Additional Information]

Identify the failing component to investigate further during installation failure **KB-000043629**.

<https://support.sophos.com/support/s/article/KB-000043629>



## Download Failed: Scenario 1

```
2022-09-20T13:05:13.6993844Z INFO : Detected architecture: 2
2022-09-20T13:05:13.6993844Z INFO : Using x86 program files for stage 2
2022-09-20T13:05:13.6993844Z INFO : Target path: C:\\Program Files (x86)\\Sophos\\CloudInstaller
2022-09-20T13:05:13.8243845Z INFO : About to delete: C:\\Program Files (x86)\\Sophos\\CloudInstaller
2022-09-20T13:05:13.8243845Z INFO : Folder not present, nothing to delete
2022-09-20T13:05:13.8243845Z INFO : Running on x64, requesting x86 Stage2
2022-09-20T13:05:13.8243845Z INFO : Sending HTTP 'POST' request to: api/download/stage2-
details/c7cbc8c3-daa5-4087-8a37-2ef4548b24fe
2022-09-20T13:05:13.8243845Z INFO : Did not discover an URL for a PAC file
2022-09-20T13:05:13.8243845Z INFO : Attempting to connect using proxy '' of type 'Empty Proxy'.
2022-09-20T13:05:13.8243845Z INFO : Set security protocol: 00000800
2022-09-20T13:05:13.8243845Z INFO : Opening connection to dqr-api-amzn-eu-west-1-9af7.api-
upe.p.hmr.sophos.com
2022-09-20T13:05:13.8243845Z INFO : Request content size: 30
2022-09-20T13:06:16.9528645Z ERROR : WinHttpSendRequest failed with error 12002
2022-09-20T13:06:16.9528645Z INFO : Failed to connect using proxy '' with error: WinHttpSendRequest
failed
2022-09-20T13:06:16.9528645Z INFO : Cleaning up extracted files
2022-09-20T13:06:16.9528645Z ERROR : Error downloading/running stage 2: Failed to get stage-2 info:
Failed to connect with any proxy
```

SophosCloudInstaller\_<Date>\_<Time>.log

SOPHOS

The SophosCloudInstaller log file shows that it did not identify a PAC file or proxy settings to use for the download, and that the download failed.

Click **Continue** when you are ready to proceed.

# Download Failed: Scenario 1



The screenshot shows the Windows Settings interface with the 'Network & Internet' section selected. A sub-menu for 'Proxy' is open, titled 'Manual proxy setup'. It displays a configuration form with the following details:

- Use a proxy server:** On
- Address:** 172.16.16.10
- Port:** 3128
- Excluded addresses:** An empty input field for specifying addresses that should not be proxied.
- Don't use the proxy server for local (intranet) addresses:**

At the bottom are 'Save' and 'Get help' buttons. To the right, a terminal window shows the command output of 'netsh winhttp show proxy':

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lucyfox>netsh winhttp show proxy
Current WinHTTP proxy settings:
    Direct access (no proxy server).

C:\Users\lucyfox>
```

In this scenario the device does not have direct Internet access and requires a proxy to be configured.

If we check the proxy settings, we can see that the user has a proxy for their browser.

If we check the system proxy settings using the **netsh winhttp show proxy** command, we can see that the device is set to direct access with no proxy settings.

## Download Failed: Scenario 1



```
Administrator: Command Prompt
C:\Windows\system32>netsh winhttp set proxy 172.16.16.10:3128
Current WinHTTP proxy settings:
Proxy Server(s) : 172.16.16.10:3128
Bypass List     : (none)

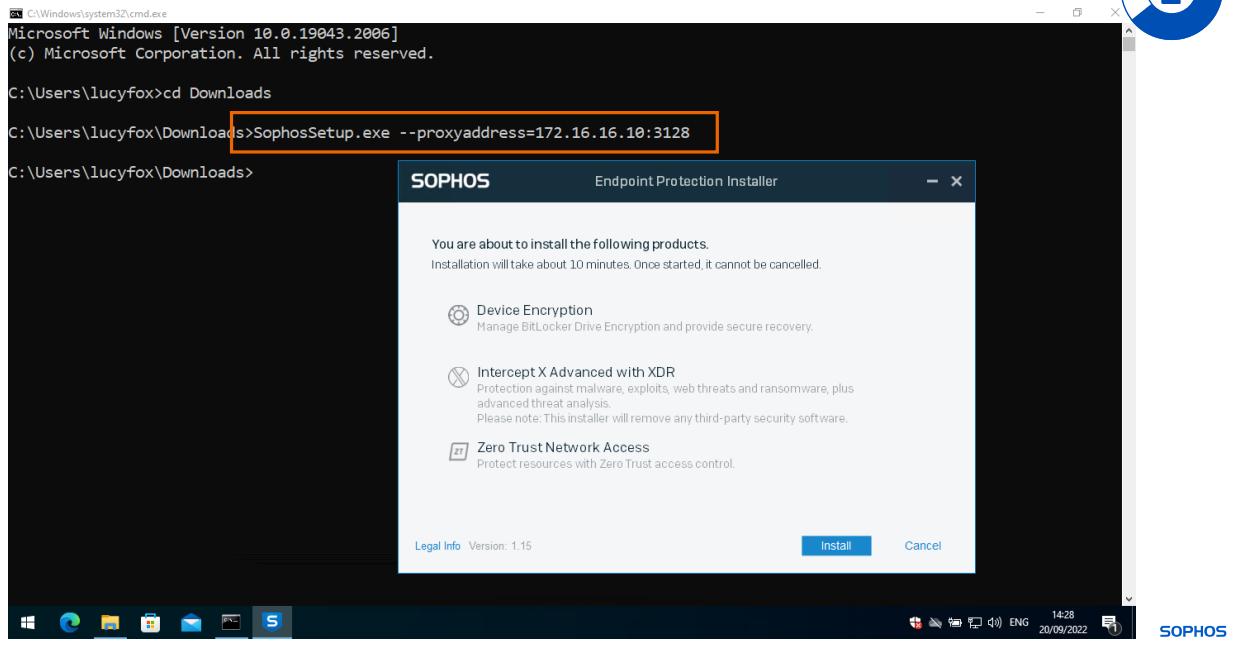
C:\Windows\system32>
```

SOPHOS

We can set the system proxy settings in an administrator command prompt window using the command **netsh winhttp set proxy**

You need to pass this command the IP or hostname of the proxy server and the port. It is also possible to import the proxy settings used by the browser using the command **netsh winhttp import proxy source=ie**.

## Download Failed: Scenario 1



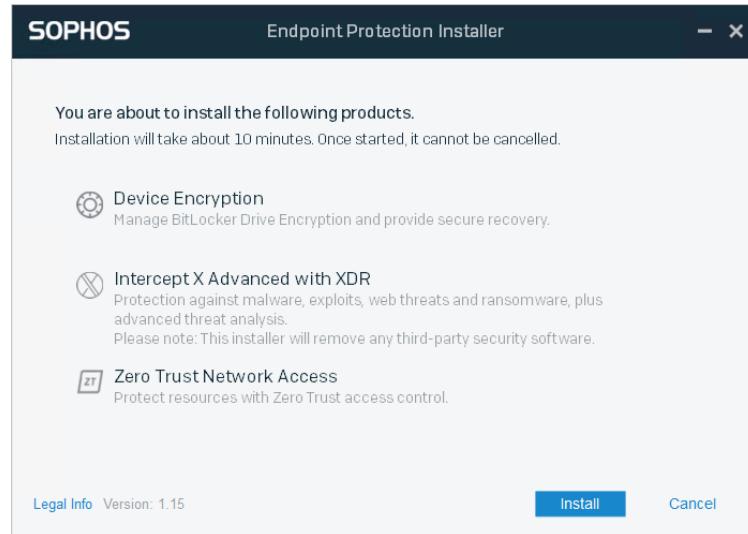
Another solution is to pass the proxy settings to Sophos Setup using the proxyaddress command line option. Doing this would allow Sophos Setup to download the Stage 2 Installer.

### [Additional Information]

Example: **SophosSetup.exe --proxyaddress=172.16.16.10:3128**

## Download Failed: Scenario 1

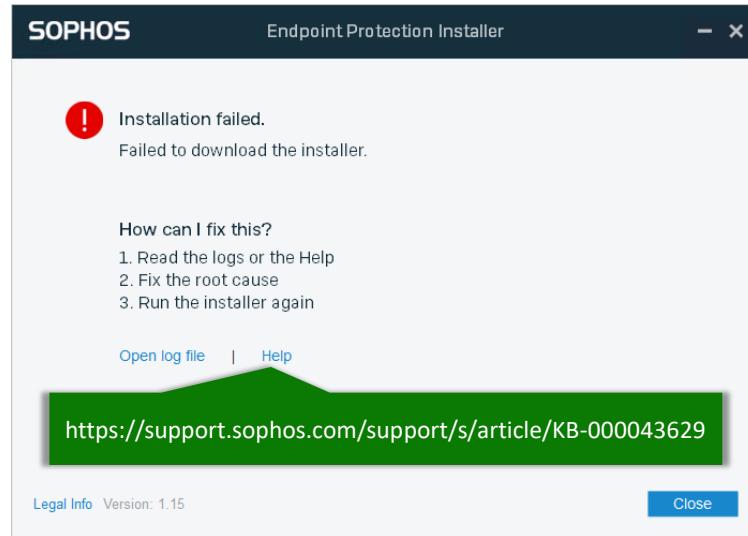
3



SOPHOS

With the proxy configured the thin installer can download the full stage 2 installer and the installation can continue to the next step.

## Download Failed: Scenario 2



SOPHOS

There are multiple reasons when the installer may not be able to download. We will look at another example now.



## Download Failed: Scenario 2

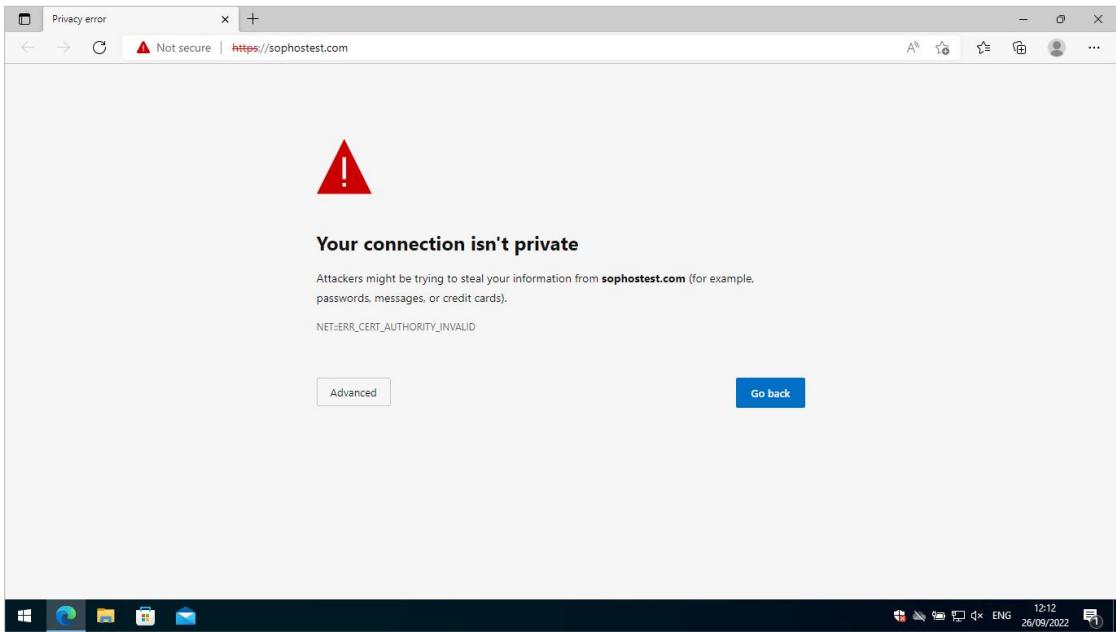
```
2022-09-26T10:40:11.7947417Z INFO : Did not discover an URL for a PAC file
2022-09-26T10:40:11.7947417Z INFO : Discovered the system proxy 172.16.16.250:3128
2022-09-26T10:40:11.7947417Z INFO : Attempting to connect using proxy '172.16.16.250:3128' of type
'System'.
2022-09-26T10:40:11.7947417Z INFO : Set security protocol: 00000800
2022-09-26T10:40:11.7947417Z INFO : Opening connection to dqr-api-amzn-eu-west-1-9af7.api-
upe.p.hmr.sophos.com
2022-09-26T10:40:11.7947417Z INFO : Request content size: 30
2022-09-26T10:40:11.9665080Z ERROR : WINHTTP_CALLBACK_STATUS_SECURE_FAILURE: 8
2022-09-26T10:40:11.9665080Z INFO : WINHTTP_CALLBACK_STATUS_SECURE_FAILURE:
WINHTTP_CALLBACK_STATUS_FLAG_INVALID_CA
2022-09-26T10:40:11.9665080Z ERROR : WinHttpSendRequest failed with certificate check failure and error
12175
2022-09-26T10:40:11.9665080Z INFO : Failed to connect using proxy '172.16.16.250:3128' with error:
WinHttpSendRequest failed: certificate check failure
2022-09-26T10:40:11.9665080Z INFO : Attempting to connect using proxy '' of type 'Empty Proxy'.
2022-09-26T10:40:11.9665080Z INFO : Set security protocol: 00000800
2022-09-26T10:40:11.9665080Z INFO : Opening connection to dqr-api-amzn-eu-west-1-9af7.api-
upe.p.hmr.sophos.com
2022-09-26T10:40:11.9665080Z INFO : Request content size: 30
2022-09-26T10:41:15.1696888Z ERROR : WinHttpSendRequest failed with error 12002
2022-09-26T10:41:15.1696888Z INFO : Failed to connect using proxy '' with error: WinHttpSendRequest
failed
```

SophosCloudInstaller\_<Date>\_<Time>.log

SOPHOS

In the SophosCloudInstaller log file we can see first that the installer is using a proxy, and then the error 'failed with certificate check failure and error 12175'.

## Download Failed: Scenario 2



If we try to access a HTTPS website in the browser we can see that we get a certificate error.

## Download Failed: Scenario 2



The screenshot shows a 'Certificate Viewer' window for the domain `sophostest.com`. The 'General' tab is selected. Key details shown include:

- Issued To:**
  - Common Name (CN): `sophostest.com`
  - Organization (O): <Not Part Of Certificate>
  - Organizational Unit (OU): <Not Part Of Certificate>
- Issued By:**
  - Common Name (CN): `SOPHOS TRAINING CA`
  - Organization (O): `Sophos`
  - Organizational Unit (OU): `Training`
- Validity Period:**
  - Issued On: Monday, June 20, 2022 at 1:00:00 AM
  - Expires On: Thursday, July 20, 2023 at 12:59:59 AM
- Fingerprints:**
  - SHA-256 Fingerprint: C2 71 34 01 03 69 8E 65 09 6C 50 9B 3B C9 BE 7E  
D1 4E 01 EC 91 DE 19 89 6A E5 8D 08 82 F6 46 E8
  - SHA-1 Fingerprint: 9A 23 7F 09 84 DD 26 E6 5F C6 EC A1 AD 48 6C C2  
79 09 07 65

If we look at the certificate we can see that it is being signed by an internal certificate authority that is not trusted.

The CA certificate should be downloaded and installed in the trusted root certificate authorities on this device.

## Download Failed: Scenario 2



SOPHOS

With the CA certificate installed you will see a different error when trying to install Sophos.

## Download Failed: Scenario 2



```
2022-09-26T13:18:30.6039011Z INFO : ValidateFileCertificateCheck: Validate certificate against file on  
WINHTTP CALLBACK STATUS SENDING REQUEST  
2022-09-26T13:18:30.6079025Z INFO : Subject certificate failed validation against root CA: SophosCA1  
2022-09-26T13:18:30.6079025Z INFO : Subject certificate failed validation against root CA: SophosCA2  
2022-09-26T13:18:30.6089011Z INFO : Subject certificate failed validation against root CA: Sophos  
SHA256 MCS Root CA3  
2022-09-26T13:18:30.6099010Z INFO : Subject certificate failed validation against root CA: Sophos  
SHA256 MCS Root CA4  
2022-09-26T13:18:30.6099010Z ERROR : Failed to validate server cert; terminating HTTP connection.  
2022-09-26T13:18:30.6119511Z ERROR : WinHttpSendRequest failed with certificate check failure and error  
12017  
2022-09-26T13:18:30.6129339Z INFO : Failed to connect using proxy '172.16.16.250:3128' with error:  
WinHttpSendRequest failed: certificate check failure  
2022-09-26T13:18:30.6129339Z INFO : Attempting to connect using proxy '' of type 'Empty Proxy'.  
2022-09-26T13:18:30.6139022Z INFO : Set security protocol: 00000800  
2022-09-26T13:18:30.6139022Z INFO : Opening connection to mcs2-cloudstation-eu-west-  
1.prod.hydra.sophos.com  
2022-09-26T13:18:30.6139022Z INFO : Sending request for connection confirmation through potential proxy  
2022-09-26T13:18:30.6149026Z INFO : Request content size: 0  
2022-09-26T13:20:36.7722693Z ERROR : WinHttpSendRequest failed with error 12002  
2022-09-26T13:20:36.7722693Z INFO : Failed to connect using proxy '' with error: WinHttpSendRequest  
failed  
2022-09-26T13:20:36.7722693Z ERROR : HTTP error: Failed to connect with any proxy: certificate check  
failure
```

SophosCloudInstaller\_<Date>\_<Time>.log

In the SophosCloudInstaller log file you can see that the installer is validating the certificate used on the connection against the Sophos certificates. The error below this is ‘failed with certificate check failure and error 12017’.

The issue here is that the Sophos installer not only requires a valid certificate, it requires that certificate to be signed by a Sophos authority. This is called certificate pinning.

## Download Failed: Scenario 2



The screenshot shows a Microsoft Edge browser window displaying the Sophos Certificate Viewer for the domain [www.sophos.com](https://www.sophos.com/en-us). The certificate details are as follows:

General	
Common Name (CN)	www.sophos.com
Organization (O)	SOPHOS LIMITED
Organizational Unit (OU)	<Not Part Of Certificate>
Issued By	SOPHOS TRAINING CA
Organization (O)	Sophos
Organizational Unit (OU)	Training

**Validity Period:**

Issued On	Wednesday, January 5, 2022 at 1:01:08 PM
Expires On	Monday, February 6, 2023 at 1:01:08 PM

**Fingerprints:**

SHA-256 Fingerprint	26 37 D3 2B 0D 47 52 C5 5A D9 9A 96 B7 82 25 3E F5 C3 44 1E AE 71 B4 88 66 A0 E1 24 A0 FD F6 02 AA 42 5E EF 50 93 3C B7 4B D7 0C 1C 49 22 94 3E E5 9A B0 CF
SHA-1 Fingerprint	

If we connect to a HTTPS site in a browser and view the certificate details we can see that it is signed by an internal CA. The device has the CA certificate and trusts it, but it is not signed by an acceptable CA for the installer.

To resolve this the Sophos domains need to be excluded from TLS inspection.

## Download Failed: Scenario 2



The screenshot shows a web browser window displaying the Sophos Certificate Viewer for the domain [www.sophos.com](https://www.sophos.com/en-us). The certificate details are as follows:

General	
Issued To	Common Name (CN) www.sophos.com Organization (O) SOPHOS LIMITED Organizational Unit (OU) <Not Part Of Certificate>
Issued By	Common Name (CN) GlobalSign Extended Validation CA - SHA256 - G3 Organization (O) GlobalSign nv-sa Organizational Unit (OU) <Not Part Of Certificate>
Validity Period	Issued On Wednesday, January 5, 2022 at 1:01:08 PM Expires On Monday, February 6, 2023 at 1:01:08 PM
Fingerprints	SHA-256 Fingerprint E1 16 3F 54 1D 85 F2 08 60 83 9E 06 EB 00 93 7C 93 EE 27 11 DB FC A5 C2 30 CD E3 71 EC 57 AF D8 28 97 3F 3C 5E D1 5F A7 18 84 C0 97 60 77 18 55 3B 60 7C E6

If the Sophos domains are excluded from TLS inspection you will see the original CA issuer on the certificate.

## Download Failed: Scenario 2

3



SOPHOS

With TLS inspection excluded for Sophos domains the installation can be completed.

# Failed to Remove Existing Security Software



Additional information in  
the notes



The screenshot shows a window titled "SOPHOS Endpoint Protection Installer". A yellow warning icon with an exclamation mark is displayed, followed by the text: "Installation succeeded with warnings. Action required". Below this, it says: "We can't remove ClamWin Free Antivirus 0.103.2.1. When you remove it, Sophos will automatically start protecting this device." A section titled "How can I fix this?" lists two steps: "1. Uninstall ClamWin Free Antivirus 0.103.2.1" and "2. Update Sophos software now, or wait for an automatic update". At the bottom, there are links "Open log file" and "Fix this problem ...", and buttons for "Legal Info", "Version: 1.15", and "Finish". A green callout box highlights the URL "https://support.sophos.com/support/s/article/KB-000034009".

SOPHOS

In this next scenario, the installation has succeeded; however, the CRT has failed to remove existing security software. This means that protection is not yet installed, but AutoUpdate will continue to try and install it, and when the third-party software is removed it will succeed and the device will be protected.

## [Additional Information]

List of third-party security software removed by Sophos KB-000034009.

<https://support.sophos.com/support/s/article/KB-000034009>

# Failed to Remove Existing Security Software



The screenshot shows two windows of the Sophos Central interface. The top window displays a summary card with an orange warning icon and the message "Update failed. Please contact IT." A blue "View details" button is highlighted with an orange border and a green arrow points down to the second window. The second window is titled "Events" and shows a list of log entries. One entry is highlighted with an orange border: "Sophos Third-party Security Software Removal Tool v0.1.25 failed to install" on 21/09/2022 at 12:02:21.

Date	Description
21/09/2022 12:03:34	Updates will complete when you restart. Meanwhile, your computer is still protected
21/09/2022 12:02:21	Sophos Third-party Security Software Removal Tool v0.1.25 failed to install

You can also see the installation failure in the Sophos Endpoint Agent.

# Failed to Remove Existing Security Software



```
2022-09-21T10:57:51.4799023Z ERROR : SetupPluginCommand::onRun() failed with  
ComponentInstaller::InstallError: Failed to install component(s): CRTSETUP  
2022-09-21T10:57:51.4799023Z INFO : Extracting CRT result from:  
C:\\\\Users\\\\lucyfox\\\\AppData\\\\Local\\\\Temp\\\\TelemetryConfig.json  
2022-09-21T10:57:51.4799023Z INFO : Command 'SetupPlugin' completed with failure with reboot code '0'  
and error message 'Could not install software'.  
2022-09-21T10:57:51.4799023Z ERROR : Installation failed.  
2022-09-21T10:57:51.4799023Z INFO : Sending HTTP 'POST' request to:  
sophos/management/ep/install/events/endpoint/8a1b6601-22e8-4468-3a64-456c2271f905  
2022-09-21T10:57:51.5423754Z INFO : Did not discover an URL for a PAC file  
2022-09-21T10:57:51.5423754Z INFO : Discovered the system proxy 172.16.16.10:3128  
2022-09-21T10:57:51.5423754Z INFO : Attempting to connect using proxy '172.16.16.10:3128' of type  
'System'.  
2022-09-21T10:57:51.5423754Z INFO : Set security protocol: 00000800  
2022-09-21T10:57:51.5423754Z INFO : Opening connection to mcs2-cloudstation-eu-west-  
1.prod.hydra.sophos.com  
2022-09-21T10:57:51.5423754Z INFO : Sending request for connection confirmation through potential proxy  
2022-09-21T10:57:51.5423754Z INFO : Request content size: 0  
2022-09-21T10:57:51.6673742Z INFO : ValidateFileCertificateCheck: Validate certificate against file on  
WINHTTP_CALLBACK_STATUS_SENDING_REQUEST  
2022-09-21T10:57:51.6673742Z INFO : Subject certificate failed validation against root CA: SophosCA1  
2022-09-21T10:57:51.6673742Z INFO : Subject certificate failed validation against root CA: SophosCA2  
2022-09-21T10:57:51.6829992Z INFO : Certificate check succeeded  
2022-09-21T10:57:51.6829992Z INFO : ValidateFileCertificateCheck:
```

SophosCloudInstaller\_<Date>\_<Time>.log

If we look in the SophosCloudInstaller log file you will see that CRT has returned with 'installation failed'.

# Failed to Remove Existing Security Software



```
21 Sep 2022 11:56:32 Info: Detected ClamWin Anti-Virus version 0.93
21 Sep 2022 11:56:32 Info: =====
21 Sep 2022 11:56:32 Info: Removing detected products...
21 Sep 2022 11:56:32 Info: Checking to see if ClamWin Anti-Virus version 0.93 is installed
21 Sep 2022 11:56:32 Info: Starting removal of ClamWin Anti-Virus version 0.93
21 Sep 2022 11:56:32 Info: Creating new process "C:\Program Files (x86)\ClamWin\unins000.exe"
/VerySilent /NoRestart /SuppressMsgBoxes
21 Sep 2022 11:56:32 Failure: (2, 'CreateProcess', 'The system cannot find the file specified.')
21 Sep 2022 11:56:32 Failure: Removal of ClamWin Anti-Virus version 0.93 failed, last error 2
21 Sep 2022 11:56:32 Failure: Return code -1
21 Sep 2022 11:56:33 Info: Known publishers list contains 41 entries
21 Sep 2022 11:56:33 Info: Telemetry written to file:
C:\Users\lucyfox\AppData\Local\Temp\TelemetryConfig.json
21 Sep 2022 11:56:35 Info: Result of calling SubmitTelem: {"ErrorCode":0,"StatusCode":200}
21 Sep 2022 11:56:35 Info: Competitor Removal Tool exit code 17
21 Sep 2022 11:56:35 Info: AVRemove finished. 1 product found, 0 products removed. Report logged to :
C:\Users\lucyfox\AppData\Local\Temp\avremove.log
Sophos Anti-Virus software detector - Version 2.21.0.4
Copyright (C) 2003-2022 Sophos Limited. All rights reserved.
Running OS: Microsoft Windows 10 [Version 10.00.19043]
Removing detected products...
AVRemove finished. 1 product found, 0 products removed. Report logged to :
C:\Users\lucyfox\AppData\Local\Temp\avremove.log
```

avremove.log

To find out more details we need to check the avremove.log

Here we can see what software was detected, and the uninstallation process that was started.

In this example, the error returned is 'the system cannot find the file specified'.

# Failed to Remove Existing Security Software



HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall  
HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Name	Type	Data
DisplayName	REG_SZ	ClamWin Free Antivirus 0.103.2.1
HelpLink	REG_SZ	http://www.clamwin.com/
Inno Setup CodeFile	REG_SZ	anyone
Inno Setup: App Path	REG_SZ	C:\Program Files (x86)\ClamWin
Inno Setup: DeselectAll	REG_SZ	internationalhelp,internationalhelp\dutch,internationalhelp\french
Inno Setup: DeselectFile	REG_SZ	DownloadDB,desktopicon
Inno Setup: Icon Group	REG_SZ	ClamWin Antivirus
Inno Setup: SelectAll	REG_SZ	clamav,clamwin,explorershell
Inno Setup: SelectFile	REG_SZ	
Inno Setup: Setup Type	REG_SZ	typical
Inno Setup: Setup Version	REG_SZ	5.1.14
Inno Setup: User	REG_SZ	lucyfox
InstallDate	REG_SZ	20220921
InstallLocation	REG_SZ	C:\Program Files (x86)\ClamWin\
NoModify	REG_DWORD	0x00000001 (1)
NoRepair	REG_DWORD	0x00000001 (1)
Publisher	REG_SZ	alch
QuietUninstallString	REG_SZ	"C:\Program Files (x86)\ClamWin\unins000.exe" /SILENT
UninstallString	REG_SZ	"C:\Program Files (x86)\ClamWin\unins000.exe"
URLInfoAbout	REG_SZ	http://www.clamwin.com/
URLUpdateInfo	REG_SZ	http://www.clamwin.com/

If we look in the uninstall section of the registry we can find the product that was detected and the uninstall string CRT is using.

# Failed to Remove Existing Security Software



Name	Date modified	Type	Size
Common Files	21/09/2022 13:53	File folder	
HitmanPro.Alert	21/09/2022 13:59	File folder	
Internet Explorer	06/07/2022 16:42	File folder	
Microsoft	16/08/2022 11:31	File folder	
Microsoft.NET	07/12/2019 09:31	File folder	
Sophos	21/09/2022 13:54	File folder	
Windows Defender	06/07/2022 16:42	File folder	
Windows Mail	06/07/2022 16:42	File folder	
Windows Media Player	06/07/2022 16:42	File folder	
Windows Multimedia Platform	07/12/2019 09:52	File folder	
Windows NT	07/12/2019 09:49	File folder	
Windows Photo Viewer	18/08/2022 17:36	File folder	
Windows Portable Devices	07/12/2019 09:52	File folder	
WindowsPowerShell	07/12/2019 09:31	File folder	

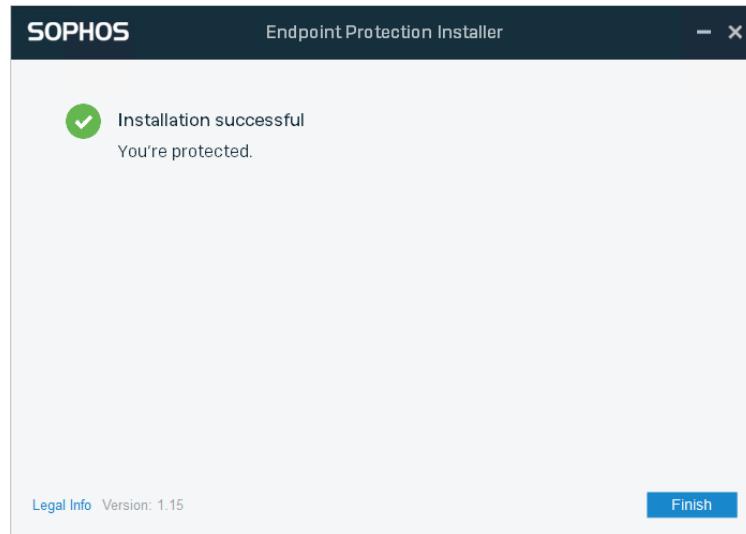
SOPHOS

As the error was that the file can not be found we can look for it. In this case the files for the installation are not present. The most likely cause would be that the registry entries are left over from a previous installation.

As the product is not installed, we can remove the registry entries. We recommend taking a backup before making any changes to the registry.

## Failed to Remove Existing Security Software

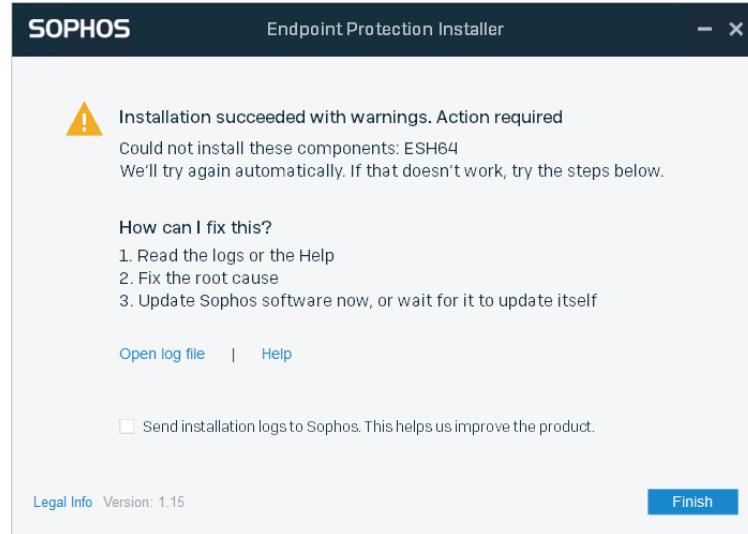
3



SOPHOS

With the registry entries removed the installation can complete.

# Failed to Install Component



SOPHOS

The last example we will look at in this chapter is where one of the components fails to install.

The error is that the installation succeeded, but it shows that one of the components could not install. In this example this is ESH64. This is Endpoint Self Help.

AutoUpdate will continue to try and install this component on each update. If the issue preventing the installation is resolved it will be installed.

# Failed to Install Component



```
022-09-27T15:09:36.7726729Z INFO : Installing Component: esh64
2022-09-27T15:09:36.7726729Z INFO : setupDll='setup.dll'; setupExe='su-setup32.exe'.
2022-09-27T15:09:36.922Z [ 9044: 2944] I Successfully established interface IProductSetup2.
2022-09-27T15:09:38.208Z [ 9044: 2944] I Reboot state: 0
2022-09-27T15:09:38.209Z [ 9044: 2944] W Failed to install product 7F682906-6E49-481B-89C5-2DCA36720F4F
3.2.339.0.
2022-09-27T15:09:38.2101921Z ERROR : su-setup: exit 1
2022-09-27T15:09:38.2101921Z INFO : Installed esh64: -2147213568 (reboot code: 0)
2022-09-27T15:11:38.2227745Z INFO : setupDll='setup.dll'; setupExe='su-setup32.exe'.
2022-09-27T15:11:38.362Z [ 884: 7172] I Successfully established interface IProductSetup2.
2022-09-27T15:11:39.203Z [ 884: 7172] I Reboot state: 0
2022-09-27T15:11:39.203Z [ 884: 7172] W Failed to install product 7F682906-6E49-481B-89C5-2DCA36720F4F
3.2.339.0.
2022-09-27T15:11:39.1965778Z ERROR : su-setup: exit 1
2022-09-27T15:11:39.1965778Z INFO : Installed esh64: -2147213568 (reboot code: 0)
2022-09-27T15:15:39.2116338Z INFO : setupDll='setup.dll'; setupExe='su-setup32.exe'.
2022-09-27T15:15:39.306Z [ 6688: 7048] I Successfully established interface IProductSetup2.
2022-09-27T15:15:40.063Z [ 6688: 7048] I Reboot state: 0
2022-09-27T15:15:40.063Z [ 6688: 7048] W Failed to install product 7F682906-6E49-481B-89C5-2DCA36720F4F
3.2.339.0.
2022-09-27T15:15:40.0699237Z ERROR : su-setup: exit 1
2022-09-27T15:15:40.0699237Z INFO : Installed esh64: -2147213568 (reboot code: 0)
2022-09-27T15:15:40.0699237Z ERROR : Installation failed
```

SophosCloudInstaller\_<Date>\_<Time>.log

The SophosCloudInstaller log file does not provide any additional useful information in this case, only showing which component failed to install.



## Failed to Install Component

```
MSI (s) (9C:7C) [16:15:39:663]: Executing op: FileCopy(SourceName=mqi73bxf.json|en-US.json,SourceCabKey=enUS.json,DestName=en-US.json,Attributes=512,FileSize=42629,PerTick=65536,,VerifyMedia=1,,,,CheckCRC=0,,,InstallMode=58982400,HashOptions=0,HashPart1=1463479269,HashPart2=423220646,HashPart3=191660229,HashPart4=1033789796,,)
MSI (s) (9C:7C) [16:15:39:663]: File: C:\Program Files\Sophos\Endpoint Self Help\Locale\en-US.json;
      To be installed; Won't patch;      No existing file
MSI (s) (9C:7C) [16:15:39:663]: Source for file 'en-US.json' is uncompressed, at
'C:\ProgramData\Sophos\AutoUpdate\Cache\decoded\esh64\Sophos\Endpoint Self Help\Locale\'.
MSI (s) (9C:7C) [16:15:39:983]: Note: 1: 1303 2: C:\Program Files\Sophos\Endpoint Self Help\Locale
MSI (s) (9C:7C) [16:15:39:983]: Product: Sophos Endpoint Self Help -- Error 1303. The installer has
insufficient privileges to access this directory: C:\Program Files\Sophos\Endpoint Self Help\Locale.
The installation cannot continue. Log on as administrator or contact your system administrator.

Error 1303. The installer has insufficient privileges to access this directory: C:\Program
Files\Sophos\Endpoint Self Help\Locale. The installation cannot continue. Log on as administrator or
contact your system administrator.
MSI (s) (9C:7C) [16:15:39:988]: Note: 1: 2265 2: 3: -2147287035
MSI (s) (9C:7C) [16:15:39:988]: User policy value 'DisableRollback' is 0
MSI (s) (9C:7C) [16:15:39:988]: Machine policy value 'DisableRollback' is 0
Action ended 16:15:39: InstallFinalize. Return value 3.
```

### Sophos Endpoint Self Help Install Log <Date><Time>.txt

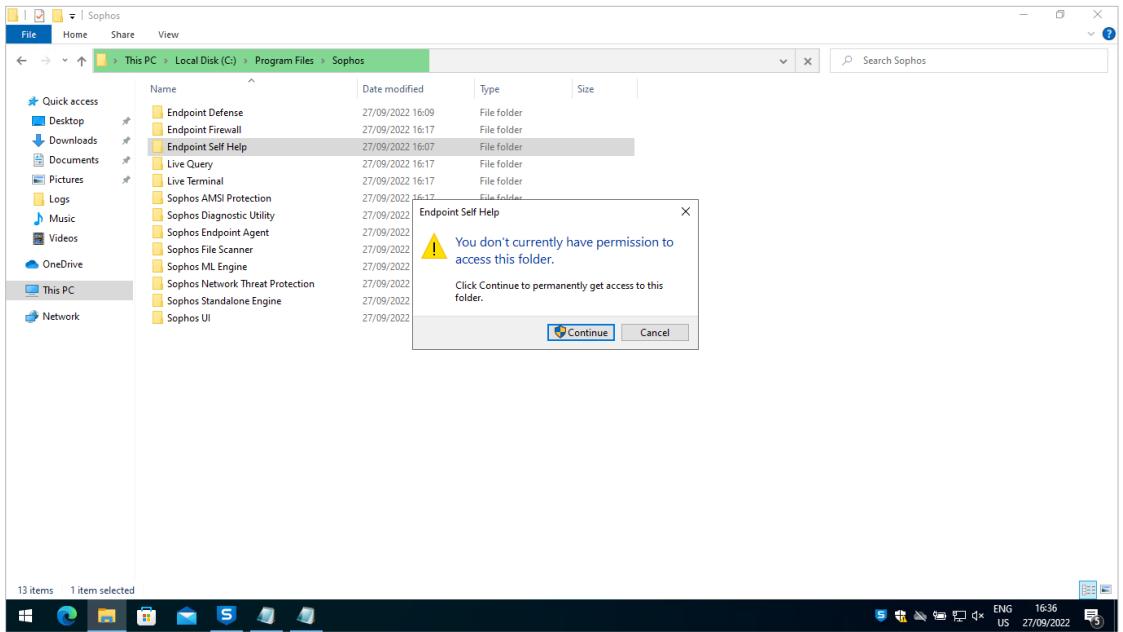
We need to look at the installation log for the component that will not install, in this example it is Endpoint Self Help.

This component has an MSI log file, which you can tell because of the MSI at the start of each line. As it is an MSI log file we can search for 'return value 3', which you can see highlighted at the bottom of this section.

Above this we can see the error encountered, 'the installer has insufficient privileges to access this directory'.

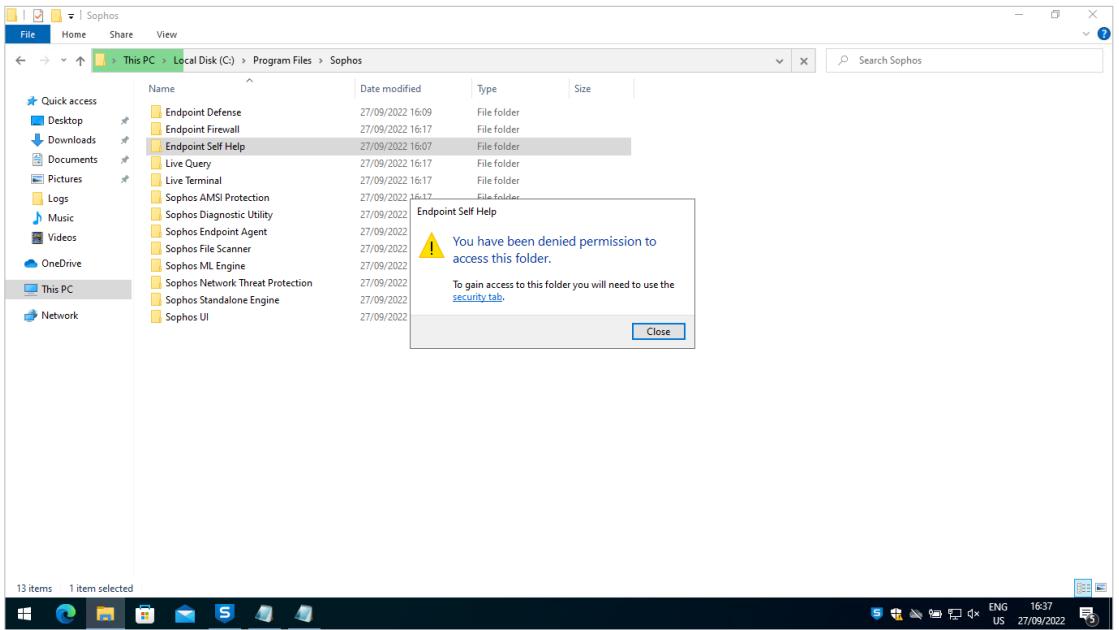
As the installation will be run as administrator or SYSTEM this should not be the case.

# Failed to Install Component



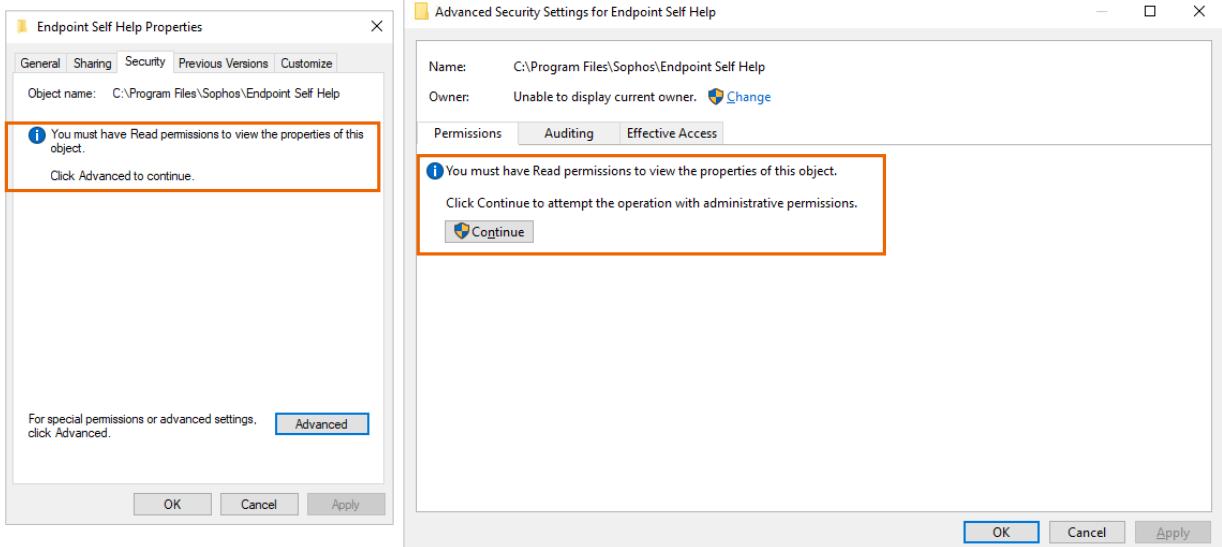
If we look at the permissions on the directory, we find we cannot access the Endpoint Self Help folder.

# Failed to Install Component



Clicking **Continue** to get access to the folder results in a denied error.

# Failed to Install Component



SOPHOS

If we take a look at the security permissions of the folder we can see that we don't have read permissions to the object.

Click **Advanced**, and then click **Continue** to attempt to access the permissions.

# Failed to Install Component



Advanced Security Settings for Endpoint Self Help

Name: C:\Program Files\Sophos\Endpoint Self Help  
Owner: Administrators (WINCLIENT1\Administrators) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	SYSTEM	Full control	None	This folder, subfolders and files
Deny	Administrators (WINCLIENT1...)	Full control	None	This folder, subfolders and files
Allow	Lucy Fox (lucyfox@ad.trainin...	Full control	None	This folder, subfolders and files
Allow	TrustedInstaller	Full control	C:\Program Files\	This folder and subfolders
Allow	SYSTEM	Full control	C:\Program Files\	This folder, subfolders and files
Allow	Administrators (WINCLIENT1...)	Full control	C:\Program Files\	This folder, subfolders and files
Allow	Users (WINCLIENT1\Users)	Read & execute	C:\Program Files\	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	C:\Program Files\	Subfolders and files only

Add Remove Edit

Disable inheritance

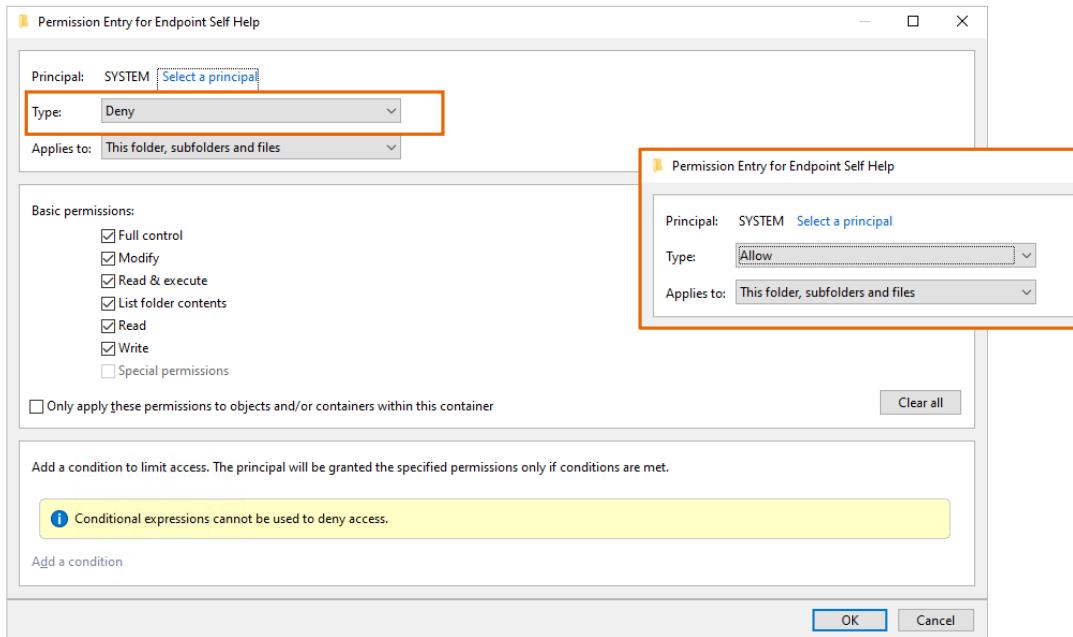
Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

SOPHOS

Here we can see that SYSTEM and Administrators have deny permissions on this folder. We will need to edit the permissions and correct this.

# Failed to Install Component



The permissions need to be changed from **Deny** to **Allow** for both SYSTEM and Administrators.

# Failed to Install Component

3

The screenshot shows two versions of the Sophos Endpoint agent interface side-by-side. Both interfaces have a dark header bar with the Sophos logo and navigation links: Status, Events, Detections, Settings, and a maximize/minimize/collapse button.

**Left Interface (Failed Update):**

- Update Status:** Shows a red warning icon and the message "Last update failed: 27 September 2022 16:17".
- Update Now:** A blue button.
- Products:** A table showing component names and versions:

Core Agent	2022.2.2.1
Sophos Intercept X	2022.11.22
Device Encryption	2022.1.0.58
ZTNA	2022.2.2.1
- Troubleshooting:** Links to "Open Endpoint Self Help Tool" and "Community forum".
- Legal Information:** Copyright 2014-2022 Sophos Limited. All rights reserved.
- Help | About:** Links at the bottom right.

**Right Interface (Successful Update):**

- Update Status:** Shows a green checkmark and the message "Last update: 27 September 2022 16:42".
- Update Now:** A blue button.

In the Sophos Endpoint agent click **Update Now**. AutoUpdate will check for updates and try to install the component, which will now succeed.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 3

Sophos uses certificate pinning. What do you need to do because of this?

Install the Sophos CA on endpoints

Exclude Sophos domains from TLS decryption

Ensure Sophos traffic does not pass through a proxy

Install the Sophos CA on your firewall

SOPHOS

## Question 2 of 3

What command can you run on Windows to see the current system proxy settings?

\_\_\_\_\_

## Question 3 of 3

A component failed to install. When you check the log file, it is an MSI log. What do you search for in the log?

\_\_\_\_\_

# Chapter Review

Both the **thin and full installers log** to the **SophosCloudInstall** log file located in the program data folder. **Component installation logs** are stored in the **temp directory**. Logs can be either Sophos or MSI logs. To search for errors in an **MSI log**, search for **return value 3**. In **Sophos logs**, search for **error** or **fail**.

Where a proxy is being used it should be **defined** in the **system proxy settings**. These are separate to the browser proxy settings. The **proxy can be passed to the installer through command line options**. Sophos domains should be excluded from TLS inspection as certificate pinning is used for security.

The **CRT checks the registry** for third-party security software and removes it to prevent conflicts. **Removal is completed using a standard uninstall**; however, this will not work if the installation has protection. The **CRT logs to the avremove.log** in the temp directory.

SOPHOS

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

Both the thin and full installers log to the SophosCloudInstall log file located in the program data folder. Component installation logs are stored in the temp directory; either the users temp directory or the Windows temp directory dependant on which user ran the installer. Logs can be either Sophos or MSI logs. To search for errors in an MSI log, search for return value 3. In Sophos logs, search for error or fail.

Where a proxy is being used it should be defined in the system proxy settings. These are separate to the browser proxy settings. The proxy can be passed to the installer through command line options. Sophos domains should be excluded from TLS inspection as certificate pinning is used for security.

The CRT checks the registry for third-party security software and removes it to prevent conflicts. Removal is completed using a standard uninstall; however, this will not work if the installation has protection. The CRT logs to the avremove.log in the temp directory.



# Troubleshooting Update Caches and Message Relays

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE2045: Troubleshooting 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.

# Troubleshooting Update Caches and Message Relays

In this chapter you will learn how to troubleshoot issues with Update Caches and Message Relays.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How an Update Cache Works
- ✓ How a Message Relay Works

DURATION     **6 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot issues with Update Caches and Message Relays.

# Update Cache Folders

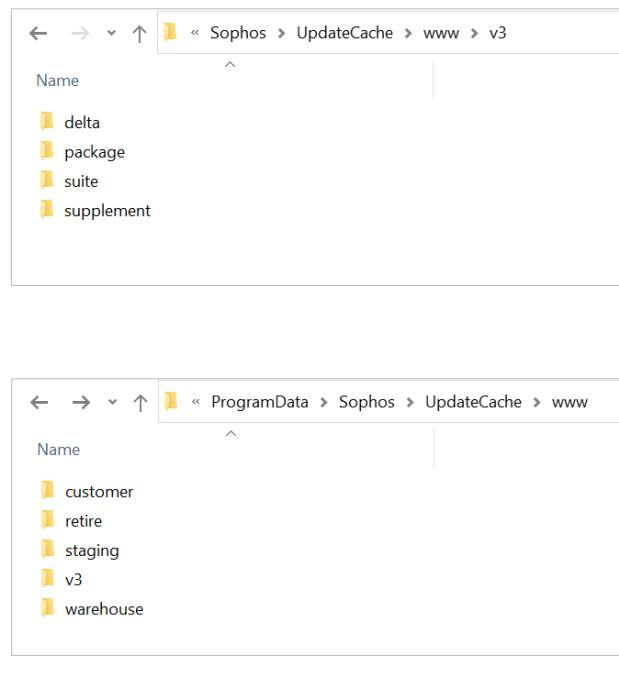
Locally cached data

C:\ProgramData\Sophos\UpdateCache\www\v3

- Delta\
- Package\
- Suite\
- Supplement\

Data is moved from the v3 local cache to the retire folder, if not requested for 3-days

- C:\ProgramData\Sophos\UpdateCache\www



SOPHOS

The Update Cache downloads data on request and stores the data in the v3 folder. Only suites and packages used by devices will be stored in the local cache.

Data from the local v3 cache will be moved to the 'retire' folder if no device has requested it for a period of 3 days. It will then remain in 'retire' for a further five days before it is purged from the disk, if not requested.

When a device updates and requests a file, if it is already stored in the local SDDS3 cache, it will be served from there. If it has been moved to the retire folder path due to the purge operation, it will be moved to the v3 cache and served from there. If it is not available in either location, a job request is submitted to download the file and place it in the local v3 cache.



Additional information in  
the notes

## Update Cache Log

uclog - Notepad

```
File Edit Format View Help
2022-08-05T10:43:03.024Z [10964] Info: [SystemHealth::EvaluateCacheHealth:48] No downloader history present
2022-08-05T10:43:03.024Z [10964] Info: [ActiveStateHandler::LaunchDownloaderProcess:290] Starting downloader from C:\Program Files\Sophos\UpdateCache\UpdateCacheDownload...
2022-08-05T11:54:26.869Z [10964] Info: [ActiveStateHandler::WaitForDownloaderProcessToEnd:374] Downloader completed (exit code=0)
2022-08-05T11:54:26.879Z [10964] Info: [FileSystem::AtomicWriteFile:224] Wrote 175 bytes to file C:\ProgramData\Sophos\UpdateCache\Status\downloader_history.xml
2022-08-05T11:54:26.880Z [10964] Info: [SystemHealth::EvaluateCacheHealth:96] Last record in downloader history is success
2022-08-05T11:54:26.881Z [10964] Info: [StateMachine::Run:52] State changing initial_download -> active
2022-08-05T11:54:26.882Z [10964] Info: [FileSystem::AtomicWriteFile:224] Wrote 493 bytes to file C:\ProgramData\Sophos\UpdateCache\Outbound\6028015_status.xml
2022-08-05T11:54:26.897Z [10964] Info: [FileSystem::AtomicWriteFile:224] Wrote 146 bytes to file C:\ProgramData\Sophos\UpdateCache>Status\current.xml
2022-08-05T11:54:26.898Z [10964] Info: ['anonymous-namespace':LogStarting:34] Active State Handler Running
2022-08-05T11:54:26.899Z [10964] Info: [SystemHealth::EvaluateCacheHealth:96] Last record in downloader history is success
2022-08-05T11:54:26.900Z [10964] Info: [HTTPServer::ConfigureSSL:167] Checking HTTP service configuration (port=8191)
2022-08-05T11:54:26.900Z [10964] Info: [HTTPServer::ConfigureSSL:173] Configuring SSL certificate
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:198] Starting HTTPServer...
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:199] Host: SRV2.sophos.local
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:200] Port: 8191
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:201] Data root path: C:\ProgramData\Sophos\UpdateCache\www
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:202] SDDS2 URL root: sophos
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:203] SDDS3 URL root: v3
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:204] Queue length: 10000
2022-08-05T11:54:26.926Z [10964] Info: [HTTPServer::Start:205] Primary source URL: https://sdds3.sophosupd.com
```

uclog - Notepad

```
File Edit Format View Help
2022-08-05T14:01:55.206Z [10964] Info: [ActiveStateHandler::LaunchDownloaderProcess:290] Starting downloader from C:\Program Files\Sophos\UpdateCache\UpdateCacheDownload...
2022-08-05T14:08:17.381Z [10700] Info: [HTTPServer::ProcessMissingSdds3Resource:994] Submitted download request for file suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat...
2022-08-05T14:08:17.386Z [1064] Info: [FileDownloaderBase::Download:124] Downloading resource suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat...
2022-08-05T14:08:17.393Z [ed0] Info: [FileDownloaderBase::Download:124] Downloading resource suite/sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat...
2022-08-05T14:08:17.394Z [10e24] Info: [HTTPServer::ProcessMissingSdds3Resource:994] Submitted download request for file suite/sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe...
2022-08-05T14:08:17.469Z [1064] Info: ['anonymous-namespace':http_save_to_file:94] http_save_to_file => size: 3923 bytes, elapsed: 12 ms, sleep: 0 ms, average rate: 2554
2022-08-05T14:08:17.506Z [ed0] Info: ['anonymous-namespace':http_save_to_file:94] http_save_to_file => size: 11398 bytes, elapsed: 38 ms, sleep: 0 ms, average rate: 2345
2022-08-05T14:08:19.523Z [10b58] Info: [FileDownloaderBase::Download:124] Downloading resource suite/sdds3.WindowsCloudClean_1.0.42.55133bcba5.dat...
2022-08-05T14:08:19.523Z [10700] Info: [HTTPServer::ProcessMissingSdds3Resource:994] Submitted download request for file suite/sdds3.WindowsCloudClean_1.0.42.55133bcba5.c...
2022-08-05T14:08:19.550Z [10b58] Info: ['anonymous-namespace':http_save_to_file:94] http_save_to_file => size: 3918 bytes, elapsed: 16 ms, sleep: 0 ms, average rate: 191
2022-08-05T14:08:21.671Z [1fb4] Info: [FileDownloaderBase::Download:124] Downloading resource suite/sdds3.WindowsCloudEncryption_2022.1.0.41.0e40ef1531.dat...
```

< Ln 132, Col 159 90% Windows (CRLF) UTF-8 >

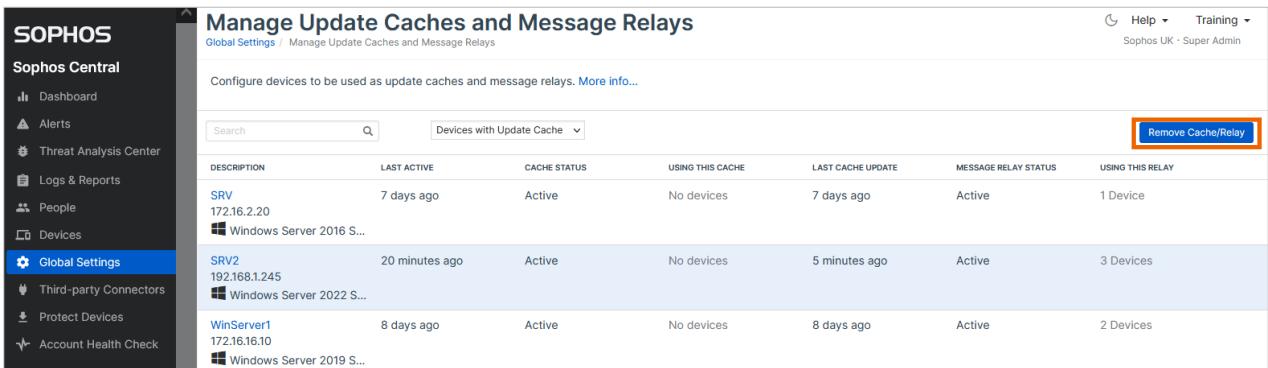
If a problem is suspected with an Update Cache, information can be found in the uc.log,

The uc.log shows a summary of the connections made and whether they were successful. It also contains details of download requests for files that are not in the cache.

### [Additional Information]

The uc.log can be found in this directory: %ProgramData%\Sophos\UpdateCache\Logs\

# Removing An Update Cache/Message Relay



The screenshot shows the Sophos Central interface under 'Global Settings'. In the left sidebar, 'Global Settings' is selected. The main page title is 'Manage Update Caches and Message Relays'. It displays a table of devices configured as update caches and message relays. The columns are: DESCRIPTION, LAST ACTIVE, CACHE STATUS, USING THIS CACHE, LAST CACHE UPDATE, MESSAGE RELAY STATUS, and USING THIS RELAY. Three devices are listed: SRV1 (Active, 7 days ago), SRV2 (Active, 20 minutes ago), and WinServer1 (Active, 8 days ago). The 'Remove Cache/Relay' button is located at the top right of the table's header row.

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY STATUS	USING THIS RELAY
SRV 172.16.2.20 Windows Server 2016 S...	7 days ago	Active	No devices	7 days ago	Active	1 Device
SRV2 192.168.1.245 Windows Server 2022 S...	20 minutes ago	Active	No devices	5 minutes ago	Active	3 Devices
WinServer1 172.16.16.10 Windows Server 2019 S...	8 days ago	Active	No devices	8 days ago	Active	2 Devices

- Uninstalls the caching and message relay software
- Removes the downloaded cache files
- Removes the Windows Firewall rules
- Removes the device as an available update location/relay for all computers

SOPHOS

If you no longer want a server to act as an update cache you can remove the cache in **Global Settings > Manage Update Caches and Message Relays**, by selecting the device and clicking **Remove Cache/Relay**. Please note that if the server is also a message relay, the message relay function will also be removed as an update cache is a requirement for message relay.

When you remove an update cache, it will:

- Uninstall the caching and message relay software
- Remove the downloaded cache files
- Remove the Windows Firewall rules
- Remove the device as an available update location or relay for all computers

Once the actions are complete, any existing settings are cleared, and the 'Cache Status' changes to 'Not installed'.

# Troubleshooting Scenarios

SOPHOS

We will now look at some update cache troubleshooting scenarios.

# Update Cache ‘Last Updated’ Time in the Future



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...](#)

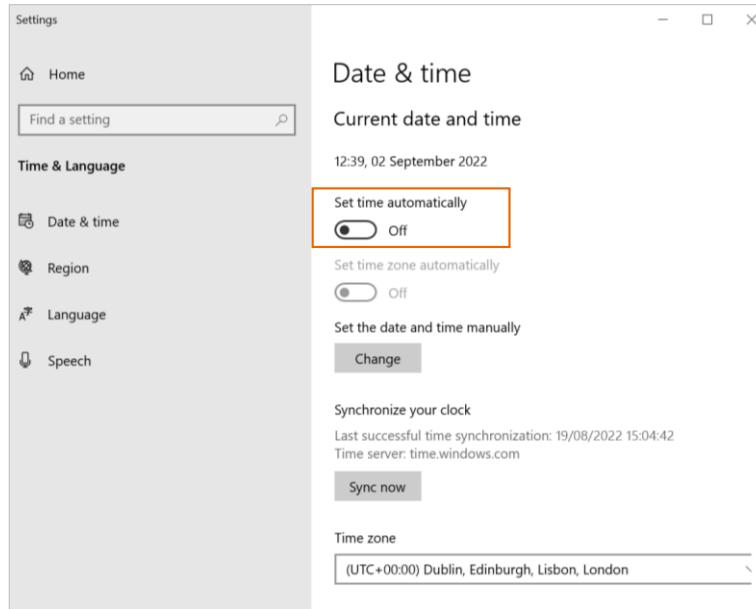
DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY STATUS	USING THIS RELAY
SRV3 192.168.1.166 Windows Server 2022 S...	an hour ago	Active	3 Devices	in 2 days	Active	2 Devices
WinServer1 172.16.16.10 Windows Server 2019 S...	20 hours ago	Active	2 Devices	20 hours ago	Active	6 Devices

Search

SOPHOS

In our first scenario, the update cache is showing a ‘Last Cache Update’ time in the future.

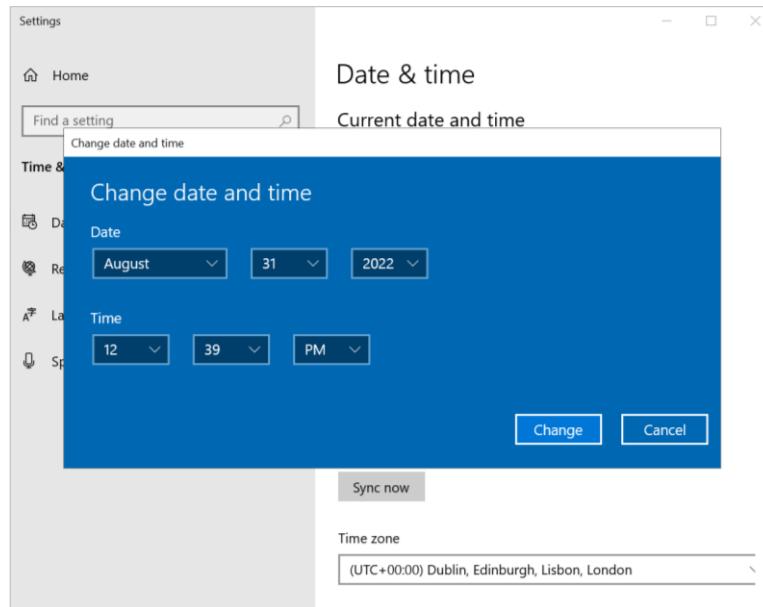
# Check Date & Time Settings



SOPHOS

The update cache device has automatic date and time configuration disabled.

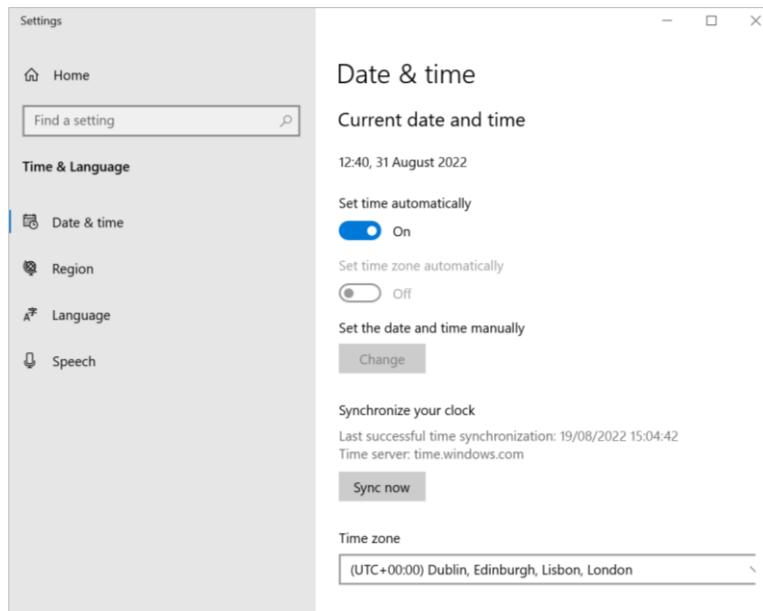
## Modify the Incorrect Date



SOPHOS

The date and time have been incorrectly configured and can be manually changed. The status of the update cache will be corrected after the next update.

## Set Time Automatically



SOPHOS

The Windows Time service synchronizes the date and time for all computers managed by Active Directory Domain Services. A device that is configured to **Set time automatically** uses a Windows time server if it is not a member of a domain.



## Update Cache Renamed

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 STATUS	USING
SRV 172.16.2.20 Windows Server 2016 S...	11 days ago	Active	No devices	11 days ago	Active	1 Dev
SRV3 192.168.1.166 Windows Server 2022 S...	31 minutes ago	Active	1 Device	an hour ago	Active	3 Dev
WinServer1 172.16.16.10 Windows Server 2019 S...	13 days ago	Active				

SOPHOS Endpoint Self Help

Status Tools

Health State

- System
- Installed Components
- Services
- Management Communication
- Update
- Policy

Update Status

Latest Update 17:53:08 Sep 18, 2022 (UTC+01:00)

Update Configuration

Update Location srv3:8191

Proxy No proxy used

Remediation

For help with issues reported on this page, see [Knowledge Base Article KB-000036449](#)

Did this help you? Yes

SOPHOS

Our second scenario looks at what happens if the server hosting an update cache is re-named. The server is named SRV3 and is used by endpoints for updating. The administrator wants to re-name the server to comply with new naming conventions.



# Update Cache Renamed

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 STATUS	USING
READING3 192.168.1.66 Windows Server 2022 S...	44 minutes ago	Active	1 Device	19 minutes ago	Active	3 Dev
SRV 172.16.2.20 Windows Server 2016 S...	11 days ago	Active	No devices	12 days ago	Active	1 Dev
WinServer1 172.16.16.10 Windows Server 2019 S...	13 days ago	Active				

SOPHOS Endpoint Self Help

Status Tools

Health State

System

Installed Components

Services

Management Communication

Update

Policy

Update Status

Latest Update 18:28:55 Sep 18, 2022 (UTC+01:00)

Update Configuration

Update Location Sophos

Proxy No proxy used

Remediation

For help with issues reported on this page, see [Knowledge Base Article KB-000036449](#)

Did this help you? Yes

SOPHOS

The update cache has the same IP address but is now named READING3. Devices are no longer able to resolve the update cache, and in this scenario have switched to Sophos for updates.

# Update Cache Renamed



The screenshot shows the Sophos Central interface for managing update caches and message relays. The left sidebar has 'Global Settings' selected. The main page title is 'Manage Update Caches and Message Relays'. It displays a table of devices configured as update caches or message relays. The columns are: DESCRIPTION, LAST ACTIVE, CACHE STATUS, USING THIS CACHE, LAST CACHE UPDATE, MESSAGE RELAY STATUS, and USING. Three rows are listed:

DESCRIPTION	LAST ACTIVE	CACHE STATUS	USING THIS CACHE	LAST CACHE UPDATE	MESSAGE RELAY STATUS	USING
AppServer 172.16.2.20 Windows Server 2016 S...	3 days ago	Not installed				Not installed
DC 192.168.1.94 Windows Server 2022 S...	an hour ago	Not installed				Not installed
READING3 192.168.1.166 Windows Server 2022 S...	14 minutes ago	Not installed				Not installed

To resolve this, the update cache must be removed and deployed again.

# Update Cache Renamed



The screenshot shows the Sophos Central interface with the 'Global Settings' menu item selected in the sidebar. A modal window titled 'Assign Devices Manually' is open, displaying two lists of devices: 'AVAILABLE DEVICES' on the left and 'ASSIGNED DEVICES' on the right. The 'AVAILABLE DEVICES' list contains 18 items, including 'AppServer', 'linux-av', 'linux-puppet-agent', 'linux-puppet-server', 'linuxserver1', 'MN-5035A1148964', 'READING3', 'SophosLab-725301', and 'SRV'. The 'ASSIGNED DEVICES' list contains 2 items, 'DC' and 'Training-W10'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

SOPHOS

Before removing the update cache, it is important to check which devices (if any) are manually assigned to the update cache so that these settings can be re-applied.

# Update Cache Renamed

3

The screenshot shows the Sophos Endpoint Self Help interface. On the left, a sidebar lists navigation options: Health State, System, Installed Components, Services, Management Communication, Update, Policy, and Server. The 'Update' option is selected and highlighted with a right-pointing arrow. The main content area displays 'Update Status' with a green checkmark and 'Latest Update' at 18:32:37 Sep 19, 2022 (UTC+01:00). Below this is 'Update Configuration' with two items: 'Update Location' set to 'reading3:8191' (highlighted with a red box) and 'Proxy' set to 'No proxy used'. Under 'Remediation', there's a link to 'Knowledge Base Article KB-000036449'. At the bottom, there are 'Launch SDU' and 'Refresh' buttons, and a 'Did this help you?' poll with 'Yes' selected.

SOPHOS

The device is now using the READING3 update cache server as its update location.

# Windows Firewall Rule Not Created



```
SophosUpdate - Notepad
File Edit Format View Help
2022-10-08T17:57:09.036Z [ 5976: 7720] I Analyzing whether to update from Sophos CDN or update cache
2022-10-08T17:57:09.091Z [ 5976: 7720] I Successfully connected to cache: https://reading3:8191/v3/suite
2022-10-08T17:57:09.091Z [ 5976: 7720] I Analysis complete - Using update cache: reading3:8191
2022-10-08T17:57:09.091Z [ 5976: 7720] I Syncing from: https://reading3:8191/v3
2022-10-08T17:57:09.348Z [ 5976: 7720] I Refreshing supplement sdds3.CEPNGSRVFLAGS.dat
2022-10-08T17:57:09.389Z [ 5976: 7720] I GET https://reading3:8191/v3/supplement/sdds3.CEPNGSRVFLAGS.dat: 200 (6754 bytes)
2022-10-08T17:57:09.407Z [ 5976: 7720] I Refreshing supplement sdds3.NTP_OVERRIDE.dat
2022-10-08T17:57:09.434Z [ 5976: 7720] I GET https://reading3:8191/v3/supplement/sdds3.NTP_OVERRIDE.dat: 200 (4033 bytes)
2022-10-08T17:57:09.451Z [ 5976: 7720] I Refreshing supplement sdds3.EPIPS_data.dat
2022-10-08T17:57:09.477Z [ 5976: 7720] I GET https://reading3:8191/v3/supplement/sdds3.EPIPS_data.dat: 200 (4122 bytes)
2022-10-08T17:57:09.498Z [ 5976: 7720] I Refreshing supplement sdds3.ScheduledQueryPack.dat
< Ln 1, Col 1 100% Windows (CRLF) UTF-8 >
```

```
SophosUpdate - Notepad
File Edit Format View Help
2022-10-08T18:05:41.906Z [ 8860: 4364] I Analyzing whether to update from Sophos CDN or update cache
2022-10-08T18:05:48.445Z [ 8860: 4364] I Could not reach cache: https://reading3:8191/v3/suite: WinHttpSendRequest failed: The
2022-10-08T18:05:48.445Z [ 8860: 4364] I Analysis complete - Using Sophos CDN
2022-10-08T18:05:48.445Z [ 8860: 4364] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy>
2022-10-08T18:05:48.526Z [ 8860: 4364] I 200 from https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudServerAV_1.3.95.273bb7fbt
2022-10-08T18:05:48.526Z [ 8860: 4364] I Syncing from: https://sdds3.sophosupd.com
2022-10-08T18:05:48.785Z [ 8860: 4364] I Refreshing supplement sdds3.CEPNGSRVFLAGS.dat
2022-10-08T18:05:48.815Z [ 8860: 4364] W GET https://sdds3.sophosupd.com/supplement/sdds3.CEPNGSRVFLAGS.dat: discarding cached
2022-10-08T18:05:49.093Z [ 8860: 4364] I GET https://sdds3.sophosupd.com/supplement/sdds3.CEPNGSRVFLAGS.dat: 200 (6754 bytes)
2022-10-08T18:05:49.112Z [ 8860: 4364] I Refreshing supplement sdds3.NTP_OVERRIDE.dat
2022-10-08T18:05:49.142Z [ 8860: 4364] W GET https://sdds3.sophosupd.com/supplement/sdds3.NTP_OVERRIDE.dat: discarding cached
< Ln 1, Col 1 100% Windows (CRLF) UTF-8 >
```

SOPHOS

In our last scenario we will look at an issue where starting the Windows Firewall service prevents endpoints from connecting to the update cache.

# Windows Firewall Rule Not Created



The screenshot shows the Windows Defender Firewall with Advanced Security window. The left sidebar has options for Inbound Rules, Outbound Rules, Connection Security Rules, and Monitoring. The main area displays the 'Inbound Rules' table:

Name	Group	Profile	Enabled	Action
SNMP Trap Service (UDP In)	SNMP Trap	Private...	No	Allow
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow
Software Load Balancer Multiplexer (TCP-In)	Software Load Balancer	All	No	Allow
Start	Start	Domai...	Yes	Allow
Start	Start	Domai...	Yes	Allow
Start	Start	Domai...	Yes	Allow
TPM Virtual Smart Card Management (DC...	TPM Virtual Smart Card Man...	Private...	No	Allow
TPM Virtual Smart Card Management /DC	TPM Virtual Smart Card Man...	Domain	No	Allow

The Actions pane on the right lists: New Rule..., Filter by Profile, Filter by State, Filter by Group, View, Refresh, and Export List... .

If the Windows Firewall service is running when the update cache is installed, it will automatically create the rule to allow TCP 8191 that is needed for clients to connect. In this scenario, the firewall service was not running during installation but has now been started and the firewall is enabled. Clients are unable to connect as the Sophos update cache rule does not exist.

# Windows Firewall Rule Not Created

3

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has options for Inbound Rules, Outbound Rules, Connection Security Rules, and Monitoring. The main area displays the 'Inbound Rules' table. The table has columns: Name, Group, Profile, Enabled, and Action. Several rules are listed, including 'SNMP Trap Service (UDP In)', 'Software Load Balancer Multiplexer (TCP-In)', and three entries starting with 'Start'. The 'Sophos Message Relay' and 'Sophos Update Cache' entries are highlighted with a red box. The right sidebar contains an 'Actions' section with options like 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', and 'Export List..'. The bottom right corner of the window has the 'SOPHOS' logo.

Name	Group	Profile	Enabled	Action
SNMP Trap Service (UDP In)	SNMP Trap	Domain	No	Allow
SNMP Trap Service (UDP In)	SNMP Trap	Private,...	No	Allow
Software Load Balancer Multiplexer (TCP-In)	Software Load Balancer	All	No	Allow
Sophos Message Relay	Sophos	All	Yes	Allow
Sophos Update Cache	Sophos	All	Yes	Allow
Start	Start	Domai...	Yes	Allow
Start	Start	Domai...	Yes	Allow
Start	Start	Domai...	Yes	Allow

- Restart the Update Cache and Message Relay services. Did it work?
- No? Restart the server. Did it work?
- No? Remove and reinstall Update Cache and Message Relay

To resolve the issue:

- Restart the Sophos update cache and Sophos message relay Service. Check to see if the Firewall rules have been added
- If not, restart the server and check again
- If the rules are still not listed, remove and reinstall the update cache and message relay



Additional information in  
the notes

# Windows Firewall Rule Not Created

The screenshot shows two windows. The top window is the Windows Services (Local) application. It lists various services, with 'Windows Defender Firewall' selected. A context menu is open over this service, with 'All Tasks' highlighted. The bottom window is a Command Prompt window titled 'Administrator: Command Prompt'. It shows the command 'net stop mpssvc' being run, followed by an error message indicating that pausing, continuing, or stopping the service is not valid.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.887]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net stop mpssvc
The requested pause, continue, or stop is not valid for this service.

More help is available by typing NET HELPMSG 2191.

C:\Users\Administrator>
```

In current versions of Windows, it is not possible to stop the Windows Defender Firewall service so the required rules for the Update Cache will be created. Older versions of Windows, such as Server 2016 allow the service to be stopped and disabled.

## [Additional Information]

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

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 3

Which 2 of the following are true if the device hosting an Update Cache has been renamed?

Clients will no longer be able to use the Update Cache

Clients must be manually assigned

The name shown in Central must be changed

The Update Cache must be redeployed

SOPHOS



## Question 2 of 3

How often is data purged from the V3 cache folder?

2 days

3 days

5 days

8 days

SOPHOS

## Question 3 of 3

What is the name of the Update Cache log file?

# Chapter Review

The **uc.log** shows a **summary of the connections** made and whether they were successful. It also contains details of **download requests** for files that are not in the cache.

If a device hosting an **update cache** is **renamed**, the update cache must be **removed and reinstalled**.

If a server is a **message relay**, this will also be **removed if the update cache** is removed. Update cache is a requirement for message relay.

SOPHOS

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

The uc.log shows a summary of the connections made and whether they were successful. It also contains details of download requests for files that are not in the cache.

If a device hosting an update cache is renamed, the update cache must be removed and reinstalled.

If a server is a message relay, this will also be removed if the update cache is removed. Update cache is a requirement for message relay



# Troubleshooting Sophos Central Updating

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE2015: Troubleshooting 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.

# Troubleshooting Sophos Central Updating

In this chapter you will learn techniques that can be used to troubleshoot Central Updating

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How Sophos Central Updates

DURATION     **9 minutes**

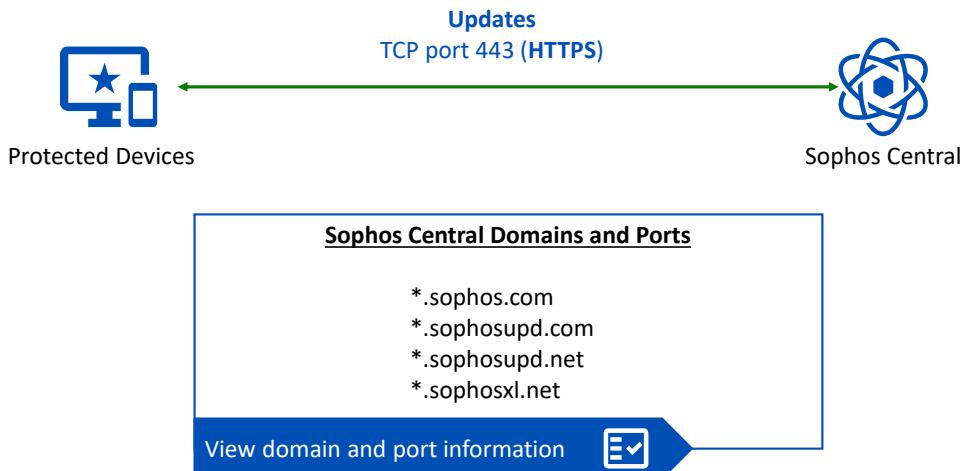
SOPHOS

In this chapter you will learn techniques that can be used to troubleshoot Central 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.

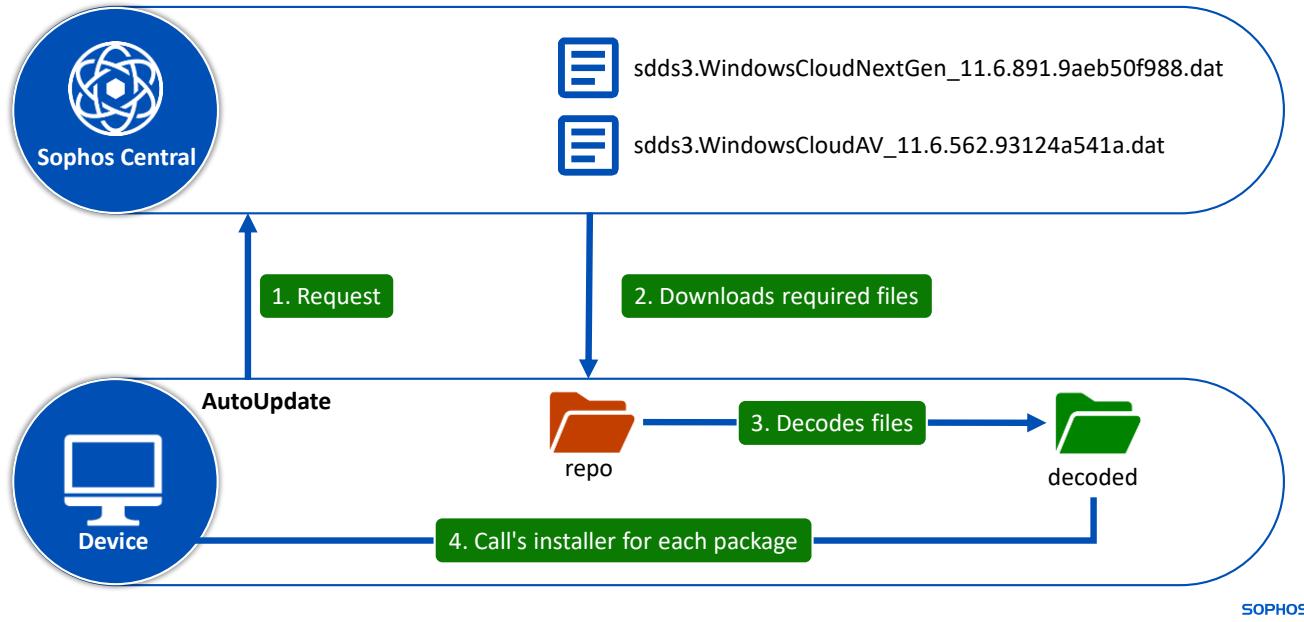
If you need to allow updating through a firewall or proxy, you need to ensure that the domains shown here are allowed. If your proxy or firewall doesn't support wildcards, you must identify the exact Sophos domains you need, then enter them manually.

## [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>

# Sophos Central Updating Overview



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**.

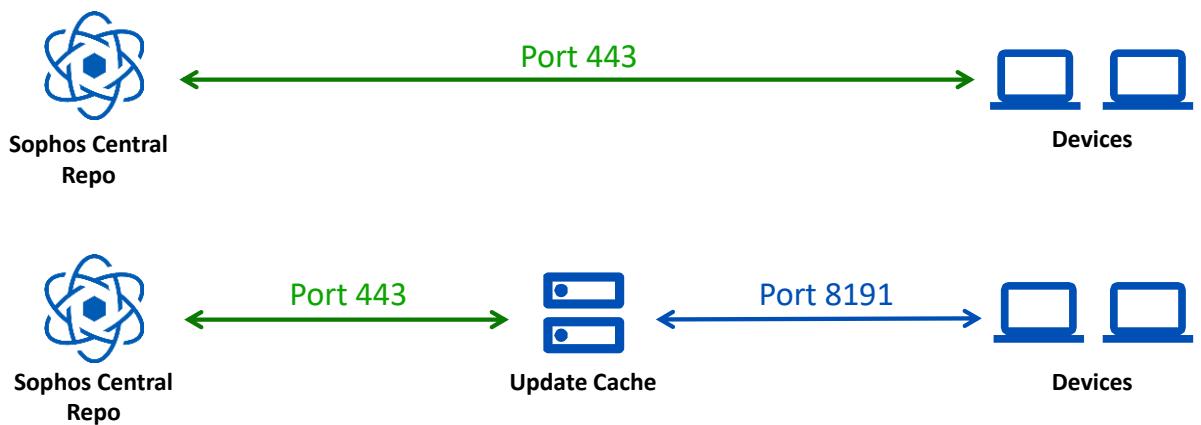
Once decoded, Sophos AutoUpdate calls the installer for each package to perform any required updates. If a component is added to a device in Sophos Central, for example Device Encryption, the devices subscription package is updated. When the device receives the new policy, Sophos AutoUpdate identifies 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`

# Sophos Central Updating Overview



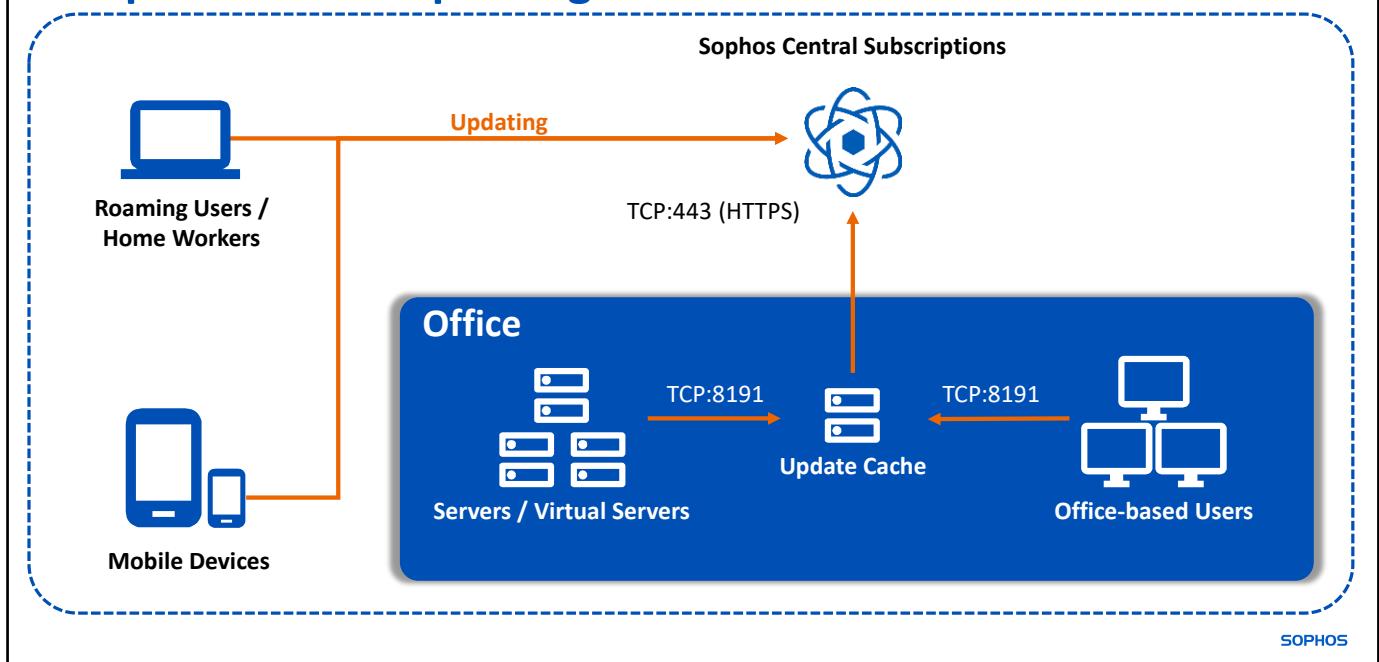
SOPHOS

Updating can be configured in two ways.

The first is for devices to communicate with, and update directly from Sophos Central.

The second is to use one or more Update Caches. This enables devices to receive updates from a cache on the network, as well as directly from Sophos. If any Update Cache is configured and a device can communicate with it, it will be used for updating. However, devices with no access to an Update Cache will still update directly from Central.

# Sophos Central Updating Overview



In this example, the Update Cache still needs to connect directly to Sophos Central. However, other devices only need to connect to the Update Cache on TCP port 8191.

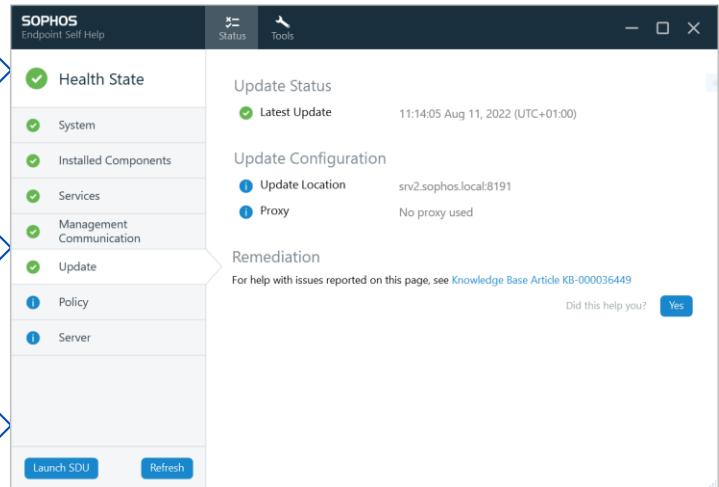
Roaming users, home workers and mobile devices with no access to the Update Cache will continue to update directly from Sophos Central. The port used for update communication is TCP port 443 for HTTPS traffic.

# Updating Overview

Sophos AutoUpdate is responsible for updating Sophos components

Sophos AutoUpdate monitors a distribution folder and updates components when there is a new version available

Sophos Central checks every hour for updates



SOPHOS

Sophos AutoUpdate is responsible for updating Sophos components installed on devices and the data used to provide threat protection.

It monitors a distribution folder and updates endpoint components whenever there are newer versions available.

Sophos Central checks every hour for updates. The first check is five minutes after the AutoUpdate service is started, then every sixty minutes after that for software, threat detection data and other available updates.

## Use Update Cache or Sophos

```
SophosUpdate - Notepad
File Edit Format View Help
2022-08-05T16:26:37.032Z [ 9072: 9068] I Trying update service url https://sus.sophosupd.com/v3/5550411b-07d2-48bd-9679-bc09a660403d/e5a5b028-adab-41bd-1^
2022-08-05T16:26:37.559Z [ 9072: 9068] I 200 from https://sus.sophosupd.com/v3/5550411b-07d2-48bd-9679-bc09a660403d/e5a5b028-adab-41bd-83e2-b8ffa205fc7^
2022-08-05T16:26:37.574Z [ 9072: 9068] I Sophos Update Service: received new configuration
2022-08-05T16:26:37.574Z [ 9072: 9068] I Syncing suites [sdds3.WindowsCloudAV_11.6.562.93124a541a.dat, sdds3.WindowsCloudClean_1.0.42.55133bcba5.dat, sd^
2022-08-05T16:26:37.574Z [ 9072: 9068] I Release groups [C]
2022-08-05T16:26:37.574Z [ 9072: 9068] I Analyzing whether to update from Sophos CDN or update cache
2022-08-05T16:26:37.612Z [ 9072: 9068] I Found no IP addresses for srv.sophos.local:8191. This update cache will be ignored.
2022-08-05T16:26:37.662Z [ 9072: 9068] I Found no IP addresses for srv2.sophos.local:8191. This update cache will be ignored.
2022-08-05T16:26:37.708Z [ 9072: 9068] I Found no IP addresses for winserver1.ad.trainingdemo.xyz:8191. This update cache will be ignored.
2022-08-05T16:26:37.708Z [ 9072: 9068] I Analysis complete - Using Sophos CDN
2022-08-05T16:26:37.708Z [ 9072: 9068] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy>
2022-08-05T16:26:37.838Z [ 9072: 9068] I 200 from https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat with proxy: <direct; no^
2022-08-05T16:26:37.838Z [ 9072: 9068] I Syncing from: https://sdds3.sophosupd.com
2022-08-05T16:26:38.558Z [ 9072: 9068] I Refreshing supplement sdds3.CIXFLAGS.dat
2022-08-05T16:26:38.608Z [ 9072: 9068] I GET https://sdds3.sophosupd.com/supplement/sdds3.CIXFLAGS.dat: 304 (not modified since 2022-08-01 10:55:44Z)
2022-08-05T16:26:38.651Z [ 9072: 9068] I Refreshing supplement sdds3.hmpa_data.dat
2022-08-05T16:26:38.784Z [ 9072: 9068] I GET https://sdds3.sophosupd.com/supplement/sdds3.hmpa_data.dat: 304 (not modified since 2022-08-04 12:40:46Z)
2022-08-05T16:26:38.740Z [ 9072: 9068] I Refreshing supplement sdds3.CEPNGFLAGS.dat
2022-08-05T16:26:38.791Z [ 9072: 9068] I GET https://sdds3.sophosupd.com/supplement/sdds3.CEPNGFLAGS.dat: 304 (not modified since 2022-07-31 15:59:50Z)
2022-08-05T16:26:38.822Z [ 9072: 9068] I Refreshing supplement sdds3.NTP_OVERRIDE.dat
2022-08-05T16:26:38.871Z [ 9072: 9068] I GET https://sdds3.sophosupd.com/supplement/sdds3.NTP_OVERRIDE.dat: 304 (not modified since 2022-07-31 16:51:42Z)
2022-08-05T16:26:38.914Z [ 9072: 9068] I Refreshing supplement sdds3.EPIPS_data.dat
Ln 41, Col 65 100% Windows (CRLF) UTF-8
```

SOPHOS

This example from the SophosUpdate log shows the endpoint analysing whether to update from Sophos or an update cache. No IP addresses are accessible for the configured Update Cache's, so Sophos is used.

# Update Management Policy

The screenshot shows the Sophos Central interface for managing update policies. On the left, a dark sidebar lists 'ANALYZE' (Dashboard, Logs & Reports), 'MANAGE PROTECTION' (People, Computers), 'CONFIGURE' (Policies, Settings, Protect Devices), and 'MORE PRODUCTS' (Free Trials). The 'Policies' option under 'CONFIGURE' is highlighted. The main content area is titled 'Endpoint Protection - View Computer Policy' and shows a policy named 'Controlled Updates' of type 'Update Management'. It indicates 0 computers and 0 groups assigned. A 'SETTINGS' tab is selected, showing a note that the policy is bypassed. Below this, the 'Scheduled Updates' section allows setting a specific time (02:00 PM) and day (Wednesday) for updates. The 'Update Cache' section notes it's for Sophos Update Cache users and provides an option to disable it. At the top right, there are 'Save', 'Cancel', 'Delete', and 'Clone' buttons, along with help and training links.

SOPHOS

Sophos Central allows for the configuration of Update Management policies which can be assigned to devices and device groups.

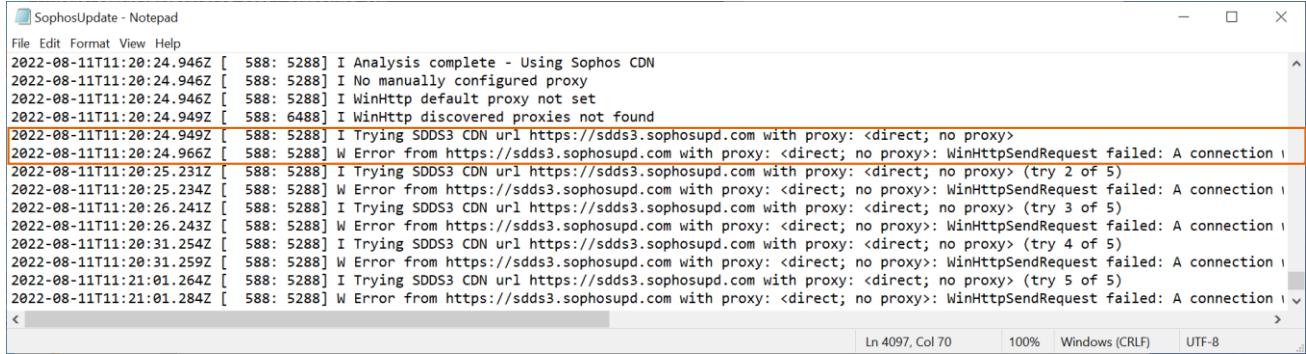
This policy can be used to schedule product updates that suit the organization. Any schedule configured will affect security updates that are used to protect devices against threats.

The policy allows you to disable an Update Cache to force devices to update directly from Sophos Central. Please note that if you select to do this, all devices will also stop using Message Relays if they have been configured.

# Sophos Update Log

AutoUpdate log location:

%ProgramData%\Sophos\AutoUpdate\Logs\

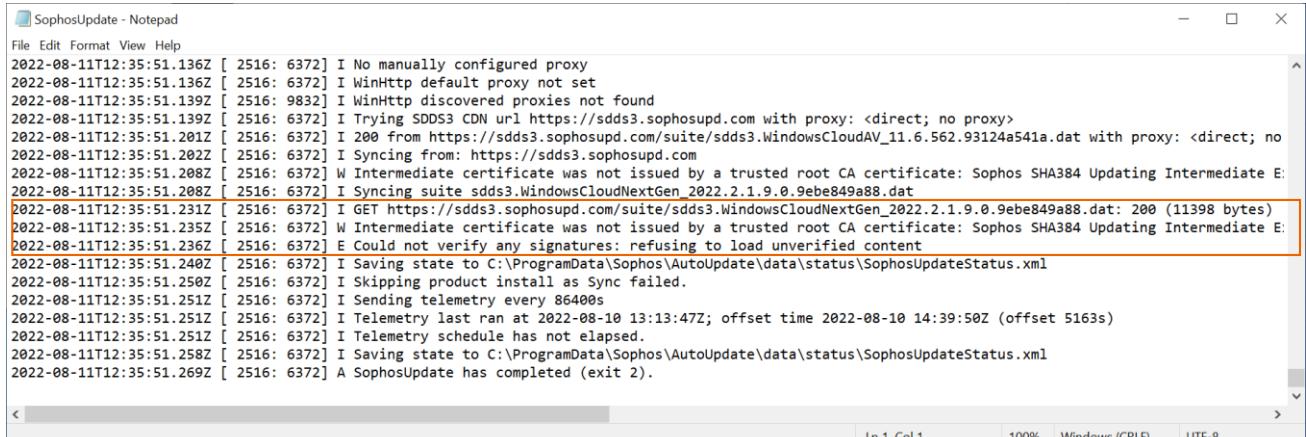


```
File Edit Format View Help
2022-08-11T11:20:24.946Z [ 588: 5288] I Analysis complete - Using Sophos CDN
2022-08-11T11:20:24.946Z [ 588: 5288] I No manually configured proxy
2022-08-11T11:20:24.946Z [ 588: 5288] I WinHttp default proxy not set
2022-08-11T11:20:24.949Z [ 588: 6488] I WinHttp discovered proxies not found
2022-08-11T11:20:24.949Z [ 588: 5288] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy>
2022-08-11T11:20:24.966Z [ 588: 5288] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>; WinHttpSendRequest failed: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because peer shut down abruptly.
2022-08-11T11:20:25.231Z [ 588: 5288] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy> (try 2 of 5)
2022-08-11T11:20:25.234Z [ 588: 5288] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>; WinHttpSendRequest failed: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because peer shut down abruptly.
2022-08-11T11:20:26.241Z [ 588: 5288] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy> (try 3 of 5)
2022-08-11T11:20:26.243Z [ 588: 5288] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>; WinHttpSendRequest failed: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because peer shut down abruptly.
2022-08-11T11:20:31.254Z [ 588: 5288] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy> (try 4 of 5)
2022-08-11T11:20:31.259Z [ 588: 5288] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>; WinHttpSendRequest failed: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because peer shut down abruptly.
2022-08-11T11:21:01.264Z [ 588: 5288] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy> (try 5 of 5)
2022-08-11T11:21:01.284Z [ 588: 5288] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>; WinHttpSendRequest failed: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because peer shut down abruptly.
```

SOPHOS

Additional information for troubleshooting can be found in the Sophos Update log. In this example, an error is logged when connecting to the URL for Sophos update.

# Troubleshooting a Failed Update – Sophos Update Log



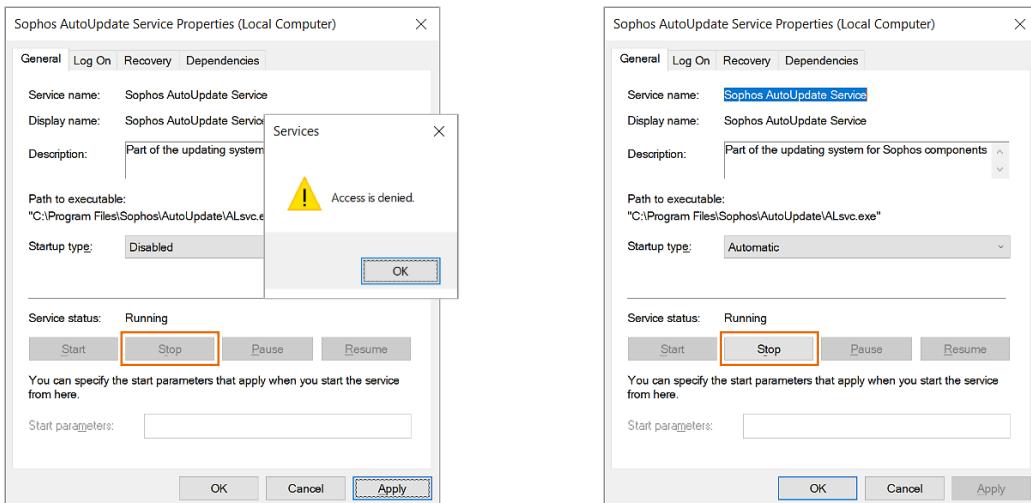
```
SophosUpdate - Notepad
File Edit Format View Help
2022-08-11T12:35:51.136Z [ 2516: 6372] I No manually configured proxy
2022-08-11T12:35:51.136Z [ 2516: 6372] I WinHttp default proxy not set
2022-08-11T12:35:51.139Z [ 2516: 9832] I WinHttp discovered proxies not found
2022-08-11T12:35:51.139Z [ 2516: 6372] I Trying SDDS3 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy>
2022-08-11T12:35:51.201Z [ 2516: 6372] I 200 from https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat with proxy: <direct; no proxy>
2022-08-11T12:35:51.202Z [ 2516: 6372] I Syncing from: https://sdds3.sophosupd.com
2022-08-11T12:35:51.208Z [ 2516: 6372] W Intermediate certificate was not issued by a trusted root CA certificate: Sophos SHA384 Updating Intermediate E
2022-08-11T12:35:51.208Z [ 2516: 6372] I Syncing suite sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat
2022-08-11T12:35:51.231Z [ 2516: 6372] I GET https://sdds3.sophosupd.com/suite/sdds3.WindowsCloudNextGen_2022.2.1.9.0.9ebe849a88.dat: 200 (11398 bytes)
2022-08-11T12:35:51.235Z [ 2516: 6372] W Intermediate certificate was not issued by a trusted root CA certificate: Sophos SHA384 Updating Intermediate E
2022-08-11T12:35:51.236Z [ 2516: 6372] E Could not verify any signatures: refusing to load unverified content
2022-08-11T12:35:51.240Z [ 2516: 6372] I Saving state to C:\ProgramData\Sophos\AutoUpdate\data\status\SophosUpdateStatus.xml
2022-08-11T12:35:51.250Z [ 2516: 6372] I Skipping product install as Sync failed.
2022-08-11T12:35:51.251Z [ 2516: 6372] I Sending telemetry every 86400s
2022-08-11T12:35:51.251Z [ 2516: 6372] I Telemetry last ran at 2022-08-10 13:13:47Z; offset time 2022-08-10 14:39:50Z (offset 5163s)
2022-08-11T12:35:51.251Z [ 2516: 6372] I Telemetry schedule has not elapsed.
2022-08-11T12:35:51.258Z [ 2516: 6372] I Saving state to C:\ProgramData\Sophos\AutoUpdate\data\status\SophosUpdateStatus.xml
2022-08-11T12:35:51.269Z [ 2516: 6372] A SophosUpdate has completed (exit 2).
```

SOPHOS

In this example, a certificate check failure is identified.

Enabling HTTPS traffic inspection and filtering may cause issues for Sophos update traffic because it can break the certificate trust between the protected device and the Sophos servers. We recommend disabling HTTPS inspection on the device update traffic.

# Troubleshooting a Failed Update - Services



SOPHOS

For some troubleshooting steps it may be necessary to temporarily stop the Sophos AutoUpdate service.

Open the services on a Windows device, then open the properties of the Sophos AutoUpdate Service. In the first example, tamper protection is still enabled and therefore the stop option is greyed out. An attempt to change the startup type to 'disabled' returns an access is denied error message.

Once tamper protection is disabled, it is possible to stop the service which allows for further troubleshooting.

# Troubleshooting a Failed Update – Clear Cache

The procedure to clear the local cache file and force and update is:

1. Stop the Sophos AutoUpdate Service
2. Rename the following folders:  
C:\ProgramData\Sophos\AutoUpdate\Cache\decoded  
C:\ProgramData\Sophos\AutoUpdate\data\repo
3. Delete the file SophosUpdateStatus.xml from C:\ProgramData\Sophos\AutoUpdate\data\status
4. Start the Sophos AutoUpdate Service
5. Open the Sophos Endpoint Agent
6. Click **About** followed by the **Update Now** button
7. Confirm that the update completes successfully

SOPHOS

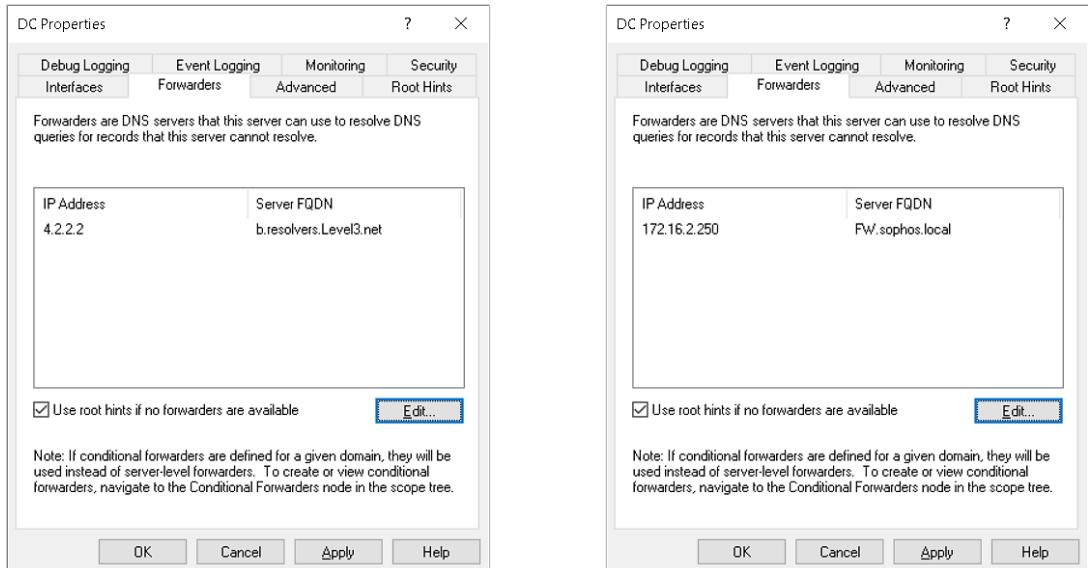
If no connectivity or service issues have been found, it may be necessary to clear the local update cache and force another update. To do this:

- Stop the Sophos AutoUpdate service
- Rename the **decoded** folder and the **repo** folder in the paths shown
- Delete the file SophosUpdateStatus.xml from the directory shown
- Start the Sophos AutoUpdate service
- Open the Sophos Endpoint Agent
- Click **About** and click **Update Now**

Confirm that the update completes successfully.

These steps will trigger a pending reboot alert in Sophos Central for the device once they have been completed.

# Domain Name Resolution



SOPHOS

The Active Directory Domain Controller acting as a DNS needs to provide resolution for external servers, such as the Sophos update locations.

DNS uses the concept of forwarding and the internal DNS is typically configured to point to a DNS located on the Internet. An example is shown here.

For greater security, it is possible to forward to another internal DNS which in turn forwards to an Internet DNS.



# Domain Name Resolution

C:\Windows\System32\drivers\etc

The screenshot shows a Windows Notepad window titled "hosts - Notepad". The file path is "C:\Windows\System32\drivers\etc". The content of the file is a sample HOSTS file. It contains several comments starting with "#", followed by two entries with IP addresses and host names, and then a localhost entry. A new line "172.16.1.200 srv.sophos.local" is added at the bottom, highlighted with an orange rectangle. The status bar at the bottom right shows "Ln 1, Col 1".

```
# Copyright (c) 1993-2009 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97      rhino.acme.com        # source server  
#      38.25.63.10        x.acme.com            # x client host  
#  
# localhost name resolution is handled within DNS itself.  
#      127.0.0.1          localhost  
#      ::1                localhost  
172.16.1.200    srv.sophos.local|
```

SOPHOS

DNS is the usual method for name resolution. However, a file named hosts can be manually configured. Entries in the hosts file are automatically loaded into the cache overriding those configured in DNS.

The hosts file requires administrative privileges to access and edit.

This example shows an entry with IP address 172.16.1.200 which resolves to the name srv.sophos.local. The lines above this entry that start with the hash sign are treated as comments.

## [Additional Information]

The file path for the hosts text file is C:\%systemroot%\System32\drivers\etc

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

**True or False:** By default, if the endpoint can find the IP address for a configured Update Cache it will use it for updating.

True

False

SOPHOS



## Question 2 of 2

What is the name of the file that can be edited to override name resolution provided by DNS?

\_\_\_\_\_

SOPHOS

# Chapter Review

By default, an **endpoint analyzes** whether **to update from Sophos or an update cache**. If no IP addresses are accessible for the configured update cache(s) Sophos is used

The **ping** command can be used to test **name resolution and connectivity**. **Telnet** can be used to test **connectivity to a specific TCP port**

For some troubleshooting steps it may be necessary to temporarily **stop the Sophos AutoUpdate service**. This requires **tamper protection** to be **disabled**

SOPHOS

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

By default, an endpoint analyzes whether to update from Sophos or an update cache. If no IP addresses are accessible for the configured update cache(s), Sophos is used.

The ping command can be used to test name resolution and connectivity. Telnet can be used to test connectivity to a specific TCP port.

For some troubleshooting steps it may be necessary to temporarily stop the Sophos AutoUpdate service. This requires tamper protection to be disabled.



# Considerations for Using Sophos Central Update Caches and Message Relays

Sophos Central Endpoint and Server Protection

Version: 4.0v1

**SOPHOS**

## [Additional Information]

Sophos Central Endpoint and Server Protection

CE2035: Considerations for Using Sophos Central 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.

# Considerations for Using Sophos Central Update Caches and Message Relays

In this chapter you will learn when to use Update Caches and Message Relays along with some of the main issues to consider when deploying them.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How Sophos Central communicates with protected devices
- ✓ How protected devices are updated
- ✓ The function of an Update Cache
- ✓ The function of a Message Relay

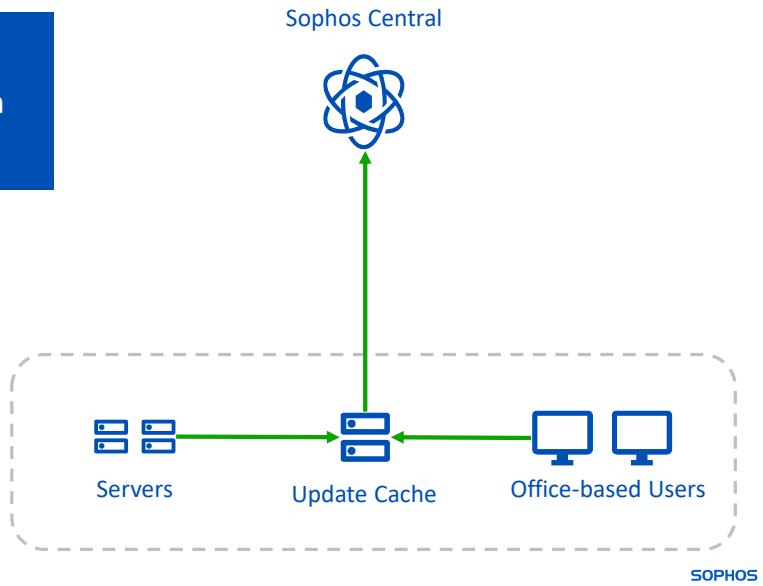
DURATION     **8 minutes**

SOPHOS

In this chapter you will learn when to use Update Caches and Message Relays along with some of the main issues to consider when deploying them.

# Update Cache Deployment Scenarios

Sites with low or limited bandwidth



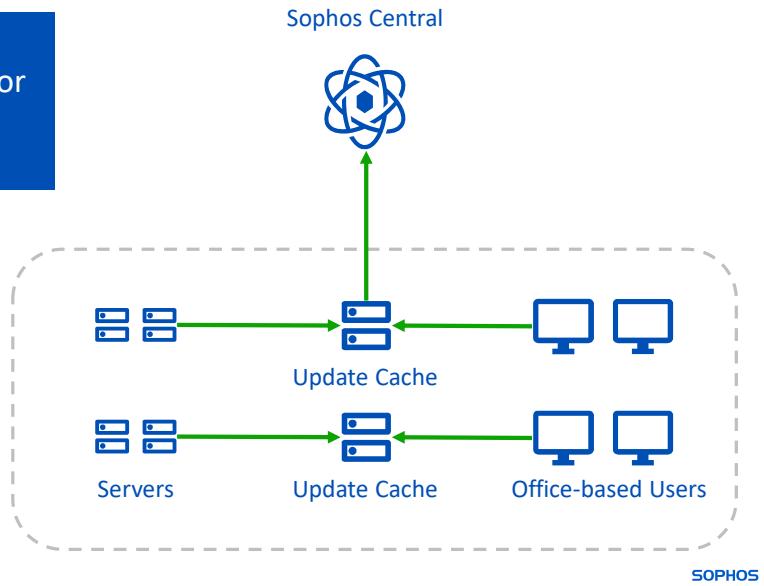
Probably the most obvious candidate for an Update Cache, are those sites that have very low or limited bandwidth.

In this scenario, Update Caches can make a big difference as devices only need to communicate with the device the Update Cache is deployed on.

Please note that in this scenario, the Update Cache must complete the initial installation and download directly from Sophos.

# Update Cache Deployment Scenarios

At larger sites, use 2 update caches for redundancy



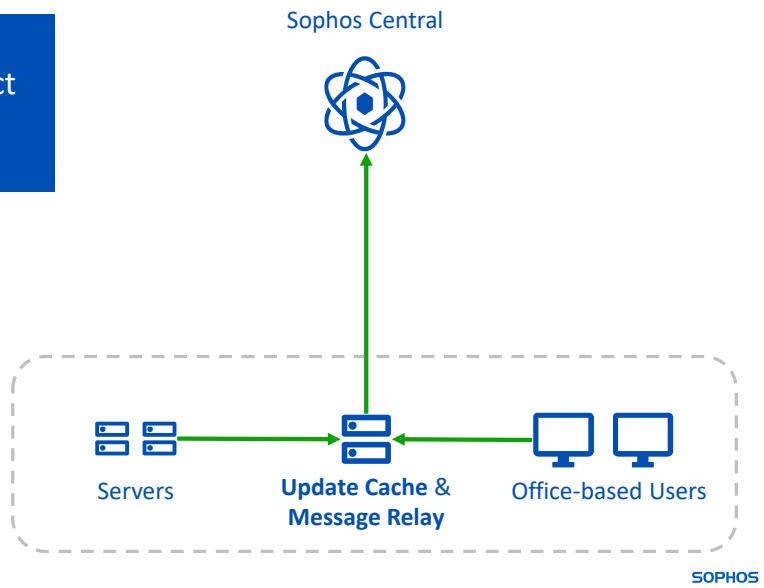
On larger sites you can deploy two Update Caches for redundancy.

As protected devices attempt to update directly from Sophos if an Update Cache is unreachable, you can deploy another Update Cache that devices will attempt to update from first, before updating directly from Sophos.

It is not required to have multiple Update Caches, however, these can be useful in scenarios where devices do not have direct Internet access.

# Update Cache and Message Relay Deployment Scenarios

Networks with restricted or no direct Internet access

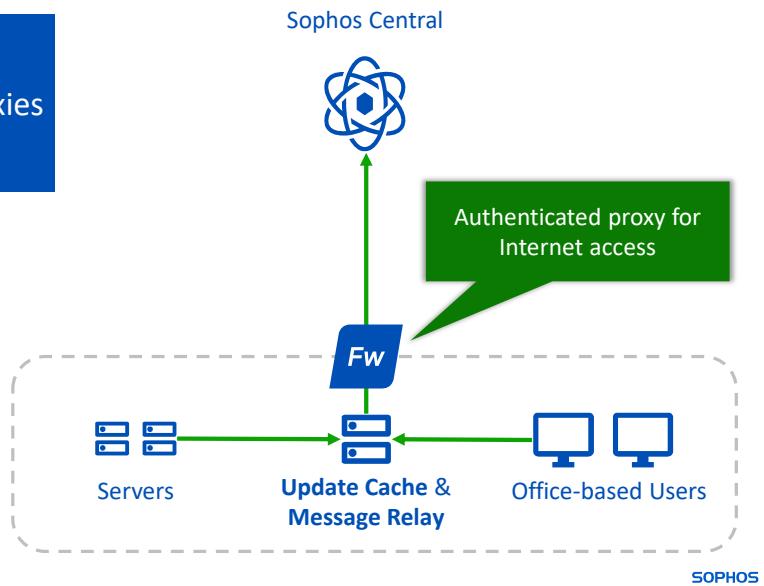


Some sites contain networks that have either restricted Internet access or no direct Internet access. In these scenarios you can choose to deploy an Update Cache and a Message Relay that can connect to Sophos. Protected devices on the restricted network connect to the Update Cache and Message Relay for updates and management.

You will need to deploy the Update Cache and Message Relay before the devices on the restricted network are protected. You can specify a Message Relay in the installer, which will be used to get a list of available Update Caches and to register with Sophos Central.

# Update Cache and Message Relay Deployment Scenarios

Multiple sites with authenticated proxies



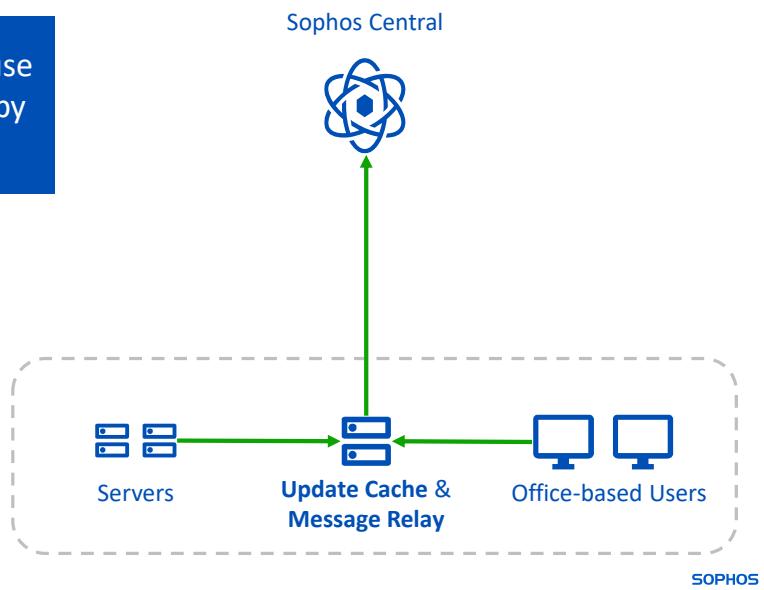
Sophos Central does not provide a mechanism to configure separate proxies for multiple sites. You can configure a proxy for devices to use when connecting to Sophos directly by navigating to **Global Settings > General > Proxy Configuration** in Sophos Central.

If you can exclude the traffic to Sophos on the proxy for all devices, then you do not need to deploy an Update Cache or a Message Relay, however, if this cannot be done, or is not allowed, an Update Cache and Message Relay can be used. The Update Cache and Message Relay server will still need to access Sophos directly.

In this scenario, one option may be to deploy the Update Cache and Message Relay in a DMZ, if the site has one.

# Update Cache and Message Relay Deployment Scenarios

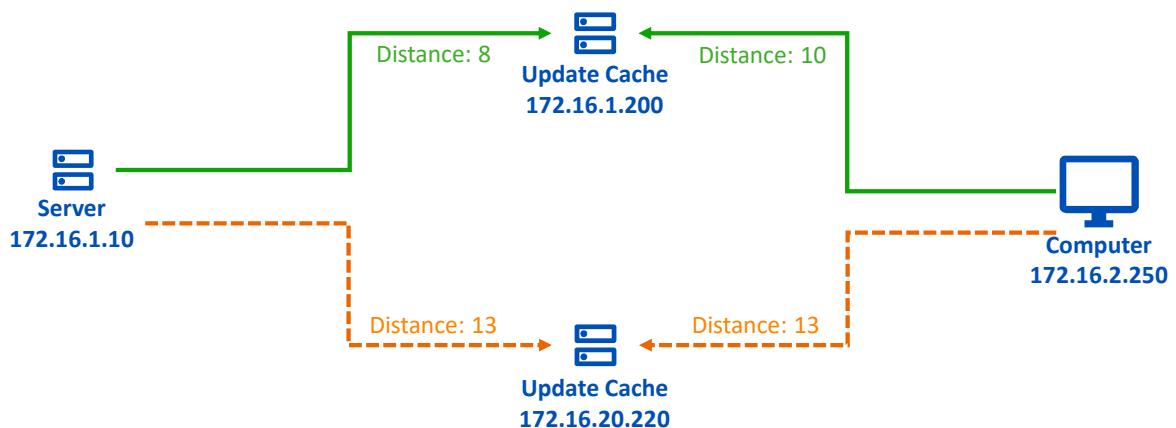
Once enabled, all devices will try to use Update Caches and Message Relays by default



Once an Update Cache and Message Relay have been deployed, all protected devices automatically default to using the Update Cache and Message Relay. If they cannot reach the dedicated server, they will fall back to updating and communicating directly from Sophos.

It is possible to exclude devices from using Update Caches and Message Relays. This becomes particularly important if you have multiple sites, as deploying a Message Relay on a single site may lead to all MCS traffic being relayed through a single Message Relay.

## How An Update Cache Is Selected



SOPHOS

Protected devices prioritize Update Caches based on how numerically close they are. It is important to consider the IP addresses of any Update Caches and devices to prevent unexpected behaviour.

# How An Update Cache Is Selected

1

The numerically nearest Update Cache is used



2

If it cannot be reached, the next nearest is used



3

If none can be reached, Sophos is used



If more than one Update Cache has been deployed, a device will first try to update from the closest Update Cache.

If the nearest Update Cache is unreachable, the next nearest Update Cache will be used.

If no Update Cache can be reached, the device will try to update from Sophos Central directly.



Additional information in  
the notes

## How An Update Cache Is Selected

Server <b>172.16.1.10</b>	10101100	00010000	00000001	00001010
Update Cache <b>172.16.1.200</b>	10101100	00010000	00000001	<b>11001000</b>
Update Cache <b>172.16.20.220</b>	10101100	00010000	<b>00010100</b>	<b>11011100</b>
				Distance: 8
				Distance: 13
Computer <b>172.16.2.250</b>	10101100	00010000	00000010	11111010
Update Cache <b>172.16.1.200</b>	10101100	00010000	<b>00000001</b>	<b>11001000</b>
Update Cache <b>172.16.20.220</b>	10101100	00010000	<b>00010100</b>	<b>11011100</b>
				Distance: 10
				Distance: 13

SOPHOS

So how is the distance calculated?

The device starts by converting its IP address, and the IP addresses of the Update Caches to bits. Ignore the bits of the Update Cache address that match the device address, then count the bits from the first one that differs. In this example the distance of the Update Cache with the IP address 172.16.1.200 is 8. The distance of the Update Cache with the IP address 172.16.20.220 is 13.

So, the server will try to use the Update Cache with the IP address 172.16.1.200 because it has the lowest distance. We can do the same for the computer, and we can see that it will use the same Update Cache as the server, although the distance is greater.

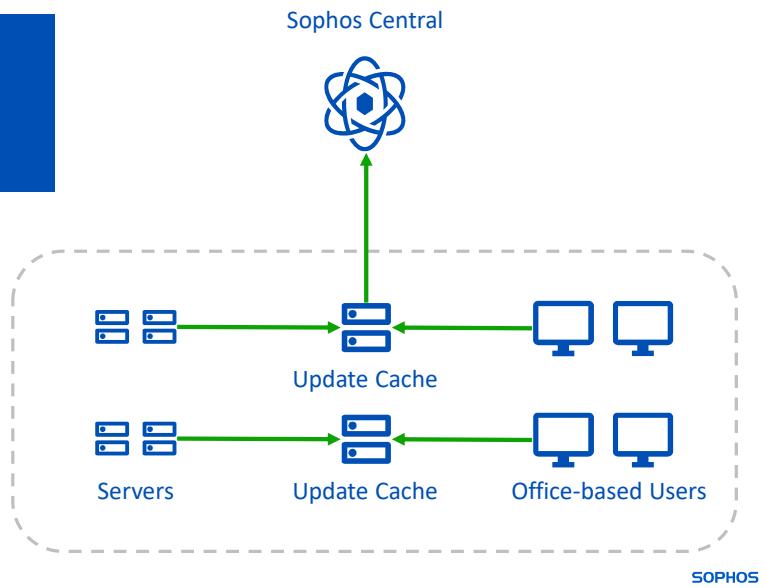
### [Additional Information]

If the calculated distance between multiple update caches is the same, it uses the first update cache in the ordered list obtained from the registry key:

HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Sophos\AutoUpdate\Service\UpdateCache

## Check Distance to the Update Cache

Check the distance calculations for Update Cache IP addresses

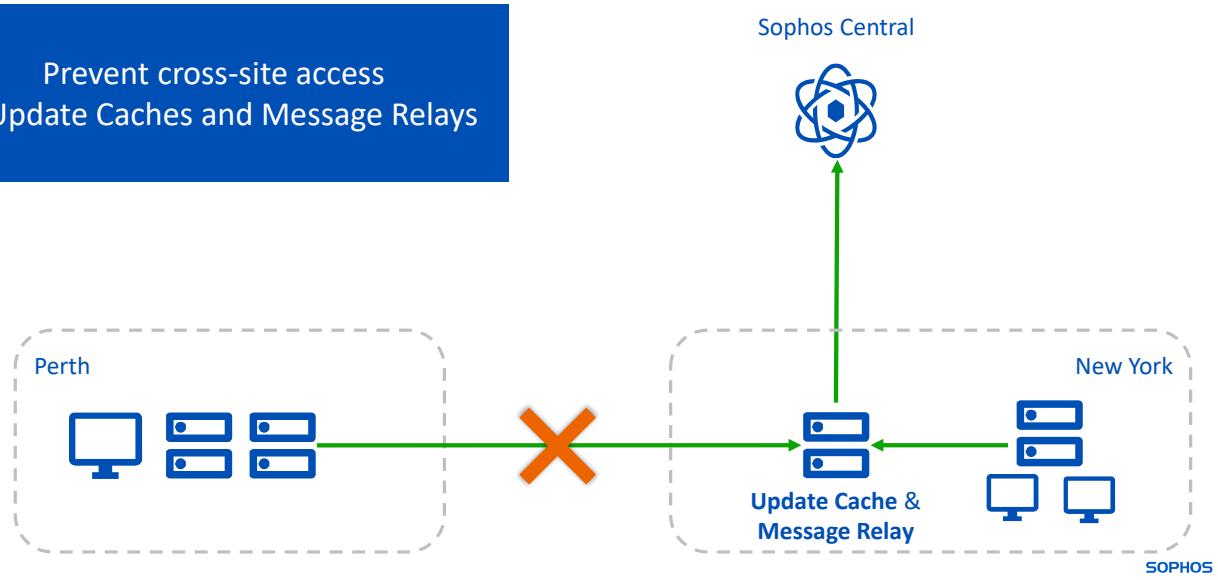


You should not leave the Update Cache behaviour to chance. When deploying Update Caches, you should check the distance to the Update Cache IP address from the devices you want it to serve.

You can manually assign devices to an Update Cache, however, this feature should primarily be used for any outlying devices.

# Considerations for Deployment

Prevent cross-site access  
to Update Caches and Message Relays



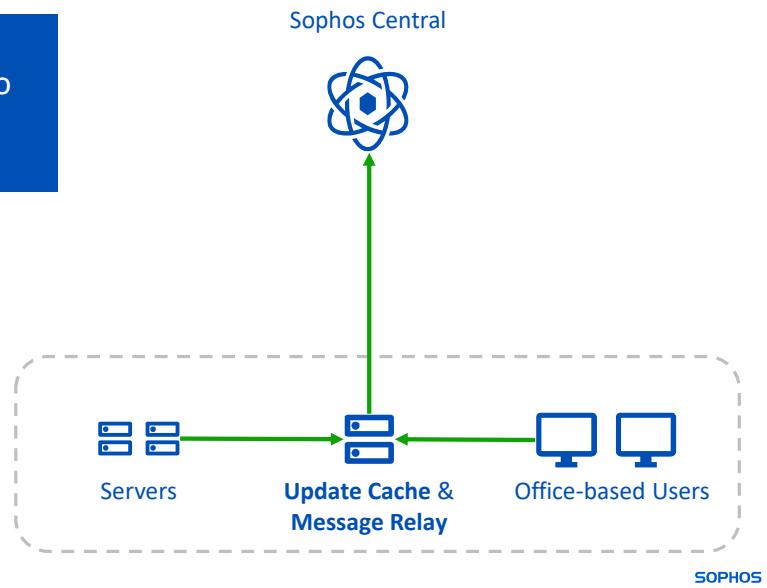
One potential unexpected result could be that devices update from an Update Cache on another site or if a Message Relay has been deployed, MCS traffic is routed through another site.

This could happen either if one site does not have an Update Cache, or because the IP address of the Update Cache on the remote site is numerically closer than on the local site. MCS traffic does not use a significant amount of bandwidth, however, it does not make sense to route MCS traffic via another site. Additionally, it is best practice to ensure that very low bandwidth sites are not used to relay traffic.

We recommend ensuring that this cannot happen by blocking cross-site traffic on TCP port 8191 and TCP port 8190 whenever Update Caches and Message Relays are being deployed.

# Considerations for Deployment

Prevent MCS traffic being subject to decryption and scanning



For devices to directly communicate with Sophos for management it is important that MCS traffic is not decrypted and scanned by firewalls.

You can choose to either exclude Sophos traffic from HTTPS scanning for all devices, or if this is undesirable, deploy a Message Relay and exclude Sophos traffic from HTTPS scanning. When excluding traffic from being decrypted and scanned, we recommend using DNS names as the IP addresses may change.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

Which of the following statements is true regarding devices that are in a different site from an Update Cache?

Devices only use a cache in their local site

The numerical distance must be less than 20 to be used

Update Caches must be manually assigned

Cross-site traffic on TCP port 8191 should be blocked

SOPHOS



## Question 2 of 2

**True or False:** Following the deployment of an Update Cache and a Message Relay devices must be assigned to use it.

True

False

SOPHOS

# Chapter Review

Once an **Update Cache and Message Relay** have been **deployed**, protected devices **automatically start using it**.

A device will first try to update from the **closest Update Cache**. If the nearest Update Cache is unreachable, the **next nearest Update Cache** will be used. If no Update Cache can be reached, the device will update from **Sophos Central** directly.

**Do not leave Update Cache and Message Relay behavior to chance.** When deploying, you should **check the distance** to the IP address from the devices you want it to serve.

SOPHOS

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

Once an Update Cache and Message Relay have been deployed, protected devices automatically start using it.

A device will first try to update from the closest Update Cache. If the nearest Update Cache is unreachable, the next nearest Update Cache will be used. If no Update Cache can be reached, the device will update from Sophos Central directly.

Do not leave Update Cache and Message Relay behavior to chance. When deploying, check the distance to the IP address from the devices you want it to serve.



# Advanced 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

CE2040: Advanced 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.

# Advanced Sophos Central Update Cache and Message Relay Deployment

In this chapter you will learn how to deploy the Sophos Central Endpoint Agent with Update Caches and Message Relays.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

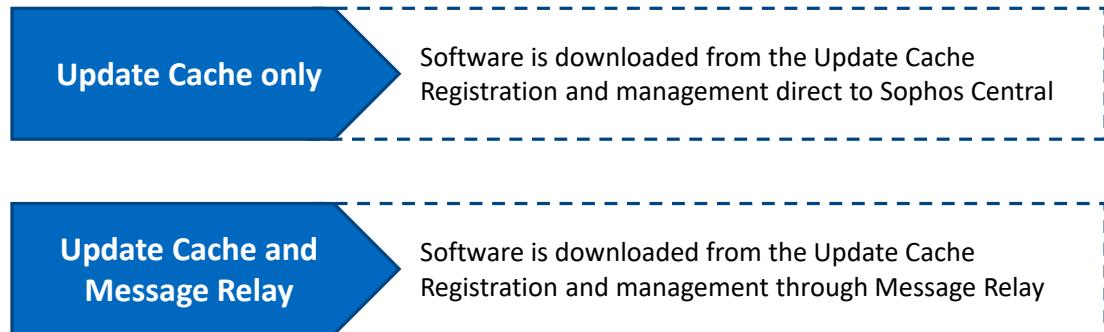
- ✓ How to deploy an Update Cache and Message Relay
- ✓ How to deploy the Sophos Endpoint Agent to devices
- ✓ How an Update Cache is selected

DURATION     **6 minutes**

SOPHOS

In this chapter you will learn how to deploy the Sophos Central Endpoint Agent with Update Caches and Message Relays.

# Install with Update Caches and Message Relays



SOPHOS

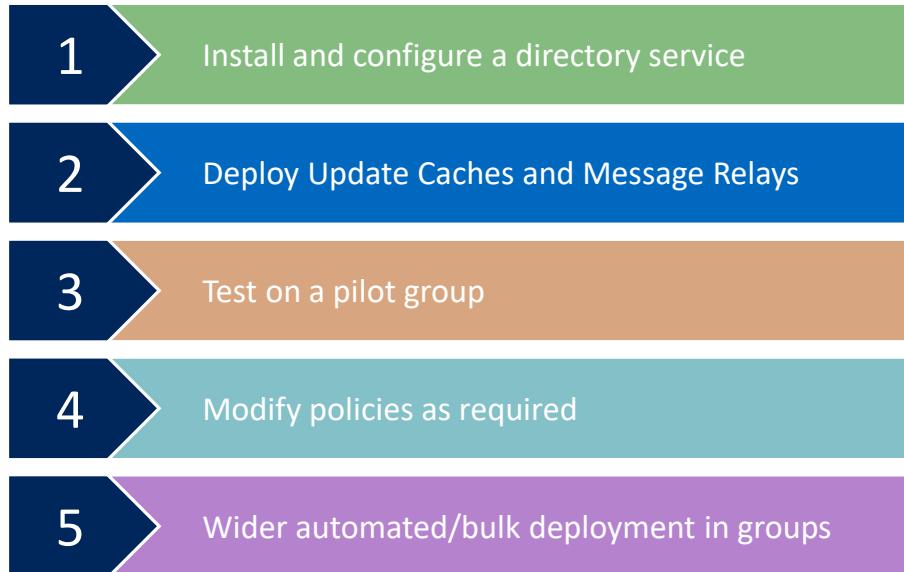
When you install the Sophos Endpoint Agent with Update Caches and Message Relays available it changes the behavior of the installer.

If there are only Update Caches available and no Message Relays, the installer will still connect directly to Sophos Central for registration and management, but all software can be downloaded from the Update Cache.

Where there are both Update Caches and Message Relays available, the registration and management traffic can be proxied through the Message Relay, and all software can be downloaded from the Update Cache.

Remember, it is not possible to have a Message Relay without an Update Cache.

# Deployment Strategy



SOPHOS

This means that to make the best use of Update Caches in low bandwidth environments, and to provide management connectivity where there is no direct Internet access, ensure that you have deployed the Update Caches and Message Relays before you start deploying the Sophos Endpoint Agent.

Here we have added Update Caches and Message Relays into our recommended deployment strategy. As part of this, remember to block cross-site access to Update Caches and Message Relays on TCP ports 8190 and 8191 to prevent undesired behaviour. You will need to manually install Sophos Protection onto devices where you will be deploying the Update Caches and Message Relays.

# Where to find Update Caches and Message Relays

Installer option...

Windows & MacOS

Windows

```
SophosSetup.exe --messagerelay=192.168.10.100:8190
```

MacOS

```
sudo ./Sophos\ Installer.app/Contents/MacOS/Sophos\ Installer --messagerelay 192.168.10.100:8190
```

SOPHOS

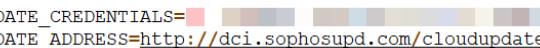
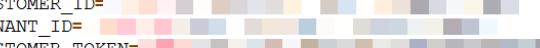
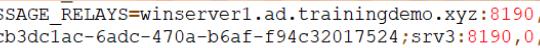
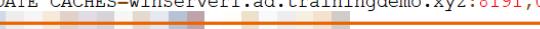
So, when installing, how does the installer know where the Update Caches and Message Relays are?

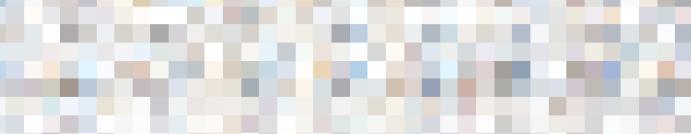
There are a few different ways. For Windows and macOS installations you can supply the address of a Message Relay as an installer option. As Message Relays are always Update Caches too, this server can act as an Update Cache.

# Where to find Update Caches and Message Relays

Included in the installer...

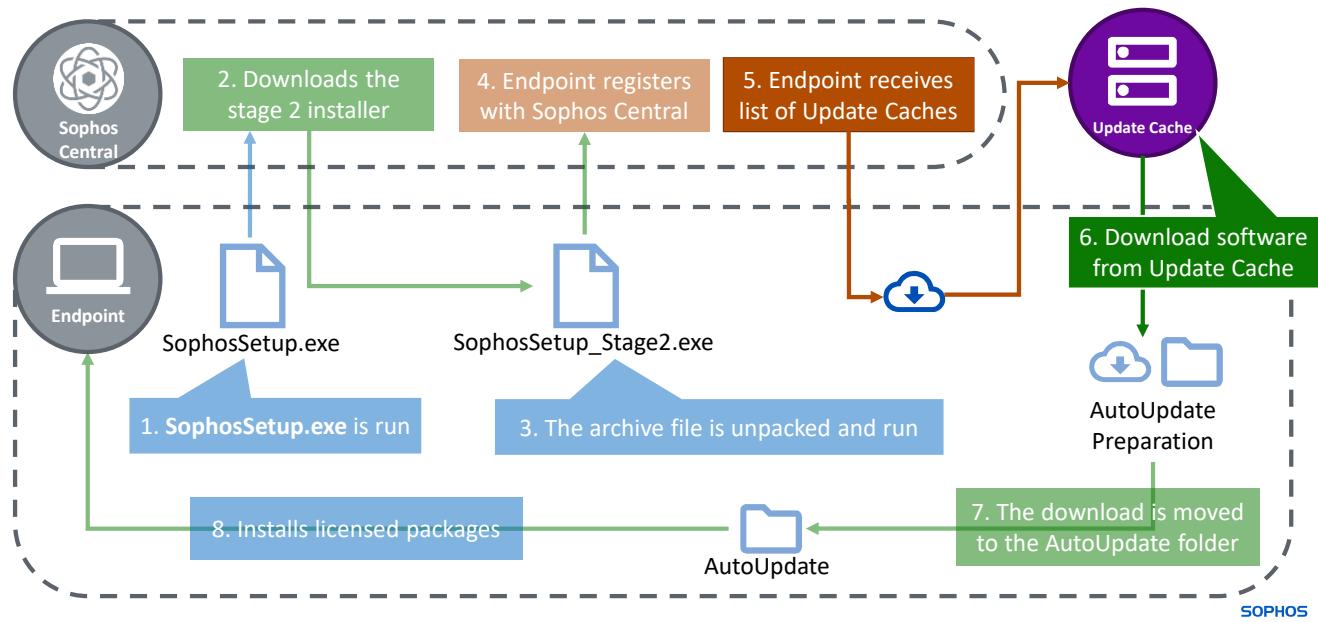
MacOS & Linux

```
643
644
645 TOKEN=
646 URL=https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep
647 PRODUCTS=all
648 UPDATE_CREDENTIALS=
649 UPDATE_ADDRESS=http://dci.sophosupd.com/cloudupdate
650 CUSTOMER_ID=
651 TENANT_ID=
652 CUSTOMER_TOKEN=
653 MESSAGE_RELAYS=winserver1.ad.trainingdemo.xyz:8190,0, ;srv.sophos.local:8190,  
0,cb3dclac-6adc-470a-b6af-f94c32017524;srv3:8190,0,
654 UPDATE_CACHES=winserver1.ad.trainingdemo.xyz:8191,0, ;srv3:8191,0,66  
  

655 __UPDATE_CACHE_CERTS__
656 -----BEGIN CERTIFICATE-----
657 MIIDXDCCAggAwIBAgIQJg8tyk0VJTK9MFcnZv0DJTANBgkqhkiG9w0BAQsFADbh
658
659
660
661
662
663
664
```

The macOS and Linux installers contain a list of Message Relays that have been deployed at the time the installer is downloaded. For this reason, it is important to ensure that you always download a current copy of the installer.

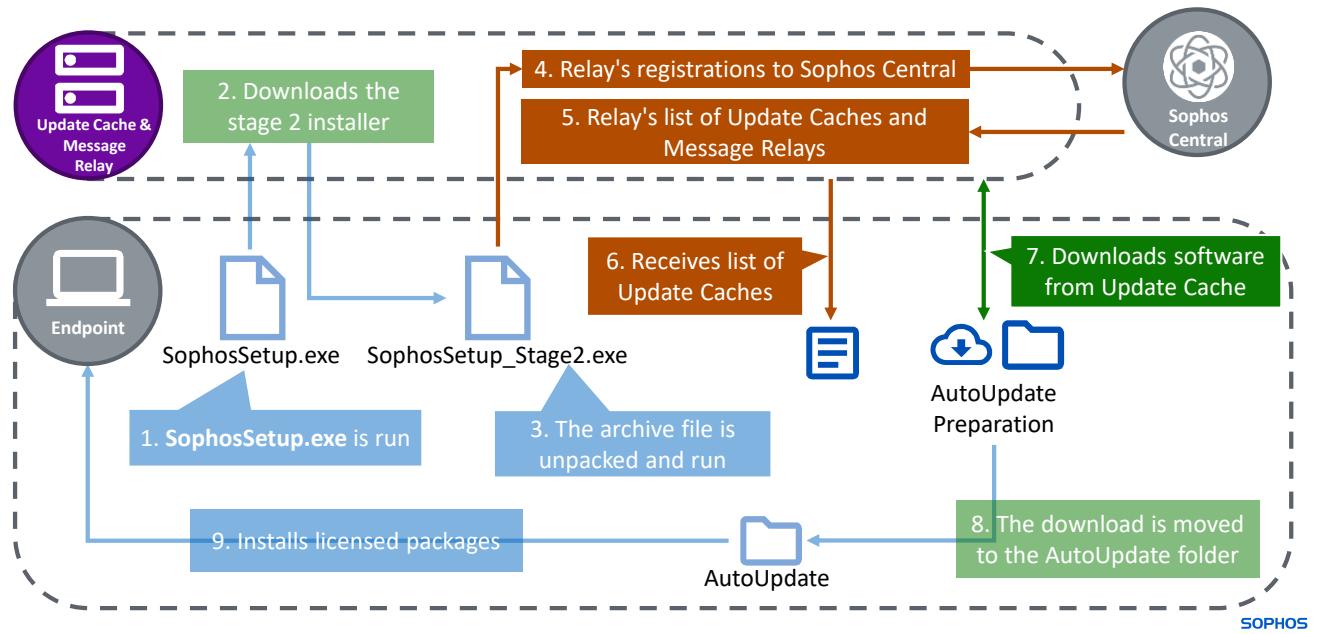
# Where to find Update Caches and Message Relays



The Windows installation process also allows for the installer to retrieve a list of Update Caches once the stage 2 installer has registered with Sophos Central.

The installer will order the Update Caches by numerical distance and then download the software from the closest before starting the installation.

# Where to find Update Caches and Message Relays



When requiring a Message Relay to install, you have to pass the details to the installer when it is run.

The installer registers with Sophos Central through the Message Relay and receives the list of Update Caches. The installer then downloads the software from the Update Cache and installs it.

# Activity



You will be presented with a few scenarios. Consider these questions for each scenario.

- **Where** would you deploy an Update Cache and a Message Relay?
- **Why** would you deploy an Update Cache and a Message Relay?

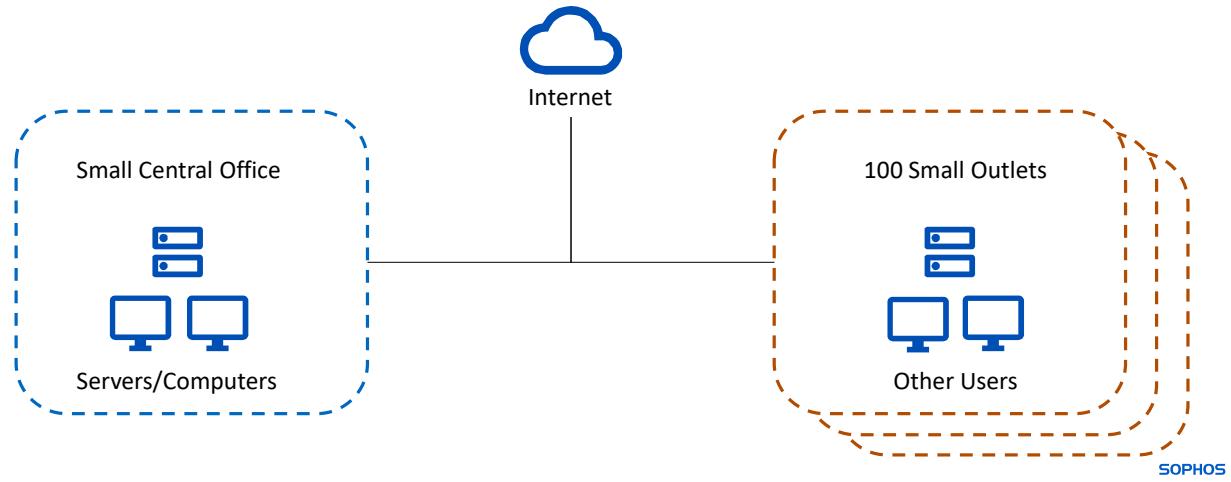
SOPHOS

You will be presented with a few scenarios. Consider these questions for each scenario.

Where would you deploy an Update Cache and a Message Relay and why?

## Deployment Scenario One

A retail company with **multiple small outlets** each with **3-8 computers**, and a small central office with **1 server** and **3 computers**.

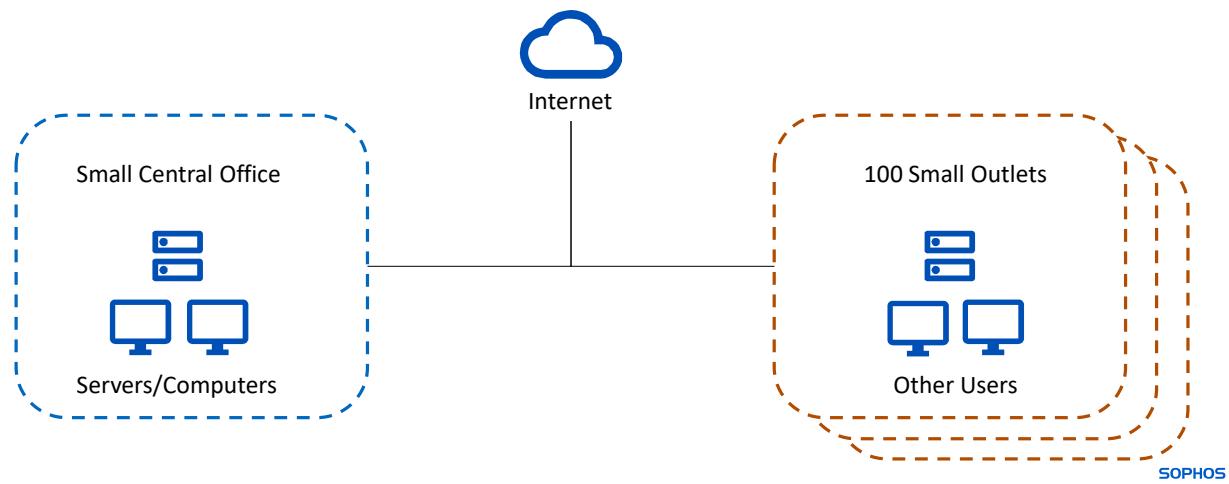


A retail company with multiple small outlets each with 3 to 8 computers, and a small central office with 1 server, and 3 computers.

What type of deployment would you recommend?

## Deployment Scenario One

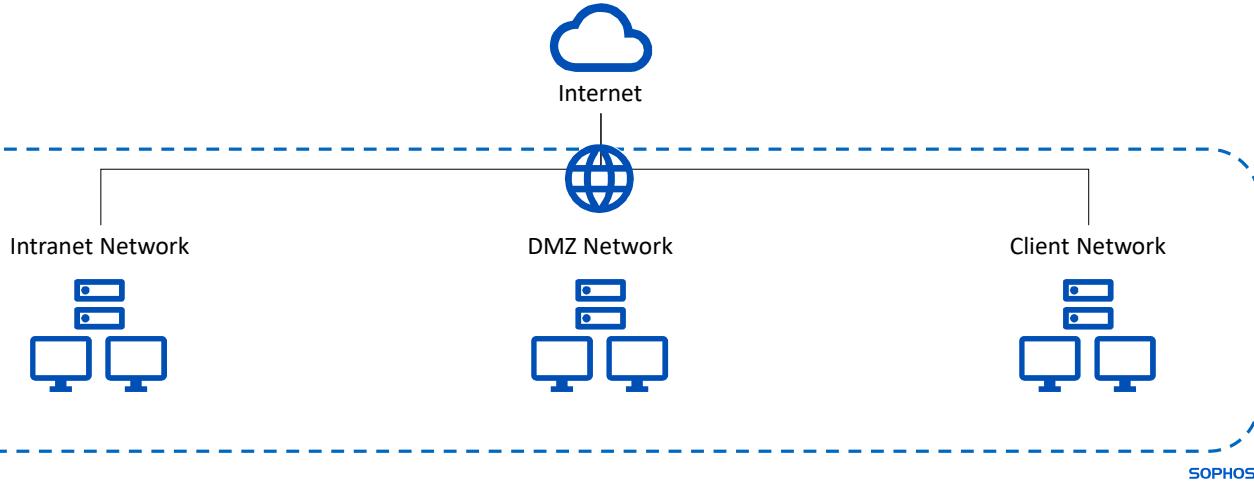
As the central office is very small and the outlets are unlikely to have a cache capable device, an **Update Cache** is **not a good fit**. There is no mention of bandwidth limitations.



As the central office is very small and the outlets are unlikely to have a cache capable device, an Update Cache is not a good fit here. There is no mention of bandwidth limitations.

## Deployment Scenario Two

A mid-sized company with **multiple networks**. The **intranet network** has no direct Internet access. The **client network** accesses the **Internet** through an authenticated proxy.

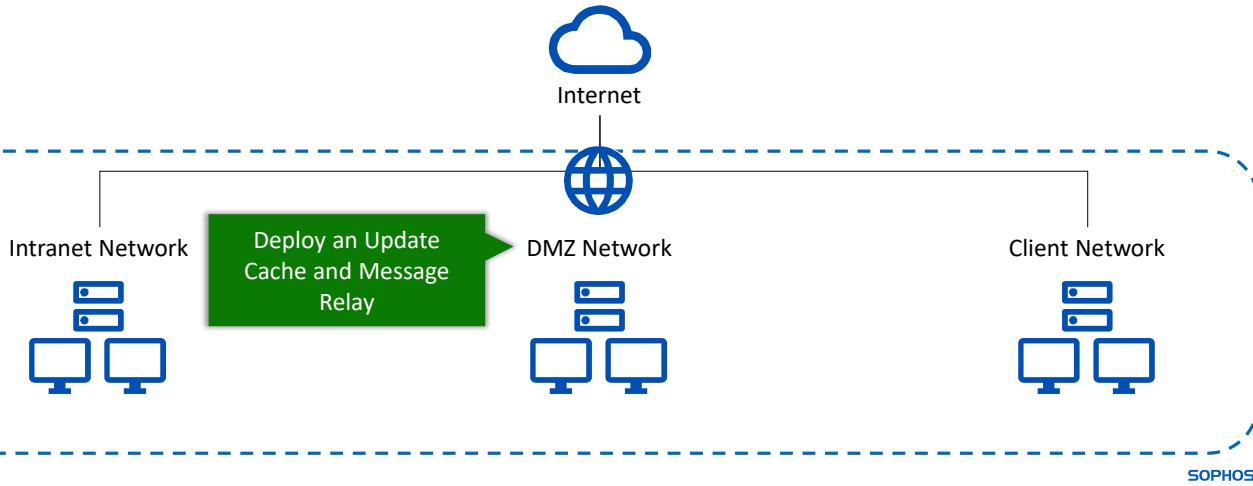


A mid-sized company with multiple networks. The intranet network has no direct Internet access. The client network accesses the Internet through an authenticated proxy.

What deployment would you recommend?

## Deployment Scenario Two

Deploy an **Update Cache and a Message Relay** in the **DMZ network**. The intranet network has no direct Internet access and there are no cache capable servers on the client network

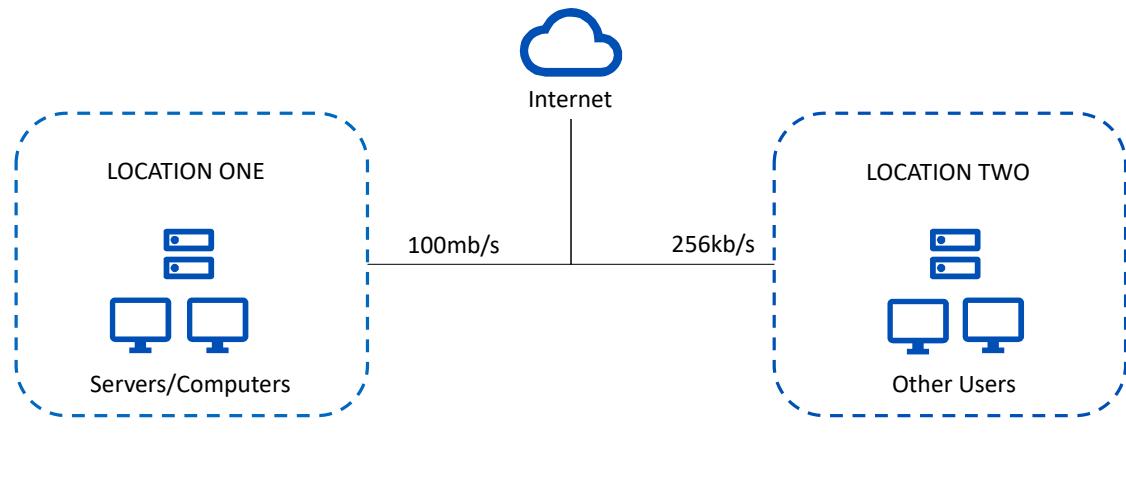


As the Intranet network has no direct Internet access and there are no cache capable servers on the client network you would deploy an Update Cache and a Message Relay in a DMZ network.

The Update Cache and Message Relay should only receive requests from the Intranet servers. The clients will then receive messages and updates directly from Sophos in the first instance.

## Deployment Scenario Three

A retail company with **two** locations, **1** with a **100 mb/s** Internet connection, the other with a **256 kb/s** connection.



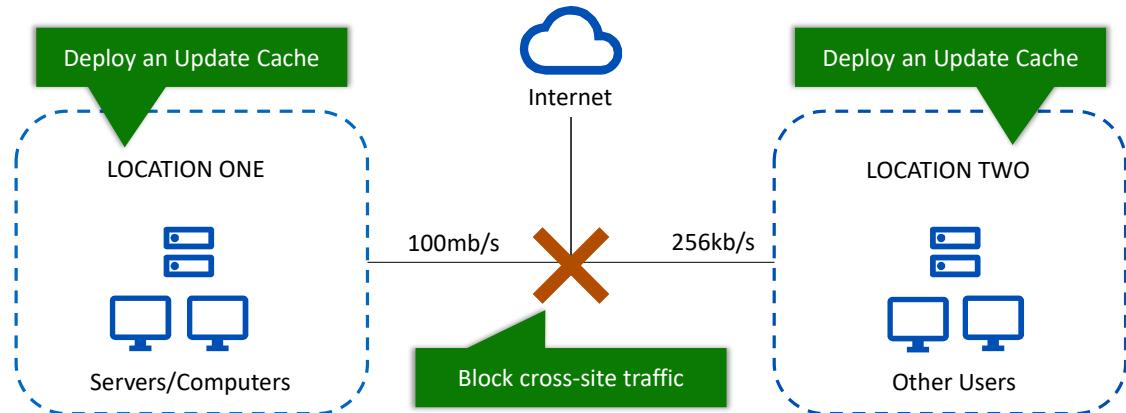
SOPHOS

A company with 2 locations, 1 with a 100 mb/s Internet connection, the other one has a 256 kb/s connection.

What type of deployment would you recommend?

## Deployment Scenario Three

Deploy an Update Cache on both sites and block cross-site traffic

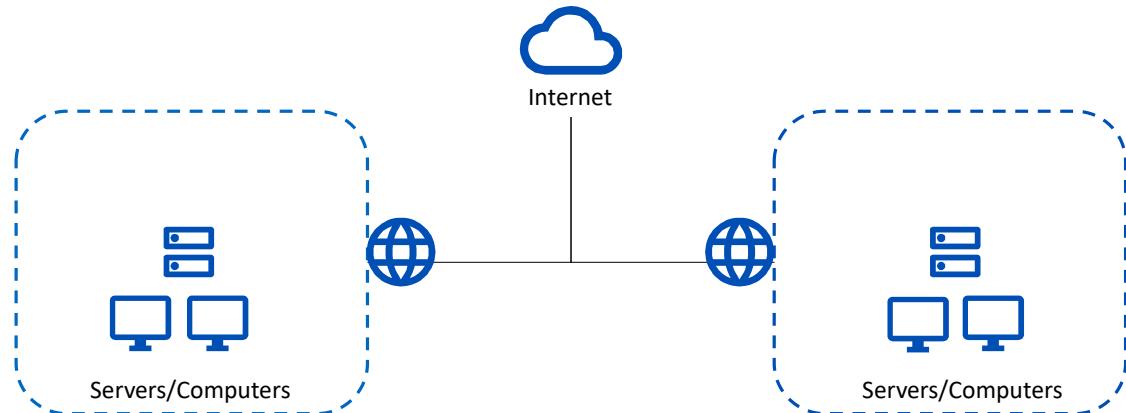


SOPHOS

Deploy an Update Cache on both sites and block cross-site traffic.

## Deployment Scenario Four

A company with **multiple locations**. Each location has an **authenticated proxy** for Internet access



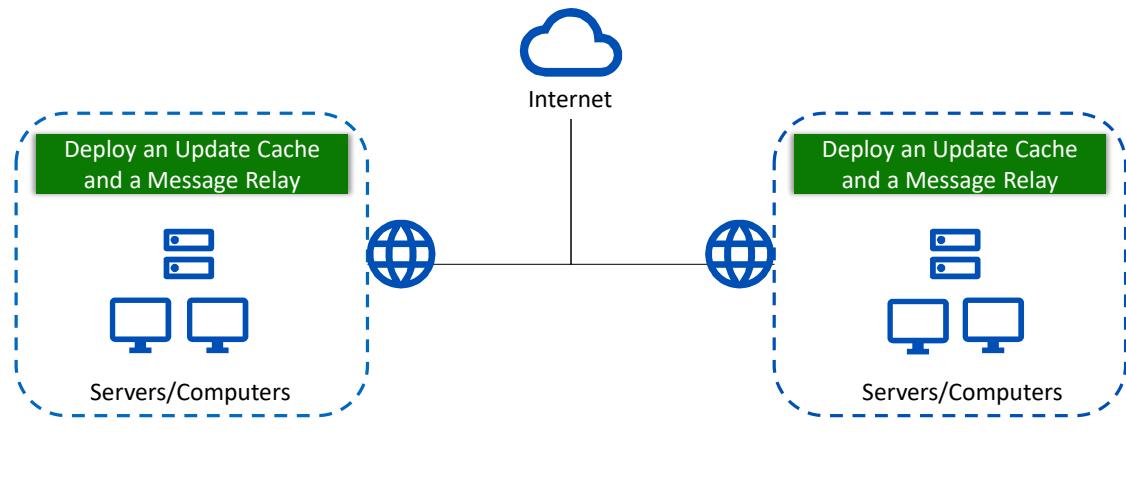
SOPHOS

A company with multiple locations. Each location has an authenticated proxy for Internet access.

What deployment would you recommend?

## Deployment Scenario Four

Deploy an Update and a Message Relay on each site. Both must be allowed access to Sophos. Alternatively, allow access to Sophos for all devices



Deploy an Update Cache and Message Relay on each site. Both must be allowed access to Sophos. Alternatively, allow access to Sophos for all devices.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

**True or False:** You can pass a list of Update Caches to the Windows installer with an option.

True

False

SOPHOS



## Question 2 of 2

Which installers include a list of deployed Message Relays when they are downloaded?

Windows

MacOS

Linux

SOPHOS

# Chapter Review

You should deploy Update Caches and Message Relays **before** starting to install the endpoint agent to take advantage of **bandwidth efficiency**, and to proxy **registration** and **management** traffic for devices without direct Internet access.

You can **pass a list of Message Relays** to the Windows and macOS installers. The **macOS and Linux installers include** a list of Message Relays at the time the installer was downloaded. The **Windows installer retrieves a list of Update Caches from Sophos Central** as part of the installation.

Update Caches and Message Relays are **not always required** and are not always a good fit in every environment or at every site.

SOPHOS

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

You should deploy update caches and message relays before starting to install the endpoint agent to take advantage of bandwidth efficiency, and to proxy registration and management traffic for devices without direct Internet access.

You can pass a list of Message Relays to the Windows and macOS installers. The macOS and Linux installers include a list of Message Relays at the time the installer was downloaded. The Windows installer retrieves a list of Update Caches from Sophos Central as part of the installation.

Update Caches and Message Relays are not always required and are not always a good fit in every environment, or at every site.



# Troubleshooting Communication between Sophos Central and Managed Devices

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE3025: Troubleshooting Communication between Sophos Central and Managed Devices

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.

# Troubleshooting Communication

In this chapter you will learn how to troubleshoot managed devices that are not communicating with Sophos Central.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

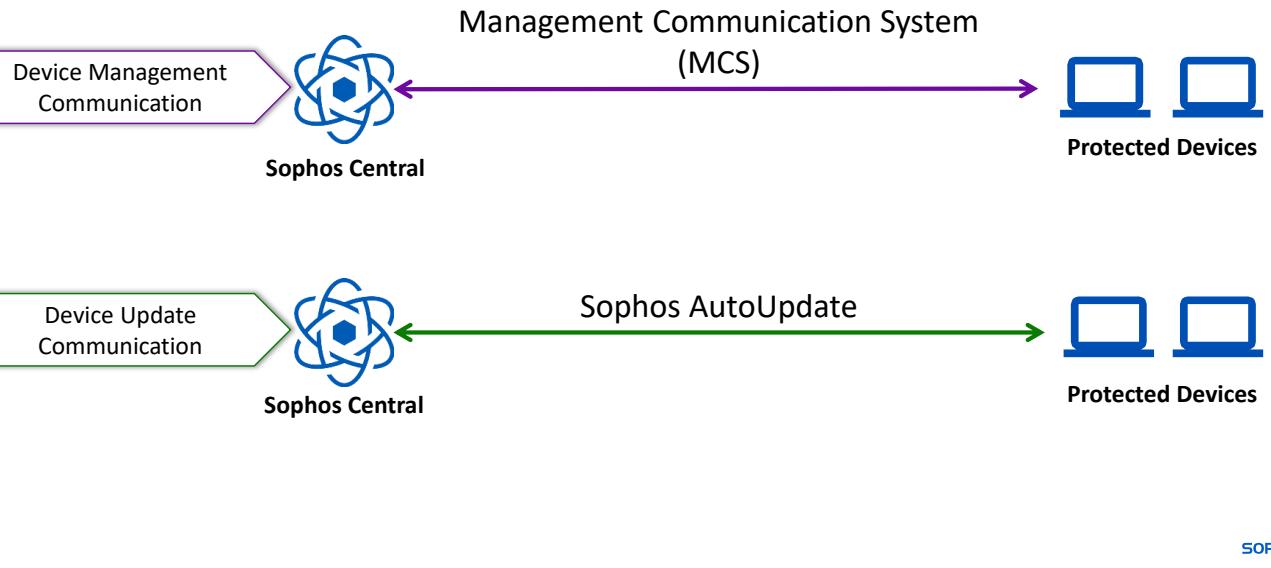
- ✓ Management of devices in Sophos Central
- ✓ How to manage Tamper Protection
- ✓ How to access the ESH tool

DURATION     **16 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot managed devices that are not communicating with Sophos Central.

# Device Management and Update Communication



There are a number of reasons you may need to perform troubleshooting for a managed device. For example, a device is not communicating with Sophos Central or not updating successfully.

Protected devices communicate management traffic using MCS and communicate updating traffic using Sophos AutoUpdate which is responsible for updating Sophos components installed on devices and the data used to provide threat protection.

Often, communication issues between Sophos Central and protected devices will affect both updating and management, therefore, the troubleshooting of these two components is similar.



Additional information in  
the notes

# Troubleshooting Communication

Run a Network Test as a first check if:

The **Update** tab displays a **bad health** state

The **Management Communication** tab displays a **bad health** state

If devices appear offline when using Live Discover or Live Response

If real-time scanning – Internet or Web Control functionality is not working

The screenshot shows the Sophos Endpoint Self Help Tool interface. The left sidebar has tabs for Known Issues, Network Test (which is selected and highlighted in red), File Info, and Product Logging. The main area is titled 'Network Test' with a 'Run' button. Below it, under 'Updating', there are three items: 'https://sus.sophosupd.com' (failed), 'https://sdds3.sophosupd.com' (failed - HTTPS response test failed, but ping and domain name tests succeeded), and 'https://sdds3.sophosupd.net' (failed). Under 'Management Communication', there is one item: 'Management Communication' (failed). Under 'Remediation', there is a link to a Knowledge Base Article. A 'Launch SDU' button is at the bottom left. A 'Did this help you?' poll is at the bottom right with 'Yes' selected.

To investigate communication issues between a protected device and Sophos Central we recommend that you use the **Network Test** tool in the Endpoint Self Help Tool. The **Network Test** tool provides a method to check specific communication channels directly to Sophos. The tests will determine whether certain checks succeed or fail, providing feedback on the specific areas of failure that can be troubleshooted further. While the network tests can be run at any time, they should be run as a first check if:

- The **Update** tab is showing a bad health status
- The **Management Communication** tab is showing a bad health status
- If devices appear offline when using Live Discover or Live Response in Sophos Central
- If the real-time scanning - Internet or Web Control functionality is not working

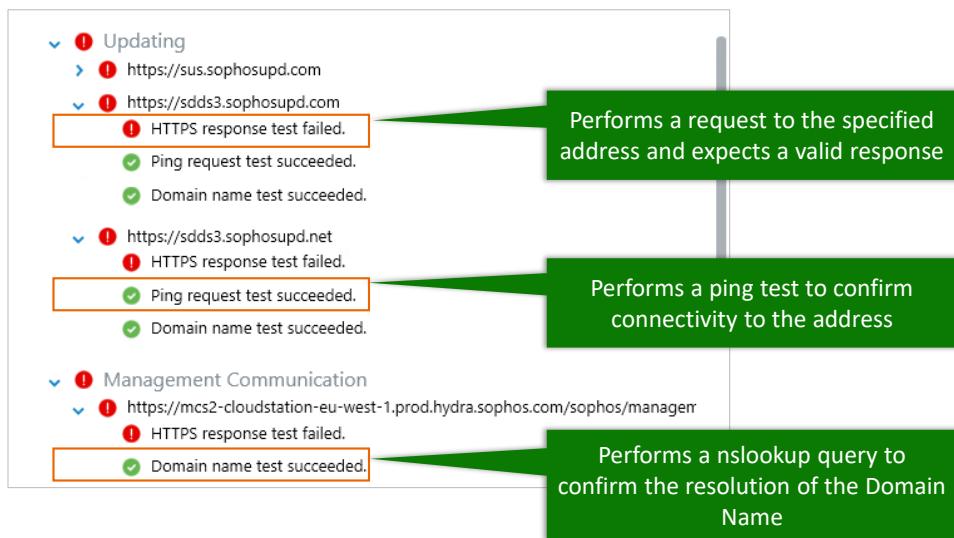
It is important to understand that in Sophos Central a device will not display a bad health status if it has not updated or communicated with Sophos Central in a few weeks. This is because it is usual that devices are not used for periods of time, for example, if users are not working for a few weeks, or over weekends. Therefore, to determine if a device is failing to communicate, we recommend running regular computer reports, so you understand what is usual in the organization. This will enable you to determine if there is a potential issue that requires investigation.

## [Additional Information]

Network Test KB-000042966. <https://support.sophos.com/support/s/article/KB-000042966>



# Troubleshooting Communication



SOPHOS

When you run the network test tool, the following checks will be performed:

- The Sophos Updating addresses and Management Communication addresses are tested and verified
- A ping test is performed to test connectivity to the addresses
- The domain name of the servers are tested and verified using the nslookup command

If these tests come back as failed, this will indicate where a potential issue may be. Cross reference the **Last Communication** timestamp with the **Last Successful** timestamp in the Endpoint Self Help tool for updating and management communication and check for any significant changes to the network infrastructure since the **Last Successful** timestamp.

If a proxy is used, confirm that the proxy address is correct.

## [Additional Information]

**KB-000036450** provides troubleshooting steps for Management Communication.

<https://support.sophos.com/support/s/article/KB-000036450>

**KB-000034818.** <https://support.sophos.com/support/s/article/KB-000034818>



Additional information in  
the notes

# Troubleshooting Communication

- Run a trace route (tracert) command to the Management Communication server address
- Confirm the Management Communication server address matches the address specified in the config.xml

<< Local Disk (C:) > ProgramData > Sophos > Management Communications System > Endpoint > Config

- Ensure the proxy is not running in transparent mode or requires authentication
- Check that the Sophos Update and Management Communication server addresses are not being blocked by the proxy server
- Check the Sophos Update and MCS logs for error

> This PC > Local Disk (C:) > ProgramData > Sophos > Management Communications System > Endpoint > Logs

> This PC > Local Disk (C:) > ProgramData > Sophos > AutoUpdate > Logs

- Ensure that the Update and Management Communication server addresses are allowed through any firewalls in place

SOPHOS

Additional troubleshooting steps that should be run if the network test returns errors include:

- Running a trace route command to the management communication server address to ensure the routing is correct and reachable
- Confirming the management communication server address matches the address specified in the config.xml
- Ensuring that the proxy (if used) is not running in transparent mode or requires authentication and ensure that the server address is not being blocked
- Check the Sophos Update and Sophos Management Communication logs for errors
- Ensure that the Update and Management Communication server addresses are allowed through any firewalls in place. If you are unable to allow domain names, ensure the IP address ranges are allowed

## [Additional Information]

config.xml is found C:\ProgramData\Sophos\Management Communications System\Endpoint\Config  
Update Log is found C:\ProgramData\Sophos\AutoUpdate\Logs

MCS Client and Agent logs are found: C:\ProgramData\Sophos\Management Communications System\Endpoint\Logs

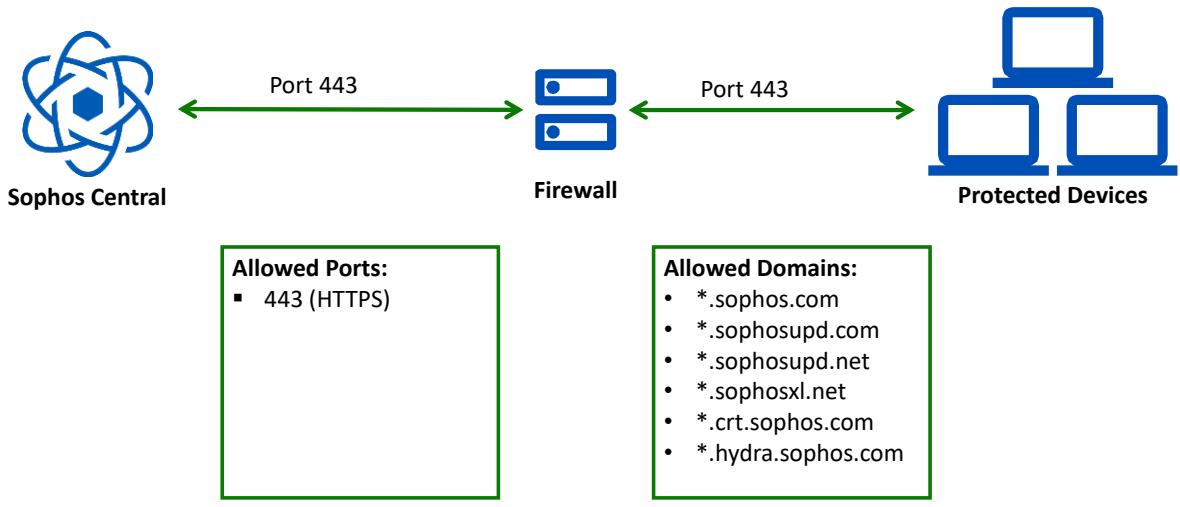
Advanced management communication **KB-000036507**.

<https://support.sophos.com/support/s/article/KB-000036507>



Additional information in  
the notes

# Communication Domains and Ports



SOPHOS

This diagram summarizes the domains that must be allowed to allow communication between protected devices and Sophos Central.

A detailed list of all domains required can be found in the Sophos Central help documentation.

Let's have a look at a few communication troubleshooting scenarios.

## [Additional Information]

The required domains and ports are listed in the Sophos Central documentation here:

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

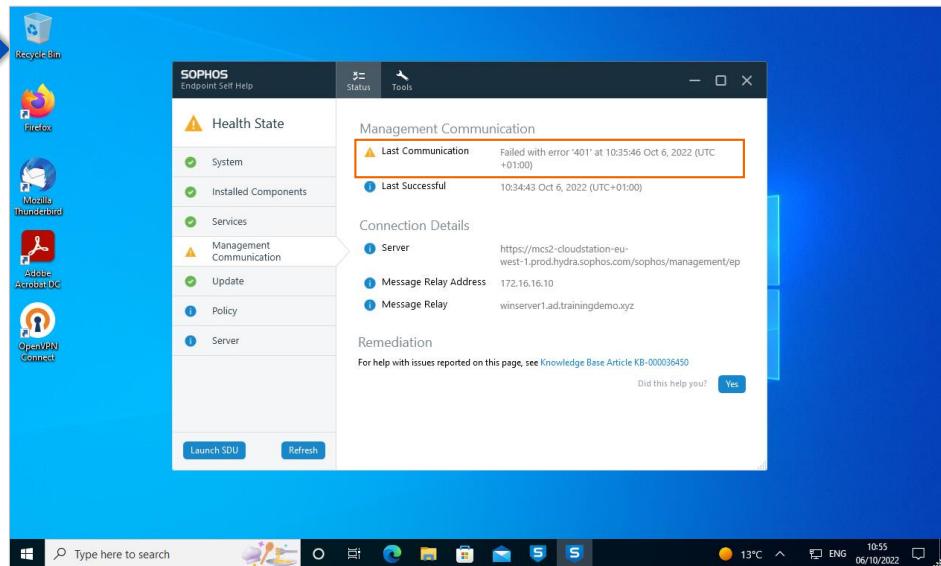
IP address ranges for firewall: <https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>

# Scenario One

1

Device not communicating

A device (WinClient4) is returning a 401 error code for Management Communication.



In this scenario, Client 4 is a managed device that is no longer communicating with Sophos Central. The Endpoint Self Help tool is displaying a 401 error code on the Management Communication tab.

## Scenario One

McsClient - Notepad

```
File Edit Format View Help
2022-10-06T10:13:57.906Z [ 3288: 724] I PUT https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/management/api/v1/management/agent/88411a01-827c-2d3e-5840-20a5bbda665
2022-10-06T10:13:58.931Z [ 3288: 724] I 401 : sent=10710 rcvd=0 elapsed=1025ms
2022-10-06T10:13:58.931Z [ 3288: 724] W Dropping connection after error
2022-10-06T10:13:58.932Z [ 3288: 724] I [backoff] waiting 7652s (7200s + 452s skew) after failures: 13
2022-10-06T10:14:26.455Z [ 3288: 724] I Re-evaluating order of preference of message relays.
2022-10-06T10:14:28.711Z [ 3288: 724] W Failed to lookup reading3. This message relay will be ignored.
2022-10-06T10:14:28.713Z [ 3288: 724] W Failed to lookup srv.sophos.local. This message relay will be ignored.
2022-10-06T10:14:28.757Z [ 3288: 724] I [connect] trying server https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/api/v1/management/ep
2022-10-06T10:14:28.757Z [ 3288: 724] I [connect] trying message relay: winserver1.ad.trainingdemo.xyz:8190
2022-10-06T10:14:28.757Z [ 3288: 724] I GET https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep
2022-10-06T10:14:29.095Z [ 3288: 724] I 200 : sent=0 rcvd=168 elapsed=320ms
2022-10-06T10:14:29.095Z [ 3288: 724] I [connect] using server https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/api/v1/management/ep via message relay winserver1.ad.trainingdemo.xyz:8190 (peer address 172.16.16.10)
2022-10-06T10:14:29.100Z [ 3288: 724] I PUT https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/management/api/v1/management/agent/88411a01-827c-2d3e-5840-20a5bbda665
2022-10-06T10:14:30.138Z [ 3288: 724] I 401 : sent=10710 rcvd=0 elapsed=1037ms
2022-10-06T10:14:30.139Z [ 3288: 724] I Dropping connection after error
2022-10-06T10:14:30.140Z [ 3288: 724] I [backoff] waiting 8780s (7200s + 1580s skew) after failures: 14
```

The code indicates unauthorized access

### 4xx Client Error

- ★ 400 Bad Request
- ★ 403 Forbidden
- 406 Not Acceptable
- ★ 409 Conflict
- 412 Precondition Failed
- 415 Unsupported Media Type
- 418 I'm a teapot (RFC 2324)
- 423 Locked (WebDAV)
- 426 Upgrade Required
- 431 Request Header Fields Too Large
- 450 Blocked by Windows Parental Controls (Microsoft)

- ★ 401 Unauthorized
- ★ 404 Not Found
- 407 Proxy Authentication Required
- 410 Gone
- 413 Request Entity Too Large
- 416 Requested Range Not Satisfiable
- 420 Enhance Your Calm (Twitter)
- 424 Failed Dependency (WebDAV)
- 428 Precondition Required
- 444 No Response (Nginx)
- 451 Unavailable For Legal Reasons

We check the MCS client log for errors.

There are 401 errors listed in the log file. An HTTP 401 error is a standard Windows response code that indicates a request lacks valid authentication credentials for the target resource. Authorization of a device happens using a registration token that is assigned to each device during agent installation. When contacting Sophos Central for management updates, the device presents the token which is validated by Sophos Central.

In this scenario, that validation is failing.

### [Additional Information]

MCS Client log can be found in file directory C:\ProgramData\Sophos\Management Communication System\Endpoint\Logs

HTTP status codes: <https://www.restapitutorial.com/httpstatuscodes.html>

# Scenario One



SOPHOS

Sophos Central

Computers

View and manage your computers

Help - Simon Smith -  
Sophos UK - Super Admin

Computers Mobile Devices Servers Unmanaged devices

Manage Endpoint Software Turn on tamper protection Retrieve Recovery Key Reset health status Export to CSV

Windows Computers Show all computers Any protection types Search

Name	IP	OS	Protection	Encryption	Last updated
Training-W10	...	Windows 10 Enterprise	✓ Intercept X Advanced with XDR	+	Training
WinClient1	...	Windows 10 Pro	✓ Intercept X Advanced with XDR	+	Sophos
WinClient5	...	Windows 10 Pro	✓ Intercept X Advanced with XDR	+	Training
WinClient2	...	Windows 10 Pro	✓ Intercept X Advanced with XDR	+	admin
Windows-XRD	...	Windows 10 Enterprise	⊕ XDR Sensor	+	Admin

1 - 5 of 5 computers / 0 selected

Last updated: Oct 6, 2022, 11:24 AM

SOPHOS

Let's check the device details in Sophos Central.

The WinClient4 device is missing from the device list. This means that Sophos Central is unable to authorize the device for management communication.

# Scenario One



The screenshot shows the Sophos Central interface with the 'Audit Log' page open. The left sidebar includes 'Logs & Reports' under 'Logs & Reports'. The main area displays an audit log table with columns: DATE, MODIFIED BY, ITEM TYPE, ITEM MODIFIED, and DESCRIPTION. An orange box highlights the last two rows of the log:

DATE	MODIFIED BY	ITEM TYPE	ITEM MODIFIED	DESCRIPTION
Oct 6, 2022 10:14:27 AM	ssmith@sophostrainin...	Authentication	ssmith@sophostraining.xyz	Login atte...
Oct 6, 2022 10:14:27 AM	ssmith@sophostrainin...	Authentication	ssmith@sophostraining.xyz	Login atte...
Oct 6, 2022 10:50:58 AM	ben.smith@sophostrai...	Computers	WinClient3	Delete on...
Oct 6, 2022 10:29:15 AM	ben.smith@sophostrai...	Computers	WinClient4	Delete on...

Below the log is an Excel spreadsheet titled 'audit(2)'. The first row contains headers: Date, Modified By, Item Type, Item Modified, and Description. The second row contains data corresponding to the highlighted log entries.

The next step is to check the audit log to identify any changes made to the device.

WinClient4 was modified by user Ben Smith. You can scroll across this page to view further details in Sophos Central, however, let's view the exported log. From the log we can see that WinClient4 was deleted from Sophos Central.

When a device is deleted in Sophos Central but the Sophos Endpoint Agent is not uninstalled on the device, any messages received using the endpoint identifier will be actively rejected by Sophos Central. Administrators are warned to remove the Sophos Endpoint Agent when selecting to delete a device from Sophos Central for this reason.

## Scenario One



If Tamper Protection was enabled on the device, any re-installation attempts will fail

Identify the Tamper Protection password for the deleted device using the Recover Tamper Protection passwords report

NAME/OS	DELETED AT	TAMPER PROTECTION	PASSWORD
WinClient3 Windows 10	an hour ago	On	<a href="#">View password details</a>
WinClient4 Windows 10	2 hours ago	On	<a href="#">Hide password details</a> • 406236589664
linuxserver1 Ubuntu 20.04.4 LTS	2 months ago	On	<a href="#">View password details</a>
WinServer2 Windows Server 2019 Standard	2 months ago	On	<a href="#">View password details</a>

SOPHOS

To resolve this issue the device must be re-registered, this can be completed by running an elevated command to re-register the device with Sophos Central.

If tamper protection was enabled on the device, you will need to disable it locally before re-registering the device. To do this, you will need to use the **Recover Tamper Protection passwords** report in Sophos Central to view the password for the deleted device.

# Scenario One



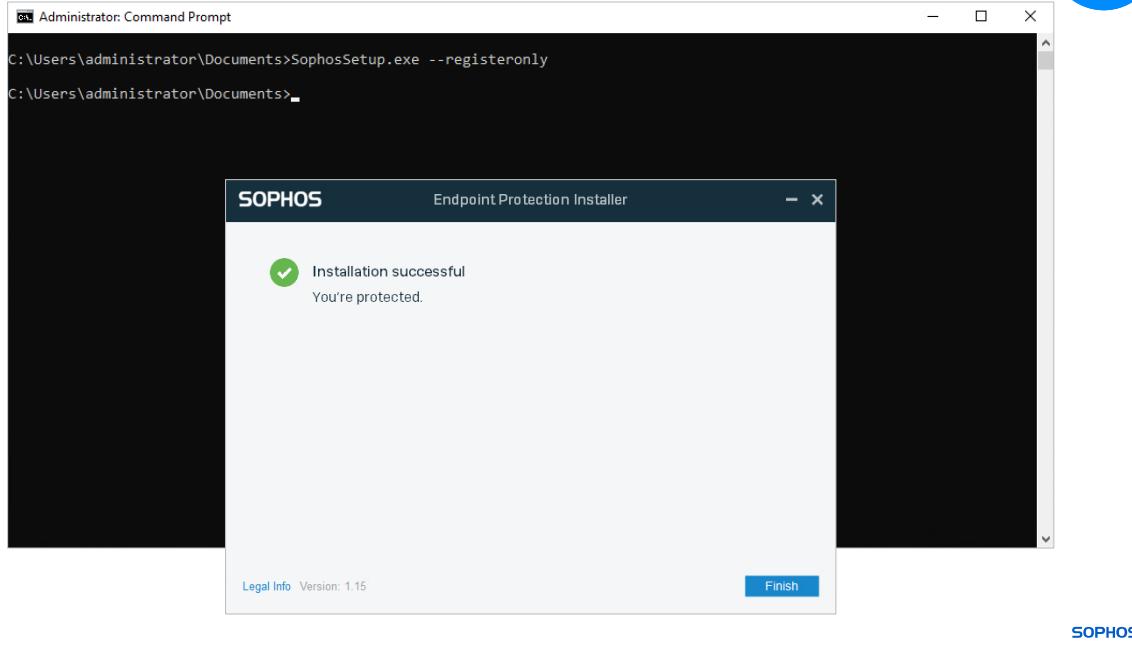
The screenshot shows the Sophos Endpoint Agent interface. On the left, there's a sidebar with 'Update Status' (Last update: 06 October 2022 14:13), 'Products' (Core Agent 2022.2.1, Sophos Intercept X 2022.1.122, Device Encryption 2022.1.0.58), and 'Troubleshooting' (Open Endpoint Self Help Tool). The main area has a search bar and a message: 'Enter tamper protection password' followed by a redacted password and a blue 'Admin sign-in' button. Below this is a note: 'Signing in as an admin lets you view and change settings. To sign in, enter the tamper protection password for this device. You can find it in Sophos Central.' On the right, the 'Settings' tab is selected. It contains sections for 'Deep Learning' (Enable Deep Learning), 'Real Time Scanning' (Files, Internet), 'Controls on Users' (Peripheral Control, Web Control, Tamper Protection - highlighted with a red box), 'Runtime Protection' (Ransomware Detection, Exploit Mitigation, Malicious Behavior Detection), and 'Miscellaneous' (Safe Browsing, Network Threat Protection, AMSI Protection). A checkbox for 'Override Sophos Central Policy for up to 4 hours to troubleshoot' is also present.

Sign into the Sophos Endpoint Agent on the device with the tamper protection password.

In the ‘Settings’ tab, select to **Override Sophos Central Policy for up to 4 hours to troubleshoot** and disable **Tamper Protection**.

## Scenario One

2



Now that tamper protection has been disabled locally, you can re-register the device with Sophos Central.

Open an elevated command prompt, navigate to the file location for SophosSetup.exe and run the command SophosSetup.exe with the parameter **--registeronly**.

This will initiate the installer on the device, which will re-register the device with Sophos Central.

### [Additional Information]

For macOS devices **KB-000035092**. <https://support.sophos.com/support/s/article/KB-000035092>

# Scenario One

3

The screenshot shows the Sophos Central interface. On the left, the navigation bar has 'Devices' selected. The main area is titled 'Computers' with a sub-section 'Windows Computers'. It lists three devices: 'WinClient4', 'Training-W10', and 'WinClient3'. A green callout box points to 'WinClient4' with the text 'The device is listed in Sophos Central'. Another green callout box points to the top right of the screen with the text 'The device is successfully communicating with Sophos Central'. The right side of the screen displays a 'Sophos Endpoint Self Help' window with tabs for 'Status', 'Tools', 'Management Communication' (showing 'Last Communication' succeeded at 12:06:11 Oct 6, 2022), 'Connection Details' (listing 'Server', 'Server Address' as 34.249.110.120, and 'Proxy' as 'No proxy used'), and 'Remediation'.

Once the Sophos Endpoint Agent has been re-installed, the device is listed in the protected 'Computers' list in Sophos Central.

The device will also now receive management updates as needed.

## Scenario Two



Device failing to communicate

A device (WinClient4) is failing to communicate with Sophos Central.

The screenshot shows the Sophos Endpoint Self Help interface. On the left, a sidebar lists categories: Health State (red exclamation mark), System (green checkmark), Installed Components (green checkmark), Services (green checkmark), Management Communication (red exclamation mark), Update (red exclamation mark), Policy (blue information icon), and Server (blue information icon). The main panel displays 'Update Status' with three entries: Latest Update (yellow triangle) at 09:19:25 Oct 10, 2022 (UTC+01:00); Last Successful Update (red circle) at 09:28:41 Oct 7, 2022 (UTC+01:00); and First Failed Update (blue circle) at 09:41:24 Oct 7, 2022 (UTC+01:00). Below this is 'Update Configuration' with three entries: Update Location (blue circle) set to Sophos; Proxy (blue circle) set to No proxy used; and Used Credentials (blue circle) set to BN47YC4ZCW. At the bottom right is a 'Did this help you?' button with 'Yes' checked. The Sophos logo is in the bottom right corner of the window.

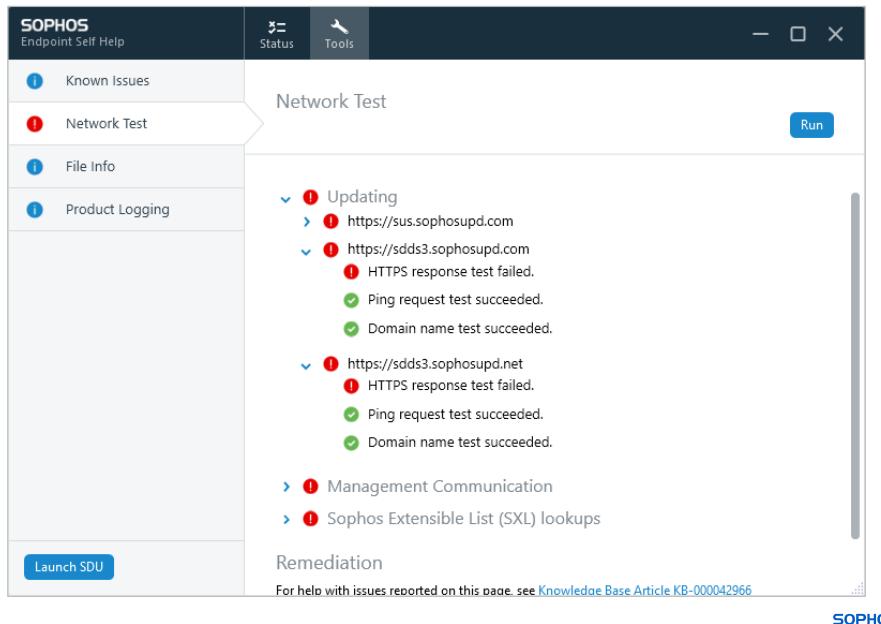
In this scenario a device is trying to update from Sophos Central, but the communication is failing.

The Endpoint Self Help tool displays the 'Update Status' which shows the last successful update date, the first failed update date and the latest update date.

## Scenario Two

2

Run the Network Test tool.



The first troubleshooting step is to run the **Network Test** tool in the Endpoint Self Help Tool.

In this scenario, the domain name is successfully resolved, and the Sophos update server can be connected to with a ping request indicating that there is no issue with the destination, this indicates that a setting on the device might be the cause of this issue.

## Scenario Two



```
SophosUpdate.log - Notepad
File Edit Format View Help
2022-10-10T10:02:52.658Z [ 1108: 6388] D WinHttpSetStatusCallback(&httpCallback)
2022-10-10T10:02:52.658Z [ 1108: 6388] D WinHttpSendRequest(... 0 byte body in one shot)
2022-10-10T10:02:52.659Z [ 1108: 6388] W Error from https://sdds3.sophosupd.net with proxy: <direct; no proxy>: WinHttpSendRequest failed: A connection with the server could not be established (12029)
2022-10-10T10:03:22.674Z [ 1108: 6388] I Trying SDDS3 CWW url https://sdds3.sophosupd.net with proxy: <direct; no proxy> (try 5 or 5)
2022-10-10T10:03:22.674Z [ 1108: 6388] D WinHttpOpen(userAgent="SophosUpdate/6.13.1014 SDDS/3.0 (t="5550411b-07d2-48bd-9679-bc09a660403d" d="8814e11a-28a7-42e3-850f-93ae9bd6e56" os="WIN_10_X64" osrel="2009 19044.2006")", accessType=1, proxy="", proxyBypass="", useHttps=1)
2022-10-10T10:03:22.674Z [ 1108: 6388] D WinHttpSetOption(WINHTTP_OPTION_SECURE_PROTOCOLS, &WINHTTP_FLAG_SECURE_PROTOCOL_TLS1_2)
2022-10-10T10:03:22.674Z [ 1108: 6388] D WinHttpSetOption(WINHTTP_OPTION_AUTOLOGON_POLICY, &WINHTTP_AUTOLOGON_SECURITY_LEVEL_HIGH)
2022-10-10T10:03:22.674Z [ 1108: 6388] D WinHttpSetTimeouts(resolveMs=5000, connectMs=5000, sendMs=5000, recvMs=5000)
2022-10-10T10:03:22.675Z [ 1108: 6388] D WinHttpConnect(host="sdds3.sophosupd.net", port=443, 0)
2022-10-10T10:03:22.675Z [ 1108: 6388] D WinHttpOpenRequest(verb="HEAD", absResource="/suite/sdds3.WindowsCloudAV_11.6.562.93124a541a.dat", NULL, WINHTTP_NO_REFERER, WINHTTP_DEFAULT_ACCEPT_TYPES, flags=8388672)
2022-10-10T10:03:22.675Z [ 1108: 6388] D WinHttpSetStatusCallback(&httpCallback)
2022-10-10T10:03:22.675Z [ 1108: 6388] D WinHttpSendRequest(... 0 byte body in one shot)
2022-10-10T10:03:22.676Z [ 1108: 6388] W Error from https://sdds3.sophosupd.net with proxy: <direct; no proxy>: WinHttpSendRequest failed: A connection with the server could not be established (12029)
2022-10-10T10:03:22.676Z [ 1108: 6388] W No reachable update locations
2022-10-10T10:03:22.676Z [ 1108: 6388] D calculate_package_thumprint()
2022-10-10T10:03:22.676Z [ 1108: 6388] D visit suite sdds3.WindowsCloudNextGen_2022.2.2.1.0.52b88181d9.dat
2022-10-10T10:03:22.676Z [ 1108: 6388] D visit loaded suite sdds3.WindowsCloudNextGen_2022.2.2.1.0.52b88181d9.dat
Ln 153144, Col 201 100% Windows (CRLF) UTF-8
```

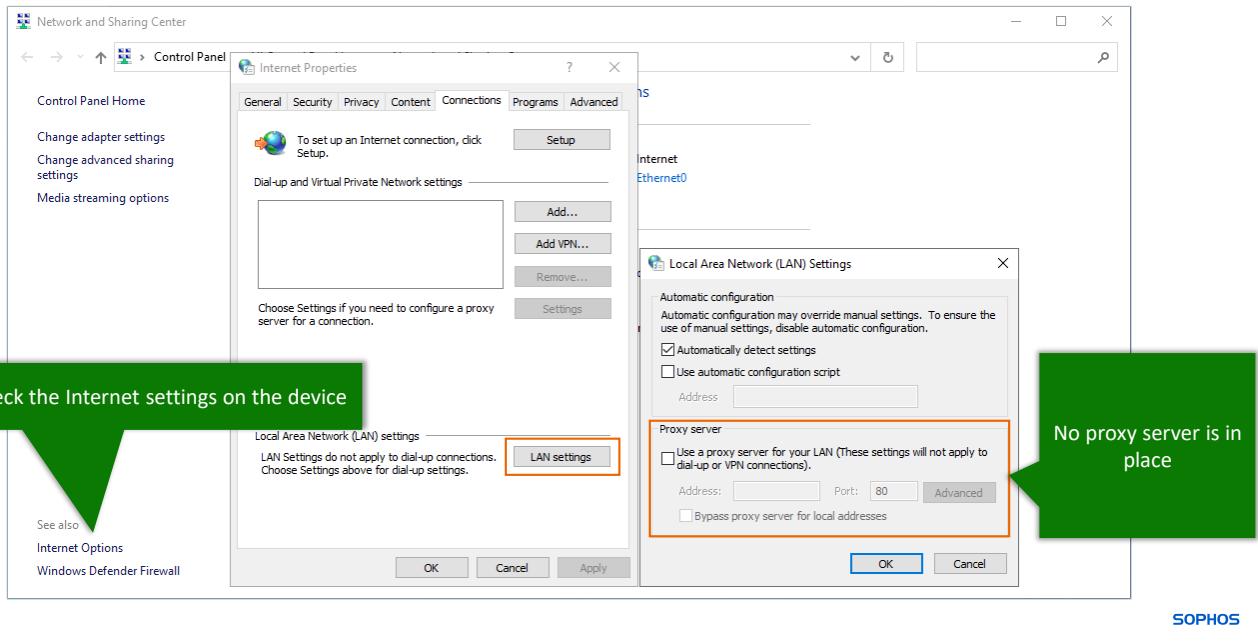
SOPHOS

It is a good idea to check the log files to see if any errors are returned. The Sophos Update log confirms that the device is trying to make a direct connection to Sophos Central with no update caches or proxy configured. It tries and fails to connect to each of the Sophos update servers.

The error further down the log file confirms that there are no reachable update locations.

## Scenario Two

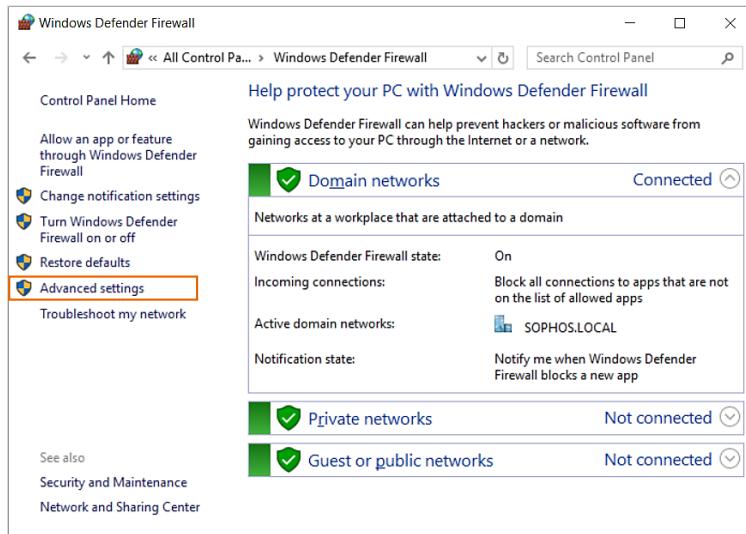
2



The advanced troubleshooting recommends checking the Internet settings on a device.

In this scenario we check the Internet settings on the device, in the LAN settings we can see that there is no proxy being used so the connection is not being blocked at the proxy level.

## Scenario Two



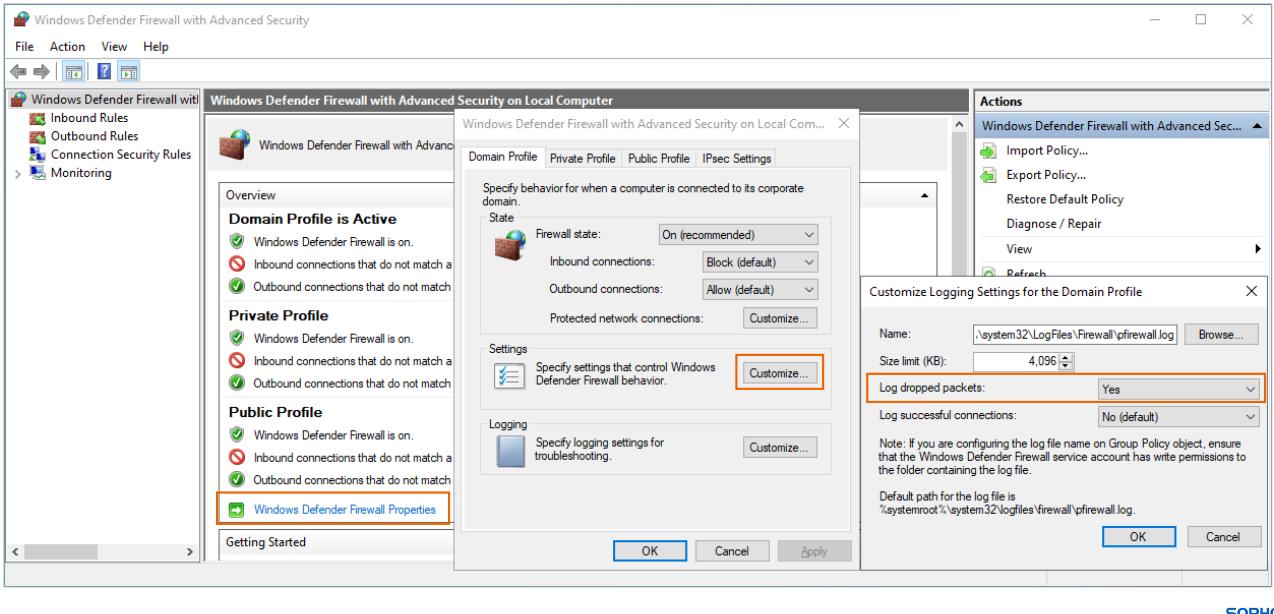
SOPHOS

The next step is to look at the client firewall. On Windows, navigate to **Control Panel > Windows Defender Firewall** this will display the firewall settings for the device.

In this scenario, the firewall is enabled for all networks and the device is currently connected to a domain network.

In the advanced settings you can configure logging and view any firewall rules for the device.

## Scenario Two



Windows Defender Firewall properties can be used to customize logging.

Typically enabling logging of dropped packets is the best way to identify issues. The logging settings page also shows the location and name of the log file.

## Scenario Two

2

The Windows Firewall log confirms that TCP packets sent to external IP addresses using port 443 are being dropped.

Check the outbound firewall rules for any block actions

TCP packets to external IP addresses on port 443 are being dropped

Name	Group	Profile	Enabled	Action	Override	Program
Block direct HTTPS	All	Yes	Block	No	Any	@Microsoft.Getstarted_10441931...
@Microsoft.MicrosoftEdge_44177631...	All	Yes	Allow	No	Any	@Microsoft.MicrosoftEdge...
@Microsoft.MicrosoftEdge_44177631...	All	Yes	Allow	No	Any	@Microsoft.MicrosoftEdge...
@Microsoft.MicrosoftEdge_44177631...	All	Yes	Allow	No	Any	@Microsoft.MicrosoftEdge...
@Microsoft.Windows.CloudExperience...	All	Yes	Allow	No	Any	@Microsoft.Windows.Cloud...
@Microsoft.Windows.ContentDeliveryM...	All	Yes	Allow	No	Any	@Microsoft.Windows.ContentDel...
@Microsoft.Windows.ShellExperienceC...	All	Yes	Allow	No	Any	@Microsoft.Windows.Shell...
@FirewallAPI.dll_80204	All	Yes	Allow	No	%System%	@FirewallAPI.dll_80200
Skype	(7BE1CD88-40E3-476E-B926...	All	Yes	Allow	No	C:\Program...
3D Viewer	3D Viewer	All	Yes	Allow	No	Any
3D Viewer	3D Viewer	All	Yes	Allow	No	Any
AllInOn Router (TCP-Out)	AllInOn Router	Doma...	Yes	Allow	No	%System%
AllInOn Router (UDP-Out)	AllInOn Router	Doma...	Yes	Allow	No	%System%
App Installer	App Installer	All	Yes	Allow	No	Any
App Installer	App Installer	All	Yes	Allow	No	Any
App Installer	App Installer	All	Yes	Allow	No	Any
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM
BranchCache Hosted Cache Client (HTTP-...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM

The Windows Firewall log confirms that TCP packets sent to external IP addresses using port 443 are being dropped.

Locate the firewall rules for the device. Sorting the action column into reverse alphabetical order will display any block rules at the top of the list. In this example, the name of the rule makes it easily identifiable.

## Scenario Two



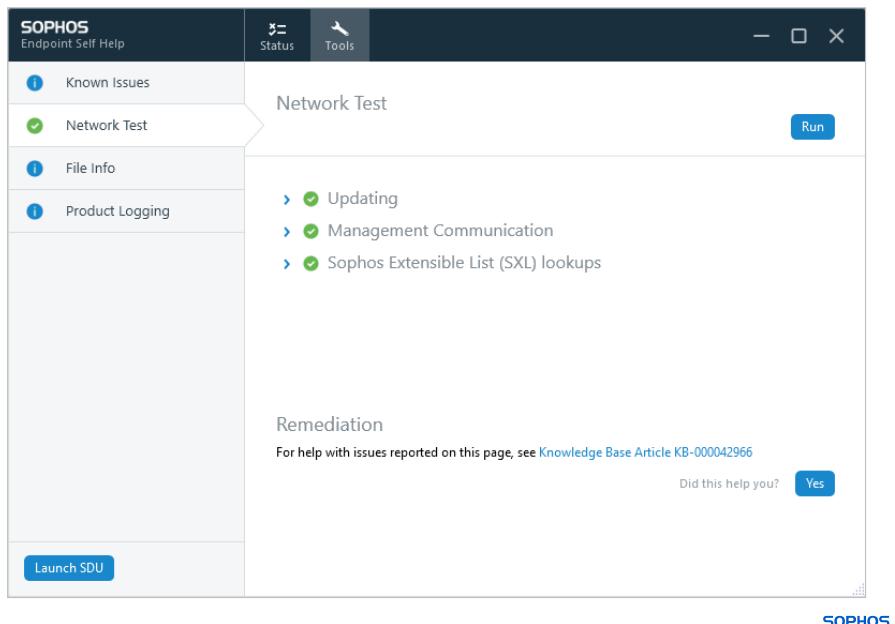
Configured to block outbound traffic on port 443 from any device on the 172.16.16.0/24 network

The firewall rule in this scenario is configured to block outbound traffic using TCP port 443 from any device on the network. This explains why the updating was failing on this device. To confirm this is the issue, temporarily disable the rule and force an update on the device.

Depending on the environment, there could be a valid reason for blocking outbound traffic in this way. Therefore, it is worth considering why a firewall rule has been configured and think of alternative solutions. In this scenario, the organization could configure the device to use a proxy for updating by using the command `netsh winhttp set proxy <server>:<port>`.

## Scenario Two

- Disable the firewall rule
- Click **Update Now**
- The device is successfully communicating with Sophos Central
- The Network Test is returning successful connections



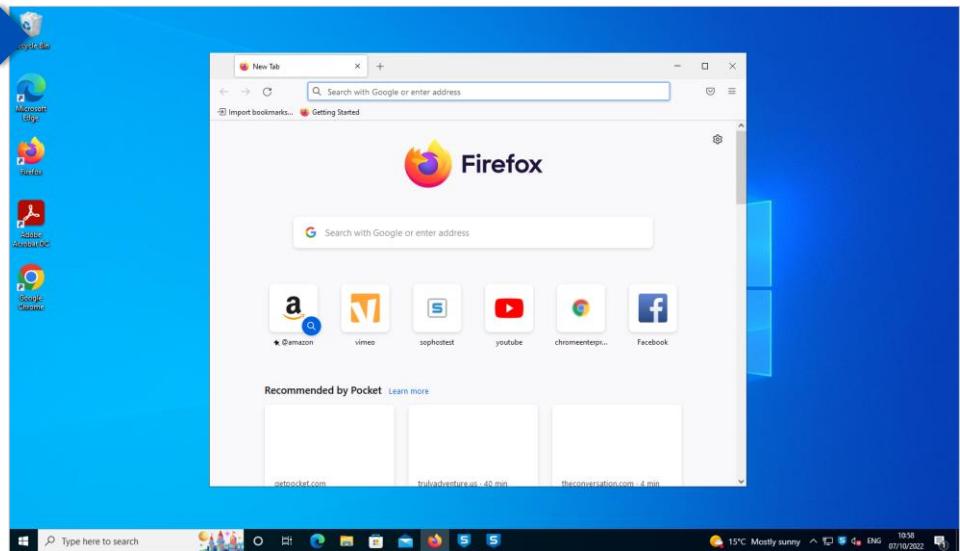
With the block firewall rule disabled the device is now successfully communicating with Sophos Central.

## Scenario Three

1

Device failing to receive a policy

A device (WinClient2) is failing to receive an application policy blocking the use of FireFox.



SOPHOS

In this scenario, a user is able to access the Internet browser FireFox which has been blocked using an application control policy in Sophos Central.

This suggests that the device is not communicating with Sophos Central.

## Scenario Three



The screenshot shows two windows side-by-side. On the left is the Sophos Endpoint Agent interface, which includes sections for Update Status (warning: Last update failed: 07 October 2022 10:50), Products (Core Agent 2022.2.1, Sophos Intercept X 2022.1.22), and Troubleshooting (Open Endpoint Self Help Tool). A green callout box points to the 'Update Now' button with the text: 'The Sophos Endpoint Agent displays the update status'. On the right is the Sophos Endpoint Self Help tool, showing a tree view of Health State, System, Installed Components, Services, Management Communication, and Update (warning: Update failed). It also shows Update Status (Latest Update: 10:50:26 Oct 7, 2022 (UTC+01:00), Last Successful Update: 10:12:21 Oct 7, 2022 (UTC+01:00), First Failed Update: 10:25:59 Oct 7, 2022 (UTC+01:00)), Update Configuration (Update Location: Sophos, Proxy: No proxy used, Used Credentials: BN47YC4ZCW), and Remediation (link to Knowledge Base Article KB-000036449). A green callout box points to the 'Tools' menu with the text: 'The Endpoint Self Help tool displays Update Status. The last successful update was at 10:12am'.

The first step is to check the Sophos Endpoint Agent on the affected device. It displays a **Last Update failed** message.

We open the Endpoint Self Help tool to view more information. We can see that the latest update is failing.

## Scenario Three



The Management Communication last succeeded at 10.14am and not since

SOPHOS Endpoint Self Help

Status Tools

Health State

System

Installed Components

Services

Management Communication

Update

Policy

Server

Launch SDU Refresh

Management Communication

Last Communication Succeeded at 10:14:41 Oct 7, 2022 (UTC+01:00)

Connection Details

Server https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep

Server Address 52.211.27.60

Proxy No proxy used

Remediation

For help with issues reported on this page, see [Knowledge Base Article KB-000036450](#)

Did this help you? Yes

SOPHOS

We check the **Management Communication** tab to see if the device is receiving management traffic. The last communication date is 10:14am in this scenario. The last update failed at 10:50am which indicates that the device is not communicating with Sophos Central successfully.

# Scenario Three



```
SophosUpdate - Notepad
File Edit Format View Help
2022-10-07T10:12:12.213Z [10876: 3740] I Performing standard update
2022-10-07T10:12:12.213Z [10876: 3740] I Limiting bandwidth to 256 Kbps
2022-10-07T10:12:12.213Z [10876: 3740] I Using cached Sophos Update Service configuration
2022-10-07T10:12:12.214Z [10876: 3740] I Syncing suite [sdds3.WindowsCloudAV_11.6.562.93124a541a.dat, sdds3.WindowsCloudClean_1.0.42.55133bcba5.dat, sdds3.WindowsCloudEncryption_26]
2022-10-07T10:12:12.214Z [10876: 3740] I Releasing groups [C]
2022-10-07T10:12:12.214Z [10876: 3740] I Analyzing whether to update from Sophos CDN or update cache
2022-10-07T10:12:14.514Z [10876: 3740] I Could not reach cache: https://reading3:8191/v3/suite: WinHttpSendRequest failed: The server name or address could not be resolved (12007)
2022-10-07T10:12:14.514Z [10876: 3740] I Analysis complete - Using Sophos CDN
2022-10-07T10:12:14.514Z [10876: 3740] I No manually configured proxy
2022-10-07T10:12:14.515Z [10876: 3740] I WinHttp default proxy not set
2022-10-07T10:12:14.515Z [10876: 3740] I WinHttp default proxy not set
2022-10-07T10:12:14.520Z [10876: 3740] I Trying SDD53 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy>
2022-10-07T10:12:20.228Z [10876: 3740] W Error from https://sdds3.sophosupd.com with proxy: <direct; no proxy>: WinHttpSendRequest failed: The operation timed out (12002)
2022-10-07T10:12:20.479Z [10876: 3740] I Trying SDD53 CDN url https://sdds3.sophosupd.com with proxy: <direct; no proxy> (try 2 of 5)
```

C:\ProgramData\Sophos\AutoUpdate\Logs

```
McsClient - Notepad
File Edit Format View Help
2022-10-07T10:12:21.383Z [3220: 1184] I [backoff] waiting 1000ms (7200s + 2808s skew) after failures: 67
2022-10-07T10:12:48.489Z [3220: 1184] I Re-evaluating order of preference of message relays.
2022-10-07T10:12:50.757Z [3220: 1184] W Failed to lookup reading3. This message relay will be ignored.
2022-10-07T10:12:50.758Z [3220: 1184] W Failed to lookup srv.sophos.local. This message relay will be ignored.
2022-10-07T10:12:50.760Z [3220: 1184] I [connect] trying server https://mcsc2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep
2022-10-07T10:12:50.760Z [3220: 1184] I [connect] trying direct connection without a proxy
2022-10-07T10:12:50.760Z [3220: 1184] I [connect] trying direct connection without a proxy
2022-10-07T10:13:06.182Z [3220: 1184] E Request failed: WinHttpSendRequest failed: The connection with the server was terminated abnormally (12030)
2022-10-07T10:13:06.182Z [3220: 1184] W [connect] no configured servers working, trying fall-back connection
2022-10-07T10:13:06.182Z [3220: 1184] I [connect] trying server https://mcsc2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep
2022-10-07T10:13:06.183Z [3220: 1184] I [connect] trying direct connection without a proxy
2022-10-07T10:13:06.183Z [3220: 1184] I [connect] trying direct connection without a proxy
2022-10-07T10:13:06.183Z [3220: 1184] E Request failed: WinHttpSendRequest failed: The connection with the server was terminated abnormally (12030)
2022-10-07T10:13:21.543Z [3220: 1184] W [connect] no working servers
2022-10-07T10:13:21.543Z [3220: 1184] I [backoff] waiting 8668s (7200s + 1468s skew) after failures: 68
```

C:\ProgramData\Management Communications System\Endpoint\Logs

SOPHOS

We check the logs for any errors. The Sophos Update log file shows that the device is unable to connect to Sophos Central to fetch updates as the operation timed out.

The MCS Client log shows that the device is unable to connect with the server.

## [Additional Information]

C:\ProgramData\Sophos\Management Communications System\Endpoint\Logs  
C:\ProgramData\Sophos\AutoUpdate\Logs

## Scenario Three



Administrator: Command Prompt

```
C:\Users\administrator>ping sophos.com
Pinging sophos.com [104.97.154.97] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 104.97.154.97:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\administrator>ping 52.211.27.60
Pinging 52.211.27.60 with 32 bytes of data:
Request timed out.

Ping statistics for 52.211.27.60:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\administrator>
```

Management Communication

Last Communication Succeeded at 10:14:41 Oct 7, 2022 (UTC+01:00)

Connection Details

- Server https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep
- Server Address **52.211.27.60**
- Proxy No proxy used

Remediation

For help with issues reported on this page, see [Knowledge Base Article KB-000036450](#)

Did this help you? Yes

SOPHOS

Perform a ping test to sophos.com and the management communication server IP address

We perform a ping test using the command prompt to test the connectivity to sophos.com.

We also run a ping command for the server IP address detailed in the **Management Communication** tab of the Endpoint Self Help tool.

Both commands return **request timed out**.

## Scenario Three

2

The screenshot shows the Sophos Endpoint Self Help Tool interface. On the left, there's a sidebar with 'Known Issues', 'Network Test' (selected), 'File Info', and 'Product Logging'. A 'Launch SDU' button is at the bottom. The main area is titled 'Network Test' and lists several test items:

- Updating
  - https://sus.sophosupd.com (Failed)
  - https://sdds3.sophosupd.com (Failed)
    - HTTPS response test failed.
    - Ping request test failed.
    - Domain name test succeeded.
  - https://sdds3.sophosupd.net (Failed)- Management Communication
  - https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com (Failed)
    - HTTPS response test failed.
    - Domain name test succeeded.
  - https://mcs-push-server-eu-west-1.prod.hydra.sophos.com/ (Failed)
- Sophos Extensible List (SXL) lookups (Failed)

A green callout box points to the 'Network Test' section with the text: "Run a Network Test in the Tools menu of the Endpoint Self Help tool".

A green callout box points to the browser window with the text: "Attempt to browse to a Sophos update address". The browser window shows an error message: "This site can't be reached. The connection was reset. Try: Checking the connection, Checking the proxy and the firewall, Running Windows Network Diagnostics. ERR\_CONNECTION\_RESET".

In the tools menu of the Endpoint Self Help tool, test the network connections.

While both the ping and domain name tests will help indicate potential network-related issues, a successful HTTPS response test is required for each communication channel to work.

In this scenario, as the HTTPS response is failing, this indicates a communication issue. If you try to access one of the Sophos Update addresses used for updating the return error page indicates that the proxy or firewall is blocking the connection.

## Scenario Three



The screenshot shows the Sophos Firewall's 'Rules and policies' section. On the left, a sidebar lists various protection and configuration options. The main area displays a table of firewall rules. A green callout box highlights rule #5, which is a 'Block' rule for traffic to WAN. The callout text states: 'A firewall rule is configured to block all traffic'. Rule #5 is highlighted with an orange border. Other rules listed include 'Traffic to DMZ', 'Auto added firewall...', '#Default\_Network\_P...', and 'Drop all'. The table columns include Rule type, Source zone, Destination zone, Status, Rule ID, Action, and Feature and service.

Rule type	Source zone	Destination zone	Status	Rule ID	Action	Feature and service
Traffic to WAN	in 0 B, out 0 B			5	Block	IPS AV WEB APP QoS HB LinkedNAT PRX LOG
Traffic to DMZ	in 0 B, out 0 B			7	Auto added firewall...	IPS AV WEB APP QoS HB LinkedNAT PRX LOG
#Default_Network_P...	LAN, Any host	WAN, Any host		8	Accept	IPS AV WEB APP QoS HB LinkedNAT PRX LOG
Drop all	Any zone, Any host	Any zone, Any host		9	Drop	IPS AV WEB APP QoS HB LinkedNAT PRX LOG

A Sophos Firewall is being used in this scenario. So we check the firewall rules being used on the Sophos Firewall.

A firewall rule that is configured to drop traffic from all sources to all destinations is turned on. Because this rule is positioned above the default firewall rule that allows communication to Sophos servers, the drop rule is being applied.

To resolve this issue, the block firewall rule would be removed or modified to not include the Sophos server addresses.

Please note in this scenario, we used a Sophos Firewall to demonstrate how firewall configuration can affect management and update communication to Sophos Central. Similar troubleshooting steps apply to other firewalls.

## Scenario Three

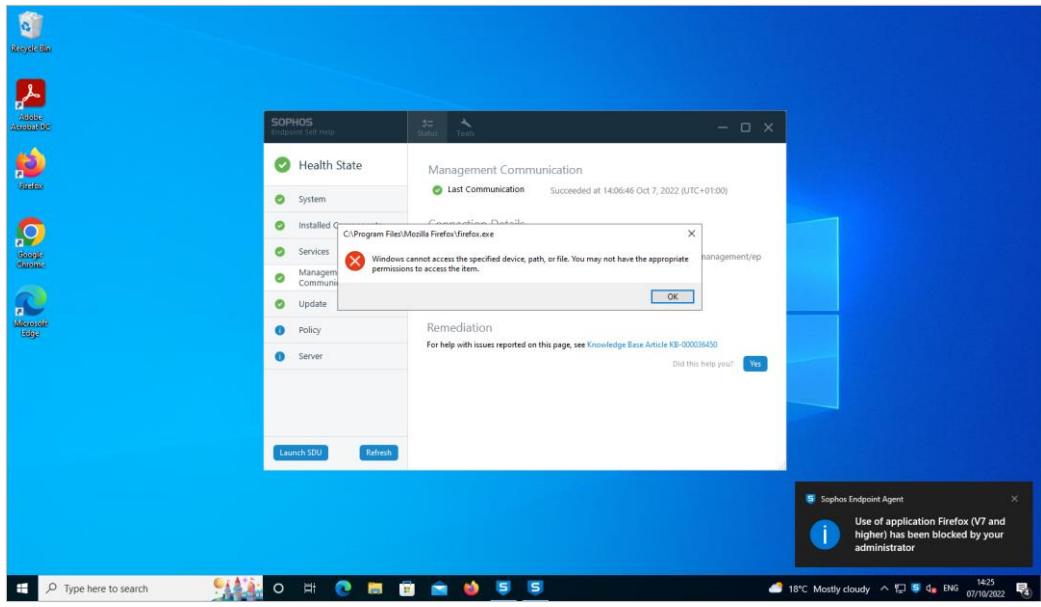
3

The screenshot shows the Sophos Endpoint Self Help interface. The top navigation bar includes links for Status, Events, and Detections. On the left, there's a sidebar with sections for Update Status (last update: 07 October 2022 14:23), Products (Core Agent 2022.2.2.1, Sophos Intercept X 2022.1.1.22), and Troubleshooting (Open Endpoint Self Help Tool, Community forum). The main content area has tabs for Status and Tools. Under Status, the Network Test section shows results for Updating, Management Communication, and Sophos Extensible List (SXL) lookups, all marked as successful (green checkmarks). A 'Run' button is available to re-run the test. Below the test results is a Remediation section with a link to a Knowledge Base Article. A 'Did this help you?' poll is present. At the bottom right is a 'Launch SDU' button.

Now that the firewall rule that was dropping traffic to Sophos update and communication servers has been modified or removed, the network test page shows that there are no network errors.

The Sophos Endpoint Agent is showing that the agent has been updated successfully.

## Scenario Three



The application control policy that blocks the use of FireFox is now applied to the device.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

Which log file contains the Management Communication server address details?

update.txt

config.xml

MCSClient.txt

MCSAgent.txt

SOPHOS

## Question 2 of 2

Type the Windows command used to test connectivity to a specific address.

\_\_\_\_\_

# Chapter Review

Protected devices communicate **management traffic using MCS** and communicate **updating traffic using Sophos AutoUpdate**.

Communication issues between Sophos Central and protected devices will often affect both updating and management. **Troubleshooting these components is similar.**

The **Network Test** tool provides a method to **check specific communication channels** directly to Sophos.

SOPHOS

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

Protected devices communicate management traffic using MCS and communicate updating traffic using Sophos AutoUpdate.

Communication issues between Sophos Central and protected devices will often affect both updating and management, therefore, the troubleshooting of these two components is similar.

The Network Test tool provides a method to check specific communication channels directly to Sophos.



# Advanced Sophos Central Policies and Exclusions

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE3550: Advanced Sophos Central Policies and 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.

# Advanced Sophos Central Policies and Exclusions

In this chapter you will learn the best practice configuration for Sophos Central policies including examples of how to modify policies without reducing security.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Creating new Sophos Central policies
- ✓ Cloning Sophos Central policies
- ✓ Accessing Sophos Central and how to manage protected devices

DURATION     **16 minutes**

SOPHOS

In this chapter you will learn the best practice configuration for Sophos Central policies including examples of how to modify policies without reducing security.

# Sophos Central Threat Protection Policy Configuration

Scheduled Scanning

Enable scheduled scan

02 : 00 AM

Sun Mon Tue Wed Thu Fri Sat

Enable deep scanning - scans inside archive files (.zip, .cab, etc.)

Scheduled Scanning

Enable scheduled scan

02 : 00 AM

Sun Mon Tue Wed Thu Fri Sat

Enable deep scanning - scans inside archive files (.zip, .cab, etc.)

Deep scanning is not automatically enabled for scheduled scans

When enabled, deep scanning scans archives and other compressed files which can increase the scan time

SOPHOS

The threat protection policy can be used to configure a scanning schedule to allow for regular scanning of protected devices.

Scheduled scanning plays an important role in detecting malware that is hidden in files that are not commonly accessed. On-access scanning will scan files that are regularly used. Due to the nature of archived files, they are not scanned regularly. This means that malicious content could be hidden in archived files which can later be used by an attacker.

By default, scheduled scanning does not include deep scanning. When enabled, deep scanning will scan archives and other compressed files. It is worth noting that when this option is enabled, a scan can take significantly longer to complete. Scheduled scanning follows the settings configured in the threat protection policy. This includes both policy and global exceptions.

# Sophos Central Threat Protection Policy Configuration

Because computers' are protected by Sophos' threat protection features and it is unlikely they will have many archived files we do not recommend enabling scheduled scans for endpoints.

## Computers

- Schedule on a weekly basis
- Deep scanning not enabled
- Schedule outside of business hours

## Servers

- Schedule on a weekly basis
- Enable deep scanning
- Schedule around server activities

SOPHOS

For computers', our recommendation is not to enable scheduled scanning as the threat protection features provided by Sophos Central Endpoint Protection and XDR will detect most threats. If you decide to enable a scheduled scan, we recommend that it is configured on a weekly basis and completed outside of business hours so that any business operations are not affected.

For servers, depending on the role of the server, a weekly scheduled scan is recommended. We also recommend enabling deep scanning. This is because file servers are more likely to have archives that are rarely scanned by on-access or threat protection features. To ensure archives have not been compromised, a regular scheduled scan is important. An administrator should consider the activities that run on servers such as backups, updates, or other processes that could be disrupted by a scan when they are configuring the schedule.

# Sophos Central Threat Protection Policy Configuration

- Append a custom message to notification pop-ups
- Message is limited to 100 characters

Consider including:

- Who to contact regarding the notification
- How to contact the correct team or person

### Desktop Messaging

Enable Desktop Messaging for Threat Protection

Configure a message to be added to the end of the standard notification

Contact [ithelp@sophotraining.xyz](mailto:ithelp@sophotraining.xyz)  
[View the IT home page for further details](#)

Note: Custom messages will not be displayed for CryptoGuard events.

SOPHOS

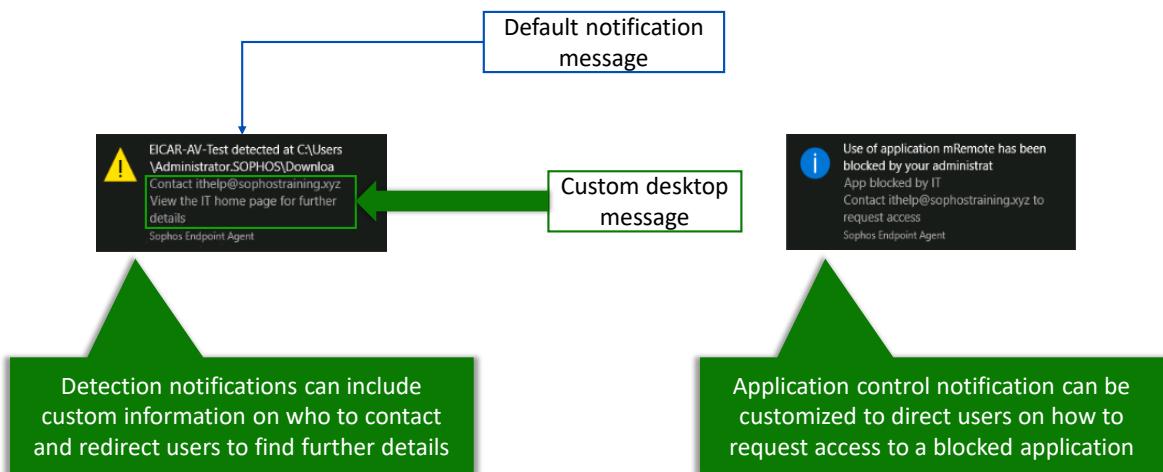
The desktop messaging feature that is included in Sophos Central policies allows you to append a custom message to notification messages shown on protected devices.

A desktop message is limited to 100 characters, so any message should be concise and easy to read. Setting up a well thought out custom message can assist in troubleshooting detections and redirecting users to useful information.

Our recommendation is to include the following information:

- Who to contact regarding the notification
- How to contact the correct team or person

# Sophos Central Threat Protection Policy Configuration



SOPHOS

When a policy rule is triggered, a notification message is displayed to users. Why the notification has been triggered is included by default, and any custom message is displayed after that.

In this example, a detection has been triggered, the user is asked to contact the IT team and to view the home page for more details. As another example, an application has been blocked due to the policy. The custom message advises users to contact the IT team to request access if required.

# Sophos Central Threat Protection Policy Configuration

Users can change the time period of notifications on screen

Windows Server 2019 : Windows > Settings > Ease of access > Other Options > Show notifications for this amount of time

Windows 11: Windows > Settings > Accessibility > Visual effects > Dismiss notifications after this amount of time

Users should be educated to:

- Read all notifications from Sophos Central Agent
- Record any activities that were happening prior to the notification
- Perform follow-up actions if a detection is not cleaned up automatically

SOPHOS

Most users are familiar with popup notifications but often do not pay attention to them. You can change the time period the notification is shown on screen to allow users more time to read the message. We recommend that users are educated to:

- Read all notifications
- Record what activities were happening prior to the notification
  - For example, which applications were open, what websites were being visited. Files that were downloaded and/or opened. Any pop-ups before the incident, and any removable media being used
- Perform follow-up actions if a detection is not cleaned up automatically

# Sophos Central Threat Protection Policy

Why create new policies?

To test new features for a sub-set of users or devices

To perform troubleshooting or testing for a specific user or device

To apply different security settings to different user or device groups

SOPHOS

Base policies are typically the only policies most Sophos Central accounts use to secure their organization. Whilst Sophos recommends the use of the pre-configured base policies, there may be circumstances that new policies are required.

For example, as the base policy is automatically applied to all users and devices, you may want to test a new security feature for a subset of users or perform troubleshooting on a specific device. A new policy could also be required to apply different security settings to different user, or device groups based on that user or groups business requirements.

# Policy Considerations



Take a moment to consider how to test new features, troubleshooting issues or apply different security settings for specific users or devices without reducing the security for an organization.

SOPHOS

Let's take a moment to consider how to test new features, troubleshoot issues, or apply different security settings for specific users or devices without reducing the security for an organization.

# Policy Considerations

New feature testing

- Clone the base policy
- Enable the new feature in the policy
- Apply the policy to the specific user/user group/device

Perform troubleshooting

- Create a new policy
- Modify the policy as required
- Apply the policy to the specific user or device that requires troubleshooting

Apply different security settings

- Create a new policy or clone a base policy
- Modify the policy to meet the required security settings
- Apply the policy to the specific user or device group the settings should apply to

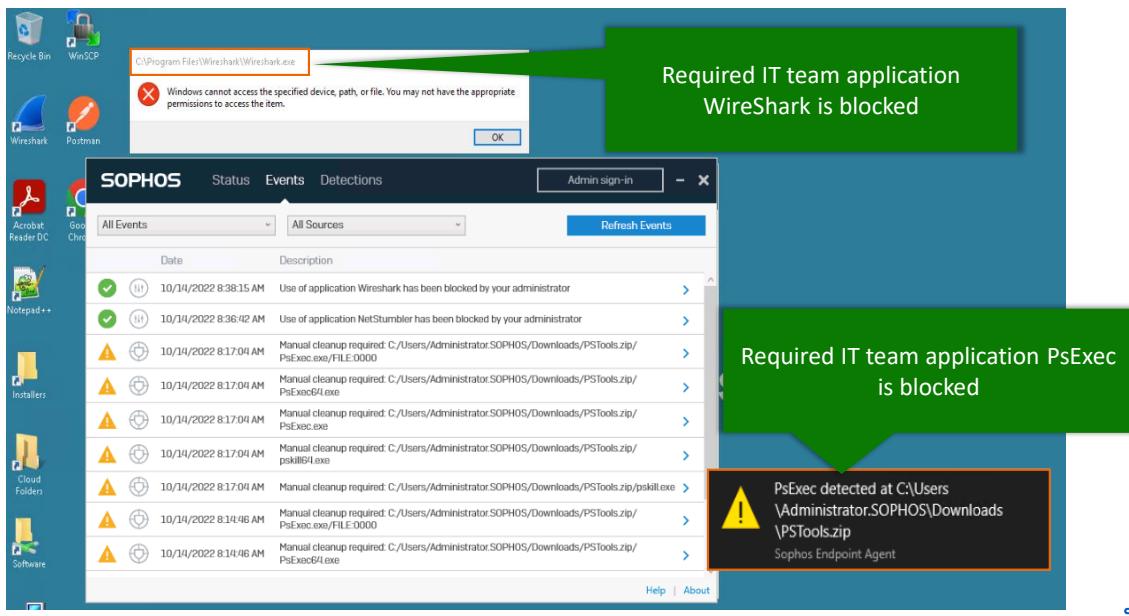
SOPHOS

There are many ways to apply different settings to different users and devices using Sophos Central. The most important factor to consider is that if you modify a base policy, the settings you apply will apply to **ALL** users and devices. This could severely reduce security because attackers can exploit vulnerable applications and system tools to move through a network. Even if a user is not using a specific application or tool, that application or tool can still be exploited by an attacker.

To protect security, we recommend that any required changes to security settings are applied by either cloning a base policy or creating a new policy. Apply any policy changes to the new or cloned policy and then assign that policy to the specific user, user group, device, or device group as required.

This approach allows administrators to provide unique security settings where required whilst maintaining the overall security of an organization. Any new security settings are only applied to specific users or devices and not the entire network.

# Apply Different Security Settings



Let's look at a specific scenario.

An IT team need to use tools that are required to perform day-to-day tasks. The current Sophos Central base policies are blocking access to the required tools for all users and devices in the organization.

In this example, there are two required IT applications that are being restricted. These are Wireshark, a packet capture tool and PsExec which is a telnet tool that allows an administrator to execute processes. These tools are controlled as they pose a potential security risk; however, an IT team also has legitimate reasons to use these tools in certain circumstances.

# Apply Different Security Settings

Modifying the base policies will change the security settings for **ALL** users which will reduce the security of the organization

**Endpoint Protection - Policies**  
Overview / Endpoint Protection Dashboard / Policies

Search  🔍

**Note:** The policies at the top of the list override the policies at the bottom of the list.

Name	Status	Type (single / group)	Last modified
Base Policy - Threat Protection	✓ Enforced		Oct 14, 2022

Name	Status	Type (single / group)	Last modified
Base Policy - Peripheral Control	✓ Enforced		Oct 14, 2022

Name	Status	Type (single / group)	Last modified
Base Policy - Application Control	✓ Enforced		Oct 14, 2022

The base policies in place are for threat protection and application control. There are no exclusions included in the threat protection policy and the 'Use recommended settings' option is selected. The application control policy has been configured to block vulnerable and unproductive applications that the organization does not want its employees to have access to.

The current base policies provide secure protection; however, these policies are preventing the IT team from accessing the tools they require. Adding exceptions to the threat protection base policy or adding the required applications to the application control base policy will allow the application tools for **ALL** users and not just the IT Team.

# Apply Different Security Settings

The screenshot shows the Sophos Endpoint Protection interface for viewing a computer policy. The left sidebar has 'Endpoint Protection' selected under 'CONFIGURE'. The main area is titled 'Endpoint Protection - View Computer Policy' for 'Allow IT Team Tools - Wireshark'. It shows '1 GROUPS' assigned, which is highlighted in blue. A green callout box points to this section with the text: 'Apply the cloned policy to the specific user group'.

POLICY NAME • Allow IT Team Tools - Wireshark

POLICY TYPE Application Control : User

Last Updated Sep 30, 2022

0 USERS 1 GROUPS SETTINGS POLICY BYPASSED

Manage which groups this policy applies to

Available User Groups

IT	X
<input type="checkbox"/> AVAILABLE USER GROUPS	2
<input type="checkbox"/> IT	
<input type="checkbox"/> IT Admin	

Assigned User Groups

Search	X
<input type="checkbox"/> ASSIGNED USER GROUPS	
<input type="checkbox"/> IT Team	

Known applications can be allowed using an application control policy. This has an advantage as you can track the use of the application that you allow.

Clone the application control base policy and modify it so that it applies to any user in the IT team group no matter which device they log into.

# Apply Different Security Settings

The screenshot shows the Sophos Central Endpoint Protection interface for viewing a computer policy. The left sidebar has 'Endpoint Protection' selected under 'CONFIGURE'. The main area is titled 'Endpoint Protection - View Computer Policy' with the sub-titles 'Overview / Computer Policies / View Computer Policy'. The policy name is 'Allow IT Team Tools - Wireshark'. The policy type is 'Application Control : User'. There are buttons for 'Save', 'Cancel', 'Delete', and 'Clone'. The status bar shows 'Last Updated Sep 30, 2022' and user information 'Simon Smith - Sophos UK - Super Admin'. Below the title, it says 'POLICY NAME \* Allow IT Team Tools - Wireshark' and 'POLICY TYPE Application Control : User'. It shows '0 USERS', '1 GROUPS', and a 'SETTINGS' button. A note says 'Policy is bypassed - all settings in this policy will be ignored. Settings will come from another policy.' Below this, it says 'Select applications you want to control and specify detection options' and has a 'Add/Edit List' button. A table shows 'CONTROLLED APPLICATIONS' with 'Network monitoring / Vulnerability tool' expanded to show '- Wireshark'. A green callout box over this table says 'Add the application you want to allow'. Under 'Detection Options', there are three toggle switches: 'Detect controlled applications when users access them (You will be notified)' (on), 'Allow the detected application' (selected), 'Block the detected application' (off), and 'Detect controlled applications during scheduled and on-demand scans' (on). A note at the bottom says 'You can request applications to be added by Sophos' and 'Application Control Request'.

Configure the cloned policy to allow the required application. In our example, the policy is configured to allow the Wireshark application.

# Apply Different Security Settings

The screenshot shows the Sophos Central interface for managing computer policies. On the left, a dark sidebar lists 'ANALYZE' (Dashboard, Logs & Reports), 'MANAGE PROTECTION' (People, Computers), 'CONFIGURE' (Policies, Settings, Protect Devices), and 'MORE PRODUCTS' (Free Trials). The 'Policies' option is highlighted with a blue bar. The main content area is titled 'Endpoint Protection - View Computer Policy' and shows a policy named 'Allow IT Team Tools - WireShark'. The policy type is 'Application Control : User'. It indicates 0 users, 1 group, and settings. A prominent button labeled 'POLICY BYPASSED' is highlighted in blue. Below it, a switch is set to 'Policy is bypassed', with a note explaining that settings won't be applied to assigned targets. A green call-to-action button at the bottom right says 'Enforce the policy'.

Don't forget to enforce the policy as cloned policies are not enforced by default.

# Apply Different Security Settings

The screenshot shows the Sophos Central interface for managing policies. On the left, a sidebar lists 'ANALYZE' (Dashboard, Logs & Reports), 'MANAGE PROTECTION' (People, Computers), 'CONFIGURE' (Policies, Settings, Protect Devices), and 'MORE PRODUCTS' (Free Trials). The 'Policies' option is selected and highlighted in blue.

The main content area displays several policy lists:

- Peripheral Control (4)**:

Name	Status	Type (single / group)	Last modified
IT Group Exceptions	Bypassed	User (0 / 2)	Oct 4, 2022
IT Workstation Exceptions	Enforced	Computer (0 / 1)	Oct 4, 2022
Base Policy - Threat Protection	Enforced		Aug 26, 2022
- Application Control (2)**:

Name	Status	Type (single / group)	Last modified
Allow IT Team Tools - Wireshark	Enforced	User (0 / 1)	Oct 17, 2022
Base Policy - Application Control	Enforced		Sep 30, 2022
- Data Loss Prevention (1)**:

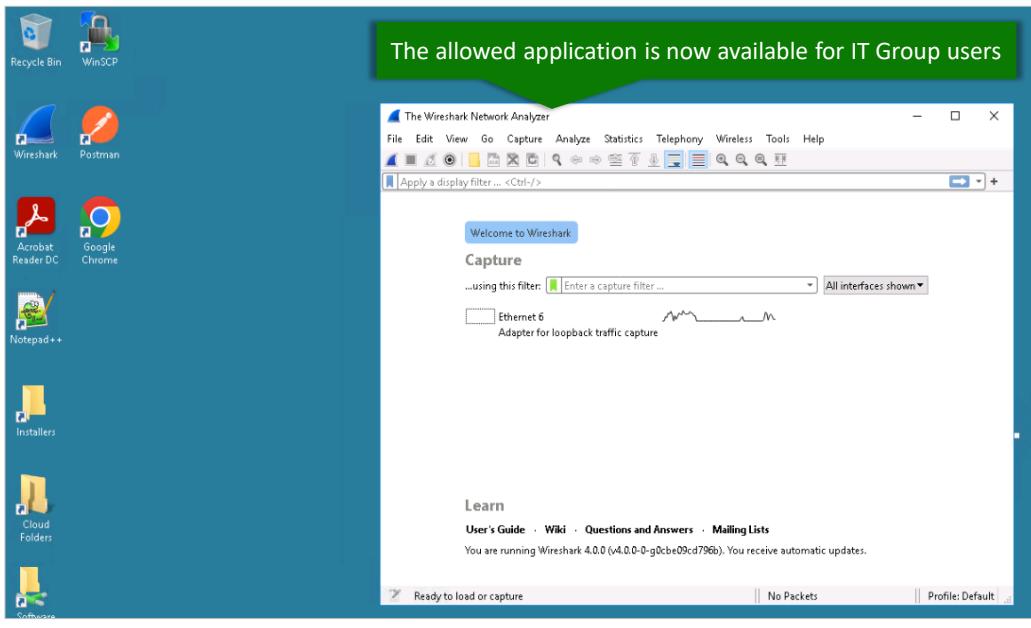
Name	Status	Type (single / group)	Last modified
Base Policy - Data Loss Prevention	Enforced		Aug 31, 2022
- Web Control (5)**:

Name	Status	Type (single / group)	Last modified

A large green callout bubble points from the text 'The new policy is listed above the base policy' to the 'Allow IT Team Tools - Wireshark' row in the Application Control list.

The policy is automatically placed above the base policy.

# Apply Different Security Settings



SOPHOS

Once the policy has been applied, the Wireshark application is allowed.

# Apply Different Security Settings

The screenshot shows the Sophos Central interface for creating a new computer policy. The left sidebar has 'Endpoint Protection' selected under 'Policies'. The main window title is 'Endpoint Protection - View Computer Policy' with the sub-path 'Computer Policies / View Computer Policy'. The policy name is 'IT Group Exceptions' and the type is 'Threat Protection : User'. A green callout box points to the 'GROUPS' tab which is selected, stating: 'A user policy is created so that the policy applies to the user regardless of the device they log into'. Below this, it says 'Manage which groups this policy applies to'. On the left, under 'Available User Groups', there is a list of 42 groups including Admin Staff (SOPHOS), Allowed RODC Password Re..., Cert Publishers (SOPHOSTR...), Cloneable Domain Controle..., Contractors (SOPHOS), Denied RODC Password Re..., DnsAdmins (SOPHOSTRAINL...), DnsUpdateProxy (SOPHOST...), and Domain Admins (SOPHOST...). On the right, under 'Assigned User Groups', there is a list with one item: 'IT Team'. A green callout box points to this list stating: 'The policy will only apply to the users in the IT Team group'.

There are some cases where an exclusion needs to be applied in a threat protection policy. This applies to potentially unwanted applications as they are detected using the threat protection features, not application control.

To create a new threat protection policy, either clone the base policy or create a new policy. In this example, the threat protection policy is cloned to ensure the security settings are used in the new policy.

The policy is created as a user policy and the IT Team group is assigned to the policy.

# Apply Different Security Settings

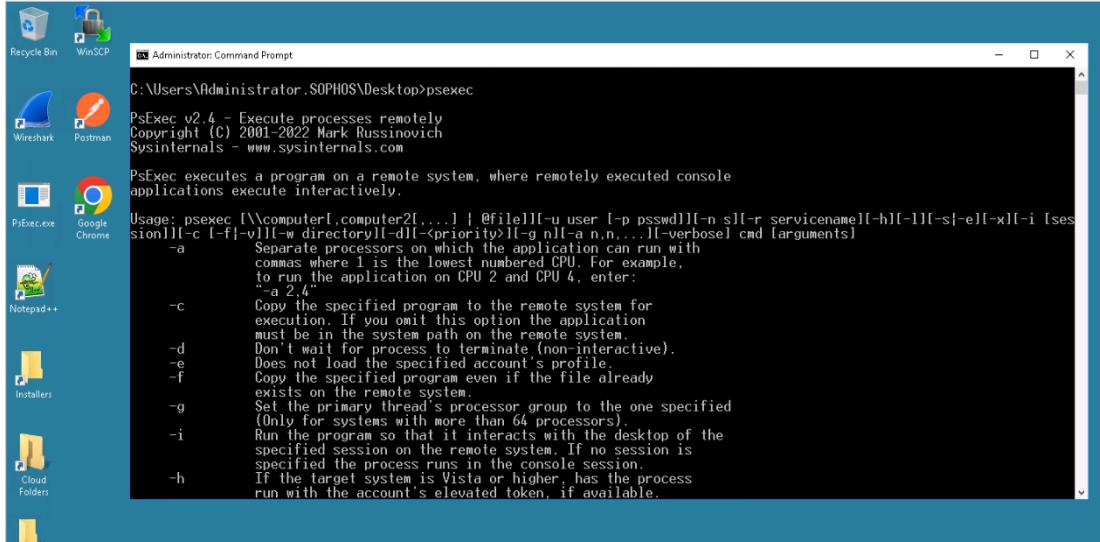
The screenshot shows the Sophos Central interface for Endpoint Protection. On the left sidebar, under 'CONFIGURE', 'Policies' is selected. In the main content area, the 'Scheduled Scanning' tab is active. A modal window titled 'Add Exclusion' is open, showing the 'EXCLUSION TYPE' as 'Potentially Unwanted Application (Windows/Mac)' and the 'VALUE' as 'PsExec'. A warning message states: '⚠ This exclusion is a significant security risk'. Below the modal, the 'Policy Exclusions' section shows a table with one row: 'EXCLUDE' (containing 'PsExec') and 'ACTIVE FOR' (empty). A note at the bottom of the page says: 'We do NOT recommend adding this exclusion example in any production environment. This is for demonstration purposes only.'

The required exclusion is added to the policy exclusions list on the **SETTINGS** tab. Exclusions should be as specific as possible especially when used in a threat protection policy. This is because any excluded items are not scanned for malware.

In this example a PUA that is considered extremely vulnerable is being added as an exception. Sophos Central highlights the security risk of adding an exclusion like this.

**We do not recommend that you add this exclusion example in any production environment, this is for demonstration purposes only.**

# Apply Different Security Settings



SOPHOS

Once the policy has been applied, an IT Team user can access the tool as required.

# Policy Precedence

A screenshot of the Sophos Central interface, specifically the Endpoint Protection - Policies page. The top navigation bar includes 'Overview', 'Endpoint Protection Dashboard', and 'Policies'. Below the navigation is a search bar with a magnifying glass icon. A callout bubble in the top right corner states 'Policies are applied in the order they are displayed'. At the bottom of the page, there is a note in a box: 'Note: The policies at the top of the list override the policies at the bottom of the list.' The left sidebar shows 'SOPHOS' at the top, followed by 'Endpoint Protection' and 'ANALYZE'.

It is important to remember when working with policies, they are processed top down. Which policies are applied will depend on the users and devices assigned to each policy.

This is noted at the top of both the Endpoint and Server policies page as shown here.

SOPHOS

# Policy Precedence

The screenshot shows the Sophos Endpoint Protection - Policies page. On the left, a sidebar menu for 'Endpoint Protection' includes 'All users' under 'Manage Protection'. A blue box highlights 'All users'. A green box highlights 'IT Team user group'. Arrows point from 'All users' to the 'IT Group Exceptions' and 'Allow IT Team Tools - Wireshark' policies, and from 'IT Team user group' to 'Base Policy - Threat Protection' and 'Base Policy - Application Control'. The main table lists policies categorized by section: Threat Protection (2), Peripheral Control (1), Application Control (2), and Data Loss Prevention (1). The 'IT Group Exceptions' and 'Allow IT Team Tools - Wireshark' policies are highlighted with green boxes and arrows pointing to them from the user groups.

Name	Status	Type (single / group)	Last modified
IT Group Exceptions	✓ Enforced	User (0 / 1)	Oct 17, 2022
Base Policy - Threat Protection	✓ Enforced		Aug 26, 2022
Base Policy - Peripheral Control	✓ Enforced		Sep 1, 2022
Allow IT Team Tools - Wireshark	✓ Enforced	User (0 / 1)	Oct 17, 2022
Base Policy - Application Control	✓ Enforced		Sep 30, 2022

Looking at our example, the new policies in the threat protection and the application control sections are listed above the base policies. Creating new policies and assigning the policy only to specific users where the exceptions are appropriate, minimizes the security risk to an organization.

When a user that is assigned to the IT Team user group logs onto a protected device, the policies assigned to the IT Team user group are applied first because they are first in the policy list, and they match the user group applied.

If a user that is assigned to another user group logs onto a protected device, the first available policy will be applied. In this example, the base policy is applied because the user group membership does not match the first policy listed.

## Testing New Features

New features are periodically introduced by Sophos to the Threat Protection base policy

New features should be tested before being applied to **ALL** users and devices

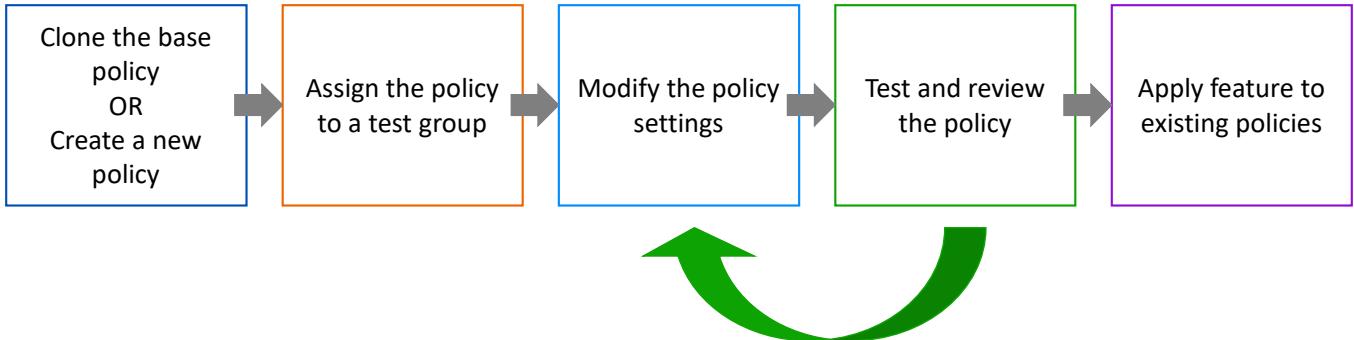
Create a new policy to test new features with a small number of users or devices assigned to the policy

SOPHOS

Sophos periodically introduces new features to the threat protection policy that are not enabled by default. We recommend that new features are tested before they are applied to all users and devices to ensure they do not interfere with normal business operations.

Creating new policies is a way of testing new features prior to applying them to all users and devices. This means that if the feature does impact business operations, only a few users and devices are affected. Any loss in productivity is limited.

# Test New Features



SOPHOS

We recommend the following process when testing new security features introduced to the threat protection policy.

1. Either clone the threat protection base policy or create a new threat protection policy
2. Assign the new policy to a representative group of testers that have been identified. Alternatively, you may have a dedicated test environment with devices and users that is used for testing
3. Modify the policy settings. Enable the new features and save the policy
4. Test and review the policy. Once the policy is applied, you can evaluate that the new security feature does not interfere with day-to-day business tasks
5. Apply to existing policies. If the new setting causes any issues, bypass the policy while you adjust the settings or research exceptions or changes that may need to be implemented

# Troubleshooting Policies

## Issue

- An administrator is under pressure to resolve an issue quickly
- They do not always follow policy configuration best practice
- They trade security for quick solutions

## Example Scenario

- A user needs to download an application that is blocked
- User requires the application urgently
- An administrator wants to make the change as quickly as possible to negate negative feedback

SOPHOS

Should an administrator be in a rush or under pressure to resolve an issue, they may not always follow the best practice for policy configuration. Trading secure solutions for quick resolutions, for example, applying a risky exclusion to a base policy which results in a less secure policy that applies to more users and devices than required.

Let's look at an example. A user needs to download an application that is currently blocked by a Sophos Central policy. They contact the IT team to request the application is allowed as they have a client meeting scheduled in half an hour. The application is required for this meeting. The sense of urgency may cause an administrator to add an application exclusion quickly to negate negative feedback.

# Troubleshooting Policies

## BEST PRACTICE

1. Investigate the legitimacy of the application
2. Determine the effect of excluding the application
3. Clone or create a policy
4. Assign the policy to an identified user/device group
5. Modify the policy settings
6. Save the policy

## QUICK FIX

1. Clone the base policy
2. Assign the policy to the specific user reporting the issue
3. Modify the policy to exclude the application
4. Save the policy

Follow-up any quick fixes with a full investigation and apply secure policies

SOPHOS

Our recommendation in this scenario would be to:

- Investigate the legitimacy of the application to determine what effect adding an exclusion for the application will have
- To identify which user or user groups require the use of the application
- Clone or create a policy and apply it to the appropriate user or user group
- Modify the settings to exclude the application
- Save the policy

Due to the time constraints of this issue, investigating the legitimacy of the application and the effect of exclusion would not be the ideal solution for the user. As a secure quick fix to this issue, an administrator could:

- Clone the base policy
- Assign the policy to the specific user reporting the issue
- Modify the policy to exclude the application
- Save the policy

Following the quick fix, an administrator can investigate the application legitimacy and use case for the application. This approach limits the danger of an unsafe application exclusion whilst allowing a user to complete business tasks. Once the investigation is complete policy changes can be made using the best practice to ensure organization security.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

**True or False:** When scheduled scanning is enabled the default configuration will scan inside archives.

True

False

SOPHOS

## Question 2 of 2

Jane is a member of the user group 'IT Group'. Jane's device is in the 'IT Workstation' device group.  
Which threat protection policy applies to Jane's device?

Threat Protection (3)			
	Name	Status	Type (single / group)
+	IT Group Exceptions	Bypassed	User (0 / 2)
+	IT Workstation Exceptions	✓ Enforced	Computer (0 / 1)
	Base Policy - Threat Protection	✓ Enforced	

IT Group Exceptions

IT Workstation Exceptions

Base Policy

# Chapter Review

By default, **scheduled scanning** does not include deep scanning. When enabled, **deep scanning will scan archives** and other compressed files.

Sophos Central **policies are processed top down**. Which policies are applied will depend on the users and devices assigned to each policy. Base policies are always assigned last and cannot be deleted.

We recommend that **new features are tested before they are applied to all users and devices** to ensure they do not interfere with normal business operations.

SOPHOS

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

By default, scheduled scanning does not include deep scanning. When enabled, deep scanning will scan archives and other compressed files.

Sophos Central policies are processed top down. Which policies are applied will depend on the users and devices assigned to each policy. Base policies are always assigned last and cannot be deleted.

We recommend that new features are tested before they are applied to all users and devices to ensure they do not interfere with normal business operations.



# Getting Started with Sophos Central Partner Global Templates

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE3555: Getting Started with Sophos Central Partner Global Templates

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 Partner Global Templates

In this chapter you will learn how to configure Sophos Central Partner Dashboard global templates.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access the Sophos Central Partner Dashboard
- ✓ Onboarding customers and managing them from the Sophos Central Partner Dashboard
- ✓ Configuration of Sophos Central global settings and policies

DURATION      **17 minutes**

SOPHOS

In this chapter you will learn how to configure Sophos Central Partner Dashboard global templates.

# Sophos Central Partner Dashboard

The screenshot shows the Sophos Central Partner Dashboard. On the left, a sidebar menu includes 'Dashboard' (selected), 'Alerts', 'Logs', 'Customers', 'Licenses', 'Managed Customer Usage', 'Trial Licenses', 'Deployments', 'Manage Groups', 'Licensing & Billing', 'Settings & Policies' (highlighted with a green box and a red arrow pointing to it), 'Marketing & Training', 'Pricing', and 'Global Security News'. The main dashboard area has sections for 'Alerts' (High Alerts: 2, Medium Alerts: 2, Info Alerts: 1, PSA Sync Alerts: 0), 'Usage For My Monthly Customers' (with a large green bar indicating usage across various categories like Server P..., Intercept..., Intercept..., Mobile C..., Mobile C..., Sophos I..., Web, Phish Th..., Central F..., Extended...), 'Sophos Central - Central' (License Management: Near Expiration: 0, Expired: 2, Over Limit: 0, Trials: 12), and 'Sophos Central - Firewalls' (License Management: Near Expiration: 0, Expired: 2). A green callout box highlights the 'Create and apply global templates' text.

Often Sophos partners manage multiple Sophos Central accounts. Multi-service providers, resellers, and Sophos partners can all make use of the Sophos Central Partner Dashboard to manage customer accounts from one place. Only Sophos partners, MSPs, and resellers will have access to the Central Partner Dashboard.

The Sophos Central Partner Dashboard includes the feature to create global templates. This means that a partner can create templates and apply them to individual or multiple customers at the same time. These templates can be used to configure base policies and global settings for managed customers.

# Global Templates

The screenshot shows the Sophos Central Partner Dashboard. The left sidebar contains navigation links for MY CUSTOMERS, SOPHOS CENTRAL, and MY BUSINESS. The main content area is titled "Settings & Policies" and includes sections for "Partner account settings", "Global customer settings", and "APIs & Integrations". A specific section, "Global templates", is highlighted with a red box. The top right corner shows the user's name, Ed Korsgaard, and the team, Global MSP Team (Private) - Partner Super Admin.

To get started with global templates, in the Sophos Central Partner Dashboard, navigate to **CONFIGURE > Settings & Policies** and select **Global templates**.

# Global Templates

- Apply policies and global settings to managed customer
- Push templates to assigned customer accounts
- Global template settings overwrite existing base policy and global settings in a customer Sophos Central account

The screenshot shows the Sophos Central Partner Dashboard with the 'Global Templates' page open. The left sidebar includes links for Dashboard, Alerts, Logs, Customers, Licenses, Managed Customer Usage, Trial Licenses, Deployment, Manage Groups, and Licensing & Billing. The 'Settings & Policies' link is highlighted. The main content area has a header 'Global Templates' with a 'Create common global settings and base-policy template sets to use across different customers.' link and a 'More Info' button. Below is a table with columns: Name, Description, # Customers, Last push, and Push status. The table lists several templates:

Name	Description	# Customers	Last push	Push status
Alvin's template		2	Jan 23, 2022, 5:52:37 PM	✓
Cameron's Template		0		
Cosmos-Team	Cosmos-Team	1	Oct 14, 2022, 2:37:24 AM	✓
Default Customer Te...	This is the standard templ...	2		⚠ Push
Ed's Training Exampl...	Used for demonstrating gl...	0		
Kyle's Template		1	Apr 12, 2022, 6:30:01 PM	✓
MSP/CSP Default Te...	Do not make any changes t...	2	Oct 4, 2022, 10:17:42 AM	⚠ Push

Global templates allow you to apply policies and global settings to managed customers. Any template can be modified to your specification and once configured, are pushed out to the assigned customer accounts.

Any global template applied to a customer account from the Sophos Central Partner Dashboard will overwrite any existing base policies and global settings in a customer Sophos Central account.

# Global Templates

The screenshot shows the Sophos Central interface with the 'Global Templates' page selected. The left sidebar includes links for 'Dashboard', 'Alerts', 'Logs', 'Customers', 'Licenses', 'Managed Customer Usage', 'Trial Licenses', 'Deployment', 'Manage Groups', 'Licensing & Billing', and 'Settings & Policies'. The main content area has a header 'Global Templates' with a 'Help' and 'Ed Korsgaard' dropdown. Below the header are buttons for 'Add template' and 'Clone', and a search bar. A note says 'Create common global settings and base-policy template sets to use across different customers. [More info](#)'. A table lists eight templates:

Name	Description	# Customers	Last push	Push status
Alvin's template		2	Jan 23, 2022, 5:52:37 PM	✓
Cameron's Template		0		
Cosmos-Team	Cosmos-Team	1	Oct 14, 2022, 2:37:24 AM	✓
Default Customer Te...	This is the standard templ...	2		<span style="color: orange;">⚠ Push</span>
Ed's Trainning Exampl...	Used for demonstrating gl...	0		
Kyle's Template		1	Apr 12, 2022, 6:30:01 PM	✓
MSP/CSP Default Te...	Do not make any changes t...	2	Oct 4, 2022, 10:17:42 AM	<span style="color: orange;">⚠ Push</span>

The 'Global Templates' view lists all configured templates including the name, description, how many customers the template is assigned to, the last push date and time, and the push status.

# Global Templates

The screenshot shows the Sophos Central interface with the 'Global Templates' page selected. A green callout box points to the search bar at the top right of the main content area, which contains the text: 'Search for templates by name or search for templates assigned to a specific customer'. The search bar itself has a magnifying glass icon and the word 'Search'.

Name	Description	# Customers	Last push	Push status
Alvin's template		2	Jan 23, 2022, 5:52:37 PM	✓
Cameron's Template		0		
Cosmos-Team	Cosmos-Team	1	Oct 14, 2022, 2:37:24 AM	✓
Default Customer Te...	This is the standard templ...	2		⚠ Push
Ed's Trainning Exampl...	Used for demonstrating gl...	0		
Kyle's Template		1	Apr 12, 2022, 6:30:01 PM	✓
MSP/CSP Default Te...	Do not make any changes t...	2	Oct 4, 2022, 10:17:42 AM	⚠ Push

Using the search bar, you can filter the templates by searching for specific template names or you can search for a specific customer.

The list will be filtered to display any templates matching the template name or assigned to the searched for customer.

# Global Templates

The screenshot shows the Sophos Central interface with the 'Global Templates' page selected. The left sidebar includes sections for 'MY CUSTOMERS' (Dashboard, Alerts, Logs), 'SOPHOS CENTRAL' (Customers, Licenses, Managed Customer Usage, Trial Licenses, Deployment), 'SOPHOS CENTRAL - FIREWALLS' (Manage Groups, Licensing & Billing), and 'CONFIGURE' (Settings & Policies). The main content area is titled 'Global Templates' and shows a list of existing templates. A green callout box points to the 'Add template' button at the top left of the list. The table columns are Name, Description, # Customers, Last push, and Push status. The data in the table is as follows:

Name	Description	# Customers	Last push	Push status
Alvin's template		2	Jan 23, 2022, 5:52:37 PM	✓
Cameron's Template		0		
Cosmos-Team	Cosmos-Team	1	Oct 14, 2022, 2:37:24 AM	✓
Default Customer Te...	This is the standard templ...	2		⚠ Push
Ed's Trainning Exampl...	Used for demonstrating gl...	0		
Kyle's Template		1	Apr 12, 2022, 6:30:01 PM	✓
MSP/CSP Default Te...	Do not make any changes t...	2	Oct 4, 2022, 10:17:42 AM	⚠ Push

To create a new template, you can either clone an existing template or create a new template by clicking **Add template**.

# Global Templates - Configuration

The screenshot shows a modal window titled "Add global template". It has a "Template name\*" field containing "Education default", a "Description (Max of 250 characters)" field containing "Default threat protection, web filtering, app control. No peripheral control or DLP. Exclusion for 'appname'", and two buttons at the bottom: "Cancel" and "Save".

The template **name** should indicate:

- Who the template is for i.e., 'Education default' or 'Finance Strict'

The template **description** should indicate:

- Protection features enabled
- Any features not enabled
- Exclusion details
- Special configuration settings

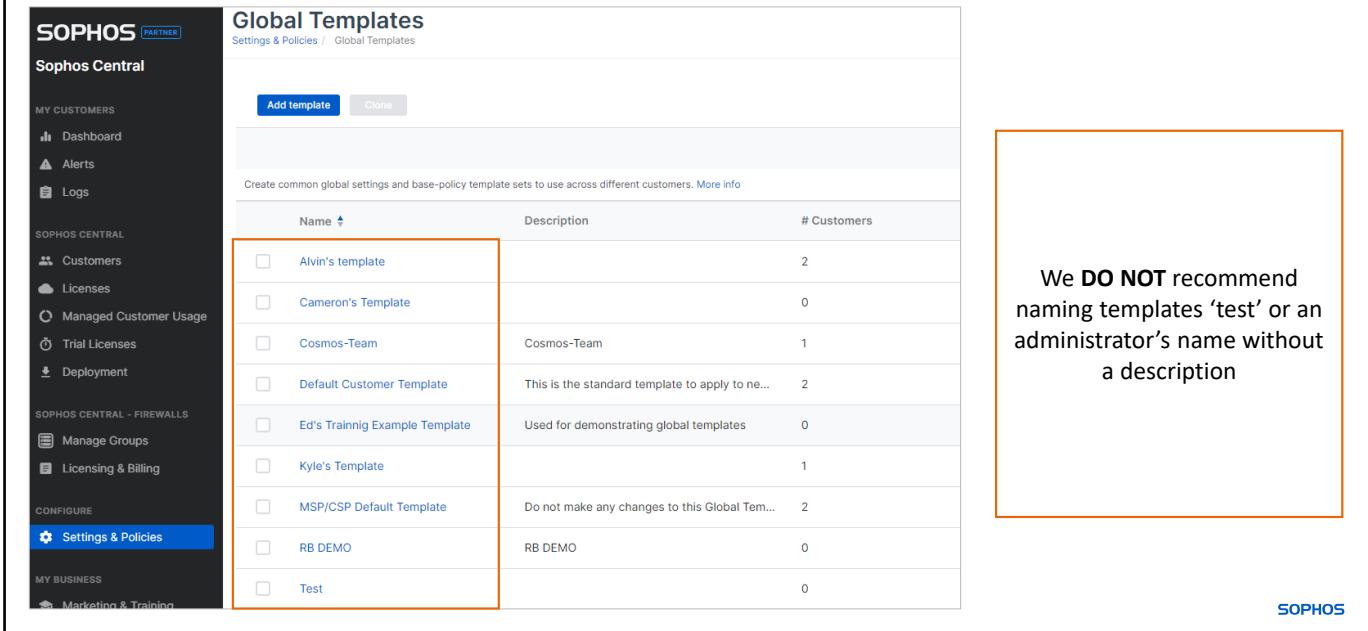
SOPHOS

When creating a new global template, only a name is required, however, the template description is important. Multiple variations of the same template could be created for customers in different industries. It is best to avoid using a customer name in a template name because templates are intended to be applied to groups of customers for efficiency and security. If a customer requires specific exclusions or custom settings, it is recommended to create a new local policy in their Sophos Central account.

Without a meaningful name and description, it can be difficult to determine the purpose of a template. The description field should be used to detail the protection features applied. For example, you can use the description field to detail the protection setting such as the threat protection settings and whether features like web filtering, app control and DLP are enabled or not. Exclusion information can also be included along with any other special configuration settings.

This information is important in the Partner dashboard because multiple administrators may be creating templates. Should a template creator not be available or leave, another administrator should be able to look at a template name and description and know the template intention.

# Global Templates - Configuration



The screenshot shows the Sophos Central interface with the 'Settings & Policies' section selected. The 'Global Templates' page is displayed, showing a list of existing templates. A red box highlights the first few rows of the template list.

Name	Description	# Customers
<input type="checkbox"/> Alvin's template		2
<input type="checkbox"/> Cameron's Template		0
<input type="checkbox"/> Cosmos-Team	Cosmos-Team	1
<input type="checkbox"/> Default Customer Template	This is the standard template to apply to ne...	2
<input type="checkbox"/> Ed's Trainning Example Template	Used for demonstrating global templates	0
<input type="checkbox"/> Kyle's Template		1
<input type="checkbox"/> MSP/CSP Default Template	Do not make any changes to this Global Tem...	2
<input type="checkbox"/> RB DEMO	RB DEMO	0
<input type="checkbox"/> Test		0

We DO NOT recommend naming templates 'test' or an administrator's name without a description

This example lists several templates that have poor names and no descriptions. An administrator who did not create these templates would not be able to determine the template intention and could edit or push an inappropriate template to customers.

# Global Templates - Configuration

ONE global template per customer account

The screenshot shows the Sophos Partner Global Templates - Configuration interface. On the left, there's a sidebar with 'MY CUSTOMERS' (Dashboard, Alerts, Logs), 'SOPHOS CENTRAL' (Customers, Licenses, Managed Customer Usage, Trial Licenses, Deployment), 'SOPHOS CENTRAL - FIREWALLS' (Manage Groups, Licensing & Billing), and 'CONFIGURE' (Settings & Policies). The 'Settings & Policies' tab is selected. In the main area, under 'Default Customer Template' (Settings & Policies / Global Templates / Default Customer Template: Customers), a modal window titled 'Edit customers' is open. The modal has two sections: 'AVAILABLE MANAGED CUSTOMERS' (listing various companies like ABC LTD, CCV-AZDEMO-ENDPOINTS, Bern Inc, etc.) and 'ASSIGNED CUSTOMERS' (empty). A search bar is at the top of each section. At the bottom of the modal are 'Cancel' and 'Save' buttons. An orange arrow points from the 'Edit customers' button in the top right corner of the modal back to the 'Edit customers' button in the main configuration area.

The '**Customers**' tab is used to assign customers to the template. We recommend that you do not assign the template to customers until you have completed the template configuration. This is to avoid another administrator accidentally pushing an unfinished template to customers.

When you have configured the template, return to the 'Customers' tab and click **Edit customers**. A list of all managed customers is displayed. You can select any number of customers from the 'Available Managed Customers' list and move them to the 'Assigned Customers' list. There is also a search box at the top to quickly filter for customers.

It is important to remember that customers can only have one global template assigned to them.



Additional information in  
the notes

# Global Templates - Configuration

The screenshot shows the Sophos Partner dashboard with the 'Settings & Policies' section selected. Under 'Global Templates', the 'Default Customer Template' is selected. The 'Global settings' tab is active, showing a list of global settings with their descriptions and last modified dates. A note at the top right indicates changes have been pushed to customers.

Name	Description	Last modified	Last modified by
Allowed Applications	See items you've allowed.	Sep 27, 2022 23:07:26 PM	Ed Korsgaard
Data Lake Endpoint Upload Settings	Manage uploads to the Data Lake from your computers.	Sep 27, 2022 23:07:49 PM	Ed Korsgaard
Data Lake Server Upload Settings	Manage uploads to the Data Lake from your servers.		
Device Migration	Allow devices to migrate from one Sophos Central account to another.		
Global Exclusions	Manage exclusions for known files, websites, and applications in order to improve performance.	Sep 27, 2022 23:08:10 PM	Ed Korsgaard
SSL/TLS decryption of HTTPS	Control decryption of websites and manage exclusions		
Website Management	Manage, categorize, and tag websites for use with Web Control and Web Gateway features.	Sep 27, 2022 23:08:48 PM	Ed Korsgaard

SOPHOS

The **Global settings** tab displays the settings that can be configured and applied.

Selecting each setting allows you to customize the settings according to your requirements. These settings are the same as the global settings included in a customer Sophos Central account.

When you configure global settings in the Partner dashboard, the settings cannot be modified in any assigned customer Sophos Central accounts.

## [Additional Information]

Configurable global settings:

Allowed applications - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/AllowedApplications/index.html>

Data Lake Endpoint Upload - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/DataLakeEndpoint/index.html>

Data Lake Server Upload - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/DataLakeServer/index.html>

Device migration - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/DeviceMigration/index.html>

SSL/TLS decryption of HTTPS websites - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/DecryptHTTPS/index.html>

Global exclusions - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/ScanningExclusions/index.html>

Website Management - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/GlobalSettings/ConfigureWebsiteList/index.html>

# Global Templates - Configuration

The screenshot shows the Sophos Partner Global Settings interface. The left sidebar includes sections for MY CUSTOMERS (Dashboard, Alerts, Logs), SOPHOS CENTRAL (Customers, Licenses, Managed Customer Usage, Trial Licenses, Deployment), SOPHOS CENTRAL – FIREWALLS (Manage Groups, Licensing & Billing), and CONFIGURE (Settings & Policies, which is selected). The main content area is titled "SSL/TLS decryption of HTTPS" and shows the breadcrumb path: Settings & Policies / Global Templates / Default Customer Template: Global Settings / SSL/TLS decryption of HTTPS. A green callout box highlights the breadcrumb menu with the text: "The breadcrumb menu shows that this is a template global setting". The right side of the page displays configuration options for SSL/TLS decryption, including a note about Threat Protection policies, a list of categories excluded from decryption (Downloads, Finance & Investment, Health & Medicine, Job Search & Career Development, Web-based E-mail), and a "Save" and "Cancel" button. A green callout box on the right states: "Partner dashboard template global settings are the same as customer Sophos Central settings".

Selecting a 'Global Setting' to configure displays the same settings that are available in a customer Sophos Central account.

The breadcrumb menu at the top of the page shows that this is a template.



Additional information in  
the notes

# Global Templates - Configuration

Endpoint Protection applies only to Windows and macOS devices

Name	Last modified	Last modified by
Endpoint Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Peripheral Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Threat Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:19 AM	Ed Korsgaard
Web Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
<b>Windows Firewall</b>		
Server Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Lockdown		
Peripheral Control		
Threat Protection	Oct 18, 2022 1:20 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:20 AM	Ed Korsgaard
Web Control		
Windows Firewall		
Encryption		
Device Encryption	Oct 18, 2022 1:20 AM	Ed Korsgaard
Email Security	Oct 18, 2022 1:20 AM	Ed Korsgaard
Email Security	Oct 18, 2022 1:20 AM	Ed Korsgaard

SOPHOS

The base policies are divided up into four sections. The first section is ‘Endpoint Protection’ which applies only to Windows and macOS devices. You can configure base policies for the sections listed.

## [Additional Information]

Set up base policies for Endpoint Protection.

Endpoint: Peripheral Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureDeviceControl/index.html>

Endpoint: Threat Protection - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureMalwareProtection/index.html>

Endpoint: Update Management - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureUpdatingPolicy/index.html>

Endpoint: Web Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureWebControl/index.html>

Endpoint: Windows Firewall - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureWindowsFirewall/index.html>

Endpoint: Application Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureAppControl/index.html>



Additional information in  
the notes

# Global Templates - Configuration

Customers (0) Global settings Base policies		
Customize base policies to be applied to customers (if you want to). Customers won't be able to change any of the base policies shown here. <a href="#">More info</a>		
Name	Last modified	Last modified by
Endpoint Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Peripheral Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Threat Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:19 AM	Ed Korsgaard
Web Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Windows Firewall		
Server Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Lockdown		
Peripheral Control		
Threat Protection	Oct 18, 2022 1:20 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:20 AM	Ed Korsgaard
Web Control		
Windows Firewall		
Encryption		
Device Encryption	Oct 18, 2022 1:20 AM	Ed Korsgaard
Email Security		
Email Security	Oct 18, 2022 1:20 AM	Ed Korsgaard

Server Protection applies only to Windows and Linux servers

The second section listed is for server protection which applies to Windows and Linux servers. Like endpoint protection, you can configure base policies, however, server protection includes the server lockdown policy.

## [Additional Information]

Set up base policies for Server Protection.

Server: Lockdown - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ServerConfigureLockdown/index.html>

Server: Peripheral Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ServerConfigurePeripheralControl/index.html>

Server: Threat Protection – <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ServerThreatProtectionInterceptX/index.html>

Server: Update Management - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureUpdatingPolicyServer/index.html>

Server: Web Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ServerConfigureWebControl/index.html>

Server: Windows Firewall - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureWindowsFirewallServer/index.html>

Server: Application Control - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ServerConfigureAppControl/index.html>



Additional information in  
the notes

# Global Templates - Configuration

Customers (0)	Global settings	Base policies
Customize base policies to be applied to customers (if you want to). Customers won't be able to change any of the base policies shown here. <a href="#">More info</a>		
Name	Last modified	Last modified by
Endpoint Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Peripheral Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Threat Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:19 AM	Ed Korsgaard
Web Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Windows Firewall		
Server Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Lockdown		
Peripheral Control		
Threat Protection	Oct 18, 2022 1:20 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:20 AM	Ed Korsgaard
Web Control		
Windows Firewall		
Encryption		
Device Encryption	Oct 18, 2022 1:20 AM	Ed Korsgaard
Email Security	Oct 18, 2022 1:20 AM	Ed Korsgaard

Device Encryption allows you to manage Windows BitLocker encryption and FileVault on macOS

The third section listed is device encryption which allows you to manage Windows BitLocker encryption and FileVault on macOS.

## [Additional Information]

Set up a base policy for Device Encryption - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/ConfigureDeviceEncryption/index.html>



Additional information in  
the notes

## Global Templates - Configuration

Customers (0)	Global settings	Base policies
Customize base policies to be applied to customers (if you want to). Customers won't be able to change any of the base policies shown here. <a href="#">More info</a>		
Name	Last modified	Last modified by
Endpoint Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Peripheral Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Threat Protection	Oct 18, 2022 1:19 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:19 AM	Ed Korsgaard
Web Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Windows Firewall		
Server Protection		
Application Control	Oct 18, 2022 1:19 AM	Ed Korsgaard
Lockdown		
Peripheral Control		
Threat Protection	Oct 18, 2022 1:20 AM	Ed Korsgaard
Update Management	Oct 18, 2022 1:20 AM	Ed Korsgaard
Web Control		
Windows Firewall		
Encryption		
Device Encryption	Oct 18, 2022 1:20 AM	Ed Korsgaard
Email Security		
Email Security	Oct 18, 2022 1:20 AM	Ed Korsgaard

Email Security allows for the modification of settings for inbound and outbound email

The fourth and final section is for email security which allows you to modify settings for inbound email messages except for enhanced content and file property scans, which apply to both inbound and outbound messages.

Please note that data loss prevention settings are not included in any base policy template.

### [Additional Information]

Set up a base policy for Email Security - <https://docs.sophos.com/central/Partner/help/en-us/Help/SettingsAndPolicies/GlobalTemplates/BasePolicies/EmailSecurityPolicy/index.html>

# Global Templates - Configuration

The screenshot shows the Sophos Partner Global Templates interface. On the left is a sidebar with 'MY CUSTOMERS' (Dashboard, Alerts, Logs) and 'SOPHOS CENTRAL' (Customers, Licenses). The main area is titled 'Default Customer Template' under 'Settings & Policies / Global Templates'. It shows a summary of the template: Name: Default Customer Template, Description: This is the standard template to apply to new customers to provide a strong base security with web filtering, Last push: (empty), Status: (empty). A red box highlights the 'Push to customers' button. Below it is a table with columns 'Name', 'Last modified', and 'Last modified by'. A green callout box points to the 'Push to customers' button with the text: 'Template is not applied until you select Push to customers'. Another green callout box points to the status row with the text: 'If a template includes new configuration a notification is displayed indicating that changes need to be pushed'. A warning message '⚠ You have changes to push' is visible in the status row.

For all new templates, or when an existing template is modified, a warning message is displayed to show that there are changes in the template that have not been pushed to the assigned customers.

Any settings configured in your template will not be applied to the assigned customers until you click '**Push to customers**'. Clicking **Push to customers** will initiate the application of the template to the customer accounts assigned. If you add another customer following the initial push, you will need to push the template to the new customer. This means that you can make any required changes and ensure that they are correct without worrying that customers will receive unintended settings.

# Customer Sophos Central Account

The screenshot shows the Sophos Central customer dashboard. On the left, there's a sidebar with various menu items like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, and Global Settings (which is currently selected). Below that is a section for 'MY PRODUCTS' with Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area is titled 'Global Settings' and contains several sections: 'General' (with Synchronized Security and Tamper Protection), 'Website Management' (with a padlock icon), 'Proxy Configuration', 'Global Exclusions' (with a padlock icon), 'Allowed Applications' (with a padlock icon), and 'Blocked Items'.

Global settings applied using a Partner template are indicated with a padlock in a customer Sophos Central account

Once templates have been pushed to a customer, the customer Sophos Central account is updated with the new settings.

In the customers Sophos Central dashboard, any global settings that have been pushed from the Partner Dashboard are indicated with a padlock.

Please note that not all global settings can be configured and applied from the Partner Dashboard.

# Customer Sophos Central Account

The screenshot shows the Sophos Central interface with the 'Website Management' section selected. A prominent yellow banner at the top states: 'Website Management is configured in Sophos Central Partner. No changes can be made here. Please contact your Sophos Central Partner.' Below this, a table lists websites with their tags and categories. The 'Override' column for both rows is greyed out with the message 'Override Disabled'. A green callout box highlights this behavior with the text: 'Customers are unable to make changes to Partner controlled global settings'.

WEBSITE	TAGGED AS	CATEGORY	Override
facebook.com	Social	Social	Override Disabled
twitch.tv	Social, Gaming	Gaming	Override Disabled

If a managed setting is selected, a banner is displayed at the top of the page alerting the user that they cannot make any changes. All modification options are greyed out.

# Customer Sophos Central Account

The screenshot shows the Sophos Central interface for Endpoint Protection Policies. On the left sidebar, under the 'CONFIGURE' section, 'Policies' is selected. The main content area is titled 'Endpoint Protection - Policies' and shows a table of policies categorized by protection type: Threat Protection (2), Peripheral Control (2), and Application Control (2). A note at the top states: 'Note: The policies at the top of the list override the policies at the bottom of the list.' In the Threat Protection section, the first policy, 'Steve's Test Policy', is listed as 'Enforced' with a status of 'User (2 / 0)' and last modified on 'Sep 1, 2022'. Below it, a policy named 'Base Policy - Threat Protection' is shown with a lock icon and the status 'Locked at partner level'. A green callout box points to this policy with the text: 'Base policies applied using a Partner template are indicated with a padlock in a customer Sophos Central account'. In the Peripheral Control section, there are two policies: 'Base Policy (cloned)' (Bypassed, User (0 / 0), Mar 30, 2022) and 'Base Policy - Peripheral Control' (Enforced, User (0 / 0), Mar 30, 2022). The bottom right corner of the interface features the 'SOPHOS' logo.

Name	Status	Type (single / group)	Last modified
Steve's Test Policy	✓ Enforced	User (2 / 0)	Sep 1, 2022
Base Policy - Threat Protection	Locked at partner level		
Base Policy (cloned)	Bypassed	User (0 / 0)	Mar 30, 2022
Base Policy - Peripheral Control	✓ Enforced	User (0 / 0)	Mar 30, 2022

When a base policy is assigned from the Central Partner Dashboard, the customer account is unable to edit the policy locally.

Any policy that is globally controlled by a partner is indicated with a padlock.

# Customer Sophos Central Account

The screenshot shows the Sophos Central interface. On the left, a dark sidebar menu includes 'ANALYZE' (Dashboard, Logs & Reports), 'MANAGE PROTECTION' (People, Computers), and 'CONFIGURE' (Policies, Settings, Protect Devices). The 'Policies' option is selected and highlighted in blue. The main content area is titled 'Endpoint Protection - View Computer Policy' under 'Computer Policies'. It shows a policy named 'Base Policy - Threat Protection' (Threat Protection : User) last updated on Mar 30, 2022. A prominent orange banner at the top states: 'Base policy is configured in Sophos Central Partner. No changes can be made here. You can create additional policies to override base-policy settings or contact your Sophos Central Partner.' Below the banner, the policy settings are displayed, including tabs for 'USERS/COMPUTERS', 'GROUPS', and 'SETTINGS' (which is selected). A green success message says 'Your policy settings give you the protection we recommend.' Under 'Live Protection', there are two toggle switches: one for 'Use Live Protection to check the latest threat information from SophosLabs online' (which is turned on) and another for 'Use Live Protection during scheduled scans'. A note below states: 'Note: The data may leave your geographic region and be shared with Sophos engineers.' The Sophos logo is in the bottom right corner.

If you select a locked policy, a banner is displayed that details the policy is configured by the Sophos Central partner. The policy cannot be modified.

# Customer Sophos Central Account

The screenshot shows the Sophos Central interface. On the left, a dark sidebar menu titled 'SOPHOS' lists 'Endpoint Protection' under 'ANALYZE' and 'Policies' under 'CONFIGURE'. The 'Policies' option is highlighted with a blue background. The main content area is titled 'Endpoint Protection - Policies' and shows a table of policies. 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 table has four columns: Name, Status, Type (single / group), and Last modified. It contains two entries under 'Threat Protection (2)': 'Steve's Test Policy' (Status: Enforced, Type: User (2 / 0), Last modified: Sep 1, 2022) and 'Base Policy - Threat Protection' (Status: Enforced, Type: User (0 / 0), Last modified: Mar 30, 2022). The base policy is noted as being 'Locked at partner level'. Below this is a section titled 'Peripheral Control (2)' with similar columns and entries.

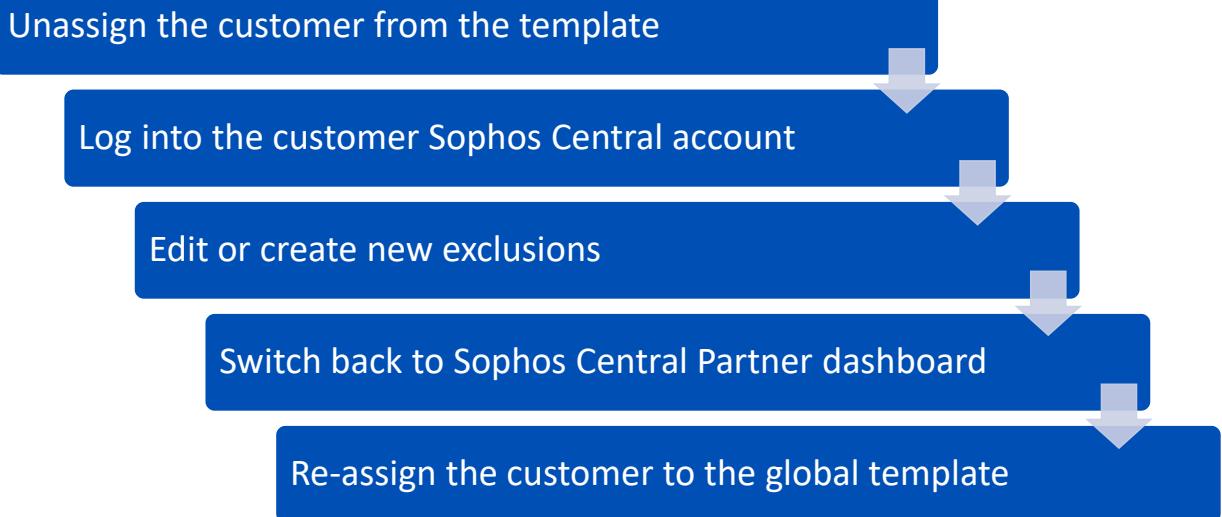
A customer can create new policies to overwrite the global base policies. It is important to work with any customers that have access to their Sophos Central account to ensure any new policies are secure

SOPHOS

Even though customers are unable to modify Partner assigned base policies, they can create new policies which could be used to apply different settings. As a new policy will take precedence over a base policy it is important to work with those customers that have administrator access to their Sophos Central account to ensure they are not creating policies that could introduce unnecessary vulnerabilities.

It is important to note that most Partners manage customer accounts and therefore it is unlikely a customer will have access to their Sophos Central account. The purpose of global policy templates is to make the configuration of policies easier and more efficient for Partners managing multiple customer accounts.

# Global Template Exclusions



SOPHOS

If a policy exclusion is applied in a customer Sophos Central account before a partner global template is applied, when the global template is applied to the customer account, the exclusions are locked. This means that a customer is unable to edit the exclusions and those exclusions are not displayed in the Central Partner Dashboard global template.

Should an exclusion need to be modified, or additional exclusions be added for a specific customer, the following steps should be performed:

- First, unassign the customer from the global template
- Next, log into the customers Sophos Central account
- Edit the exclusion or create new exclusions as required
- Switch back to the Sophos Central Partner Dashboard
- And re-assign the customer to the global template

# Global Template Management

If a global template is deleted or a customer is unassigned from a template

- All assigned customers retain all settings including exclusions
- All editing options are enabled and all settings can be modified locally
- The padlock icon is removed for any configured settings

If a customer is unassigned from one template and assigned to another

- The new template overwrites all configured settings
- Local exclusions remain if they were applied before the template was applied

SOPHOS

The management of any configured global templates is important to understand. Let's look at some examples.

If a global template is deleted or a customer is unassigned, any customer account that was assigned to the template retains the settings from the template including all exclusions. The customer will be able to modify all settings locally, the padlock icon will be removed, and all editing options will be displayed.

If a customer is unassigned from one template and assigned to another the settings, policies, and exclusions from the previous template are overwritten, however, local exclusions that were in place before the template was applied will remain.

# Global Template Best Practice

## Scenario

- New Managed Service Provider (MSP)
- Using Sophos Central endpoint and server protection to secure customer accounts
- Using Sophos Central Partner Dashboard to apply and manage global settings

SOPHOS

Let's look at how to configure global templates as a new Managed Service Provider (MSP).

In this scenario, the MSP is using Sophos Central endpoint and server protection to secure their customers and the Sophos Central Partner Dashboard to manage the base policies and global settings.

# Global Templates Best Practice

- Configure a default global template **BEFORE** onboarding new customers
- The template needs to provide secure protection whilst specific configuration requirements are investigated

- We do not recommend configuring global settings for the default template

Customers (0)	Global settings	Base policies
Customize global settings to be applied to customers. Customers won't be able to change these custom settings. <a href="#">More info</a>		
Name ^	Description	
Allowed Applications	See items you've allowed.	
Data Lake Endpoint Upload Settings	Manage uploads to the Data Lake from your computers.	
Data Lake Server Upload Settings	Manage uploads to the Data Lake from your servers.	
Device Migration	Allow devices to migrate from one Sophos Central account to another.	
Global Exclusions	Manage exclusions for known files, websites, and applications in order to improve performance.	
SSL/TLS decryption of HTTPS	Control decryption of websites and manage exclusions	
Website Management	Manage, categorize, and tag websites for use with Web Control and Web Gateway features.	

SOPHOS

Our recommendation is that the MSP configures a default global template before onboarding any customers. The default global template is the first template that will be assigned to customer accounts providing secure protection settings whilst the MSP investigates any special configuration requirements.

We do not recommend the configuration of any global settings for the default template. This is because this template is used primarily for monitoring applications and providing secure protection to customers whilst investigating customer specific requirements.

# Global Template Best Practice

## Endpoint

- Threat protection: Use recommended settings
- Configure Application Control to allow but not block the controlled applications to create visibility of use
- Configure Peripheral Control in monitor mode, for visibility

## Server

- Threat protection: Use recommended settings
- Configure Peripheral Control in monitor mode for visibility

We do not recommend the configuration of any exclusions in a global template

SOPHOS

The most important factor for the default template is that it is secure yet compatible. We therefore recommend the following:

- Do not add any exclusions without good reason. Global exclusions reduce security and should be considered carefully before applying them, additionally an exclusion required by one customer may not be required by another and therefore should not be applied through a global template
- Use the recommended settings for the Threat Protection base policy
- Configure the application control base policy to allow all applications but not to block. Ensure you select controlled application in the policy to build visibility of which apps are being used
- Configure the peripheral control policy in monitor mode to create visibility of what devices are being used

For server protection, our recommendation is to ensure the threat protection policy is configured with the recommended settings and to configure the peripheral control policy in monitor mode for visibility.

# Global Template Best Practice

## Customer One

- Switch to Sophos MSP as a new provider
- Previous provider removed ALL security software
- Customer is currently unprotected

## Solution

- Deploy the Sophos Endpoint Agent to all devices
- Assign the customer to default global template

SOPHOS

The default global template is configured, the MSP can begin onboarding customers.

The first customer has switched to the MSP as their new provider. Their previous provider has removed all security software leaving the customer unprotected.

The MSP would deploy the Sophos Endpoint Agent to all devices and then assign the customer to the default global template to apply the most secure settings.

# Global Template Best Practice

## Customer One

- Sophos protection is in place
- Default template is assigned
- Customer requests web protection

## Solution

- Clone the default template
- Name the new template appropriately
- Configure the new template with web protection
- Push the template to the customer
- Review the policy with the customer and make any modifications required

SOPHOS

Now that customer one is protected, the MSP can work with the customer to identify any custom security features that are required. For example, the customer may want to make use of web protection. As web protection is not included in the default global template the MSP will need to create a new template for the customer.

The MSP can clone the existing default global template, changing the template name so the purpose of the template is easily determined. The MSP applies the recommended web protection settings. Should the customer see any issues, the policy can be modified to meet the customer requirements.

# Global Template Best Practice

## Customer Two

- Controlled migration to Sophos MSP
- Default protection required
- Web Protection required

## Solution

- Deploy the Sophos Endpoint Agent to all devices
- Assign the default template to provide protection
- Assign customer two to the global template created for customer one
- Identify any website exclusions
- Add identified exclusions to the customer two Sophos Central account locally
- Push the global template to all customers

SOPHOS

The MSP is approached by customer two who are planning to switch providers and would like to migrate their settings from their current provider to Sophos.

The MSP deploys Sophos Endpoint Agent to customer two and applies the default template to provide secure protection. Customer two would like to enable web protection. The MSP identifies the template created for customer one and adds customer two to the global template.

Following testing, customer two identifies websites that are required but are blocked by the policy. The MSP investigates the required websites and determines that the website exclusions are only required by customer two. The MSP logs into customer two's Sophos Central account to apply the required website exclusions locally in the threat protection policy.

The global template is pushed again which will mean that all locally added exclusions are retained.

## Considerations | Exclusions



Take a moment to consider what information a partner or an MSP needs to have before applying any exclusions for a customer.

SOPHOS

Let's take a moment to consider what information a partner or an MSP needs to have before applying any exclusions for a customer.

# Exclusions Best Practice

Any exclusions should be carefully considered before being applied

## APPLICATIONS

- What is the impact of excluding the app?
- What is the purpose of the app?
- Was the app blocked by app control?
- What was the app blocked as malicious or a PUA?
- Is the app legitimate and incorrectly categorized?
- Does an app request need to be submitted to Sophos?

## WEBSITES

- What is the impact of excluding the website?
- Is the website already categorized?
- Is the website for business use?
- Does a request need to be submitted to Sophos to re-categorize the website?
- What can be downloaded from the website?

## FILES/FOLDERS

- What is the impact of excluding the file or folder?
- What other files would this exclusion allow to be accessed/run?
- What is the use of the file/folder? Is there another way to achieve the customer requirements without creating an exclusion?
- Is the exclusion business critical?

SOPHOS

Any exclusion being applied should be carefully considered as an exclusion to any security policy can reduce protection.

When considering an exclusion request, a Partner or MSP should consider asking their customer several questions to determine why the exclusion is required. Some questions are shown here for some of the exclusion types that can be applied.

The important point to remember is that you need to understand why an exclusion is required before you make any policy changes.

## Exclusions Best Practice

### To who and where should exclusions be applied?

- Only exclusions that are required for ALL customers should be included in a global template
- Specific customer exclusions should be applied locally in the customer Sophos Central account

SOPHOS

If an exclusion is found to be appropriate, the next consideration is who the exclusion should apply to. Our recommendations are:

- Only exclusions that are required for ALL customers should be included in a global template
- Specific customer exclusions should be applied locally in the customer Sophos Central account

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!

# Question 1 of 3



Which security feature is not included in any base policy template?

Application Control

Web Protection

Server Lockdown

Data Loss Prevention

SOPHOS

## Question 2 of 3

**True or False:** A customer can only be assigned to one global template.

True

False

## Question 3 of 3

Which icon indicates a global setting or policy is managed by a Sophos Partner?



# Chapter Review

Create global templates to **efficiently apply security settings** to multiple customers. Global templates are used to **configure base policies and global settings** for managed customers.

**Global template settings overwrite existing base policy and global settings** in assigned customer Sophos Central accounts. It is important to remember that **customers can only have one global template assigned to them**.

Only exclusions that are required for **ALL** customers should be included in a global template.

SOPHOS

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

Create global templates to efficiently apply security settings to multiple customers. Global templates are used to configure base policies and global settings for managed customers.

Global template settings overwrite existing base policy and global settings in assigned customer Sophos Central accounts. It is important to remember that customers can only have one global template assigned to them.

Only exclusions that are required for ALL customers should be included in a global template.



# Troubleshooting Sophos Central Policies

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE3575: Troubleshooting 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.

# Troubleshooting Sophos Central Policies

In this chapter you will learn how to troubleshoot issues with policy communication.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

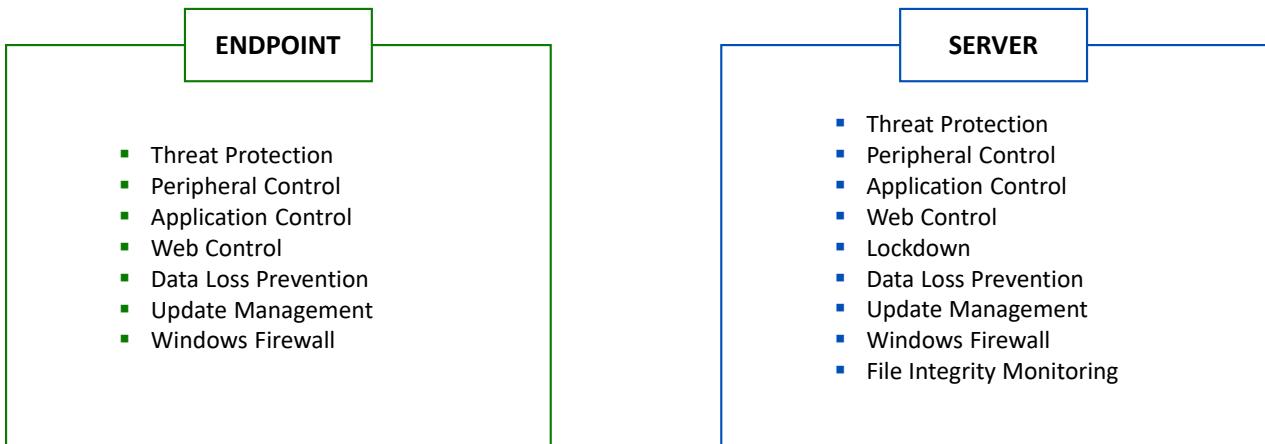
- ✓ How to protect devices with Sophos Central
- ✓ How to create and clone policies
- ✓ How to assign policies to devices and users

DURATION      **14 minutes**

SOPHOS

In this chapter you will learn how to troubleshoot issues with policy communication.

# Sophos Central Base Policies



Base policies cannot be deleted or disabled

SOPHOS

Sophos Central policies apply specific settings to protected devices. Sophos Central includes a number of base policies.

For endpoints, a base policy is provided for threat protection, peripheral control, application control, web control, data loss prevention, update management, and Windows Firewall. For Servers, a base policy for Server lockdown and for file integrity monitoring are provided.

All base policies can be edited and cloned to suit requirements, however, it is important to understand that if a base policy is edited and the pre-configured recommended settings are disabled, your protection is significantly reduced. Whilst base policies can be edited and cloned, they cannot be deleted or disabled.

# Enforcing Policies

The screenshot shows the Sophos Central interface for managing computer policies. The left sidebar has sections for ANALYZE (Dashboard, Logs & Reports), MANAGE PROTECTION (People, Computers), and CONFIGURE (Policies, Settings). The Policies tab is selected. The main content area is titled "Endpoint Protection - View Computer Policy" and shows a policy named "Base Policy - Peripheral Control" for "Peripheral Control : User". The status bar indicates "POLICY ENFORCED". A section titled "Manage Peripherals" allows configuration of peripheral control settings. Below this, a summary table shows totals for various peripherals like Bluetooth and Modem. A prominent message at the bottom states: "Some policies are NOT configured by default" and "ALWAYS check your policies to ensure that your organization is protected".

When troubleshooting policies, it is important to understand which policies are enabled by default, and those which require configuration.

The threat protection policy is automatically applied by default to all protected devices. The other policies are specific to individual organizations, as such, they are not configured by default. For example, the peripheral and application control policies require configuration.

# Enforcing Policies

The screenshot shows two policy configuration pages from Sophos Central:

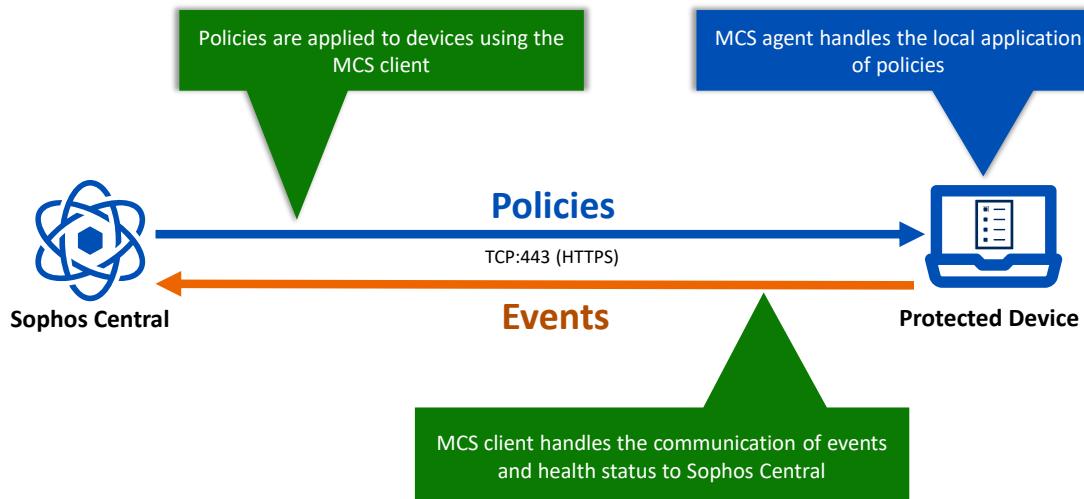
- Server Protection:** Under "Runtime Protection", three checkboxes are checked: "Protect document files from ransomware (CryptoGuard)", "Protect from remotely run ransomware", and "Protect from Encrypting File System attacks". An "ACTION TO TAKE ON RANSOMWARE DETECTION" dropdown is set to "Terminate Process". A note at the bottom states: "This setting only applies to servers you add to the New Server Protection Features EAP. Join the EAP now".
- Endpoint Protection:** Under "Runtime Protection", three checkboxes are checked: "Protect document files from ransomware (CryptoGuard)", "Protect from remotely run ransomware", and "Protect from Encrypting File System attacks". An "ACTION TO TAKE ON RANSOMWARE DETECTION" dropdown is set to "Terminate Process". A note at the bottom states: "This setting only applies to endpoints you add to the New Endpoint Protection Features EAP. Join the EAP now".

A green callout box with white text states: "Some features are only implemented for those devices included in an EAP".

In the threat protection policy, some features are only implemented if you have signed up for an early access programme and have included protected devices in the programme.

These settings are indicated in the **SETTINGS** tab for both the server and endpoint policies.

# Policy Communication



SOPHOS

Let's look at how policies are communicated to devices. Management traffic can be defined as everything sent and received by the management communication system, MCS.

MCS has an adapter that is installed for each component of the Sophos Endpoint Agent that allows for the exchange of messages, policy application, and event information including the detection of malware or a change in the endpoint health status. MCS uses TCP port 443 for communication.

The MCS service is divided into two sub services:

- The MCS client which handles the communication between Sophos Central and the protected device
- The MCS agent which handles the local application of policies once the device has received them



Additional information in  
the notes

# Configuration File

```
*C:\ProgramData\Sophos\Management Communications System\Endpoint\Config\Config.xml - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Config.xml
1 <?xml version="1.0" encoding="utf-8"?>
2 <Configuration>
3   <McsClient>
4     <LogPath />
5     <servers>
6       <server>https://dzc-mcs-amzn-eu-west-1-9af7.up.e.p.hmr.sophos.com/sophos/management/ep</server>
7     </servers>
8     <proxies />
9     <proxyCredentials />
10    <messageRelays>
11      <messageRelay address="srv.sophos.local" id="315286ce-6f6f-4412-ba33-339eaa5381bb" port="8190" priority="0"></messageRelay>
12    </messageRelays>
13    <useSystemProxy>1</useSystemProxy>
14    <useAutomaticProxy>1</useAutomaticProxy>
15    <commandPollingInterval>60</commandPollingInterval>
16    <presignedUrlServiceUrl></presignedUrlServiceUrl>
17    <presignedUrlServiceCredentials></presignedUrlServiceCredentials>
18    <policyChangeServers />
19    <useDirect>1</useDirect>
20    <registrationToken>a2e58f8bb680f29f3551b9baee051f410926f2e028652716499390233ec29cd7</registrationToken>
21    <randomSkewFactor>1</randomSkewFactor>
22  </McsClient>
23 </Configuration>

eXtensible Markup Language file length : 891 lines : 24 Ln : 21 Col : 47 Sel : 0 | 0 Unix (LF) UTF-8 INS .
```

SOPHOS

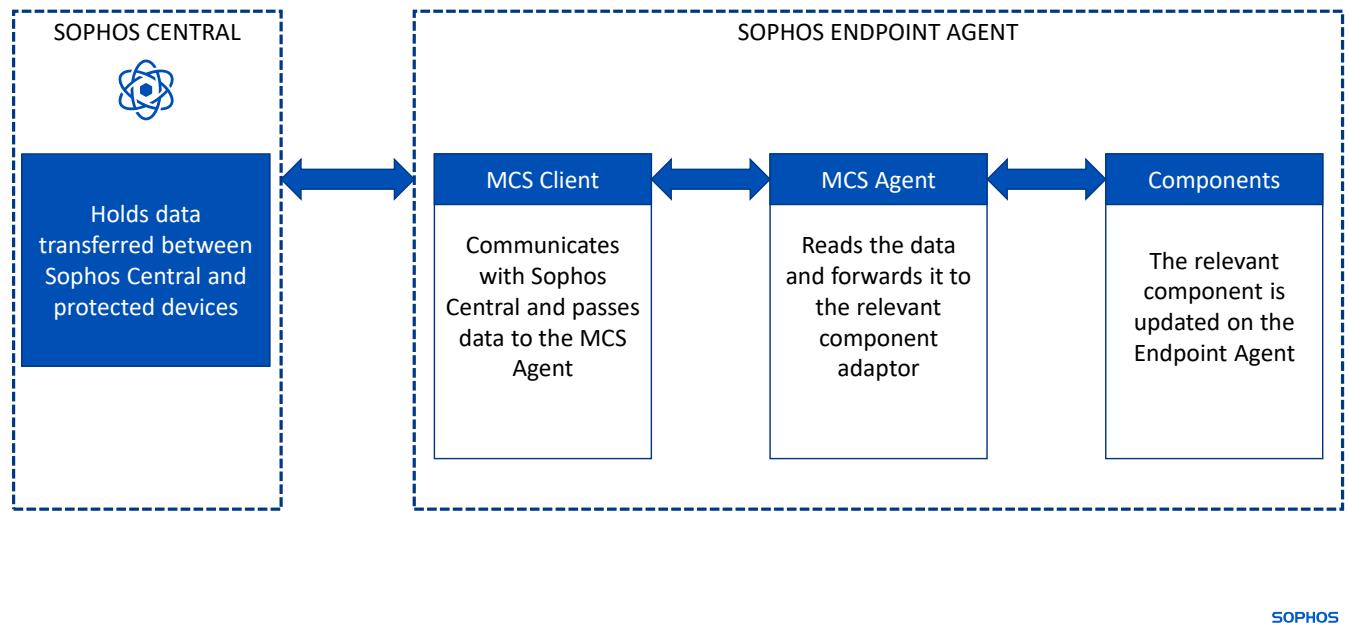
A configuration file is used to hold the management communication configuration information.

The config.xml file includes details of the Sophos server and any message relays that may be configured. It also holds the registration token which identifies the device to Sophos Central.

## [Additional Information]

The config.xml can be found in %ProgramData%\Sophos\Management Communication System\Endpoint\Config

# Policy Communication



When a policy update is received from Sophos Central the MCS Client passes it to the MCS Agent for processing. The MCS Agent reads the data and sends it to the appropriate component adaptor, for example, a web control policy update will be passed to the web control component. The component then applies the policy to the device.

When the device health or status changes, an update is sent to Sophos Central using the following steps:

- The component collects data related to the event and sends it to the MCS Agent
- The MCS Agent forwards the data to the MCS Client
- The MCS Client sends the data to Sophos Central
- The data is collected in Sophos Central and stored
- Sophos Central displays the data in the Admin console

# Policy Communication

The screenshot shows the Sophos Central interface for Endpoint Protection Policies. On the left, a dark sidebar menu includes 'ANALYZE' (Dashboard, Logs & Reports), 'MANAGE PROTECTION' (People, Computers), and 'CONFIGURE' (Policies, Settings). The 'Policies' option under 'CONFIGURE' is highlighted. The main content area is titled 'Endpoint Protection - Policies' and shows a table of Threat Protection policies:

Name	Status	Type (single / group)
Policy 3	Enforced	Computer (2 / 0)
Policy 2	Enforced	User (0 / 1)
Policy 1	Enforced	Computer (2 / 0)
Base Policy - Threat Protection	Enforced	

A note at the top states: 'Note: The policies at the top of the list override the policies at the bottom of the list.'

In the center, another screenshot shows the 'Endpoint Protection - WinClient2' device record. The 'Computers' tab is selected. A green callout box on the left says 'Multiple policies can be configured'. A green callout box on the right points to the 'POLICIES' tab in the top navigation bar of the device record page. The 'POLICIES' tab is selected, showing a list of assigned policies:

TYPE	NAME
Encryption: Device Encryption	Base Policy - Device Encryption
Endpoint Protection: Application Control (user)	Base Policy - Application Control
Endpoint Protection: Data Loss Prevention (user)	Base Policy - Data Loss Prevention
Endpoint Protection: Windows Firewall (user)	Base Policy - Windows Firewall
Endpoint Protection: Peripheral Control (user)	Base Policy - Peripheral Control
Endpoint Protection: Threat Protection (device)	Policy 1
Endpoint Protection: Update Management (user)	Base Policy - Update Management
Endpoint Protection: Web Control (user)	Base Policy - Web Control

If you have multiple policies, you can view which policy is assigned to a specific device by navigating to the device page.

On the **POLICIES** tab for each protected device, you can view all of the policies assigned to the device. In this example, this device has the threat protection policy – policy 1 assigned.

# Policy Communication

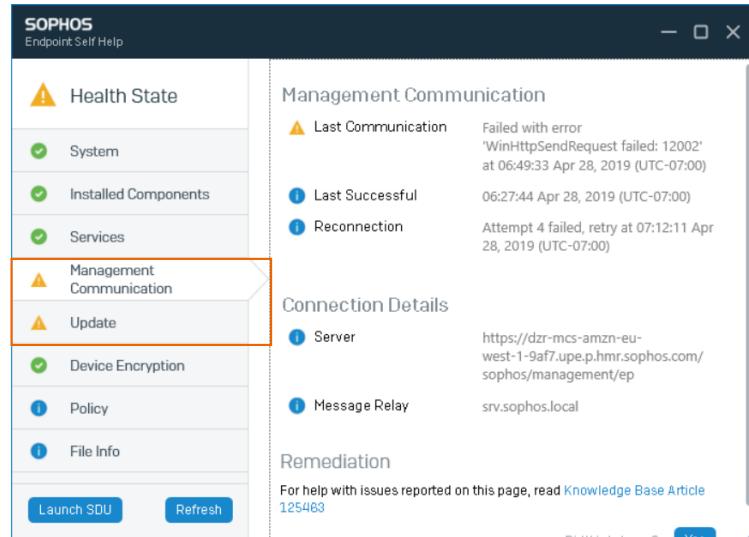
The screenshot shows the Sophos Endpoint Self Help interface. On the left is a sidebar with icons for Health State, System, Installed Components, Services, Management Communication (which is selected), Update, and Policy. At the bottom of the sidebar are 'Launch SDU' and 'Refresh' buttons. The main area has tabs for 'Management Communication' (selected) and 'Connection Details'. Under 'Management Communication', there's a section for 'Last Communication' which shows 'Succeeded at 13:25:06 Jun 16, 2021 (UTC+00:00)'. Under 'Connection Details', it lists 'Server' (https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep), 'Server Address' (52.209.158.255), and 'Proxy' (No proxy used). Below these tabs is a 'Remediation' section with a link to a Knowledge Base Article and a 'Did this help you?' button with 'Yes'.

The Management Communication tab displays the last communication date

If you have a device that is not receiving a policy, then checking the last communication time is a good first step for troubleshooting the issue. Using the Endpoint Self Help tool you can see the communication details for management traffic. This includes the date and time of the last communication.

The connection details provide the name of the management communication server, the IP address of the server, and the proxy address if used. If you have also made use of message relays, the message relay DNS will be displayed here.

# Policy Communication



SOPHOS

The troubleshooting steps used to resolve management communication issues are similar to troubleshooting updating issues.

Communication issues will often affect both updating and management communication components.

# Forcing Management Communication

## Why?

- To test policy changes
- Verify issue resolution

## How?

- Click **Update Now** in the Sophos Endpoint Agent
- The device will perform an **update first** and then establish management communication
- Can take some time to complete
- Does not need tamper protection disabled on the device

SOPHOS

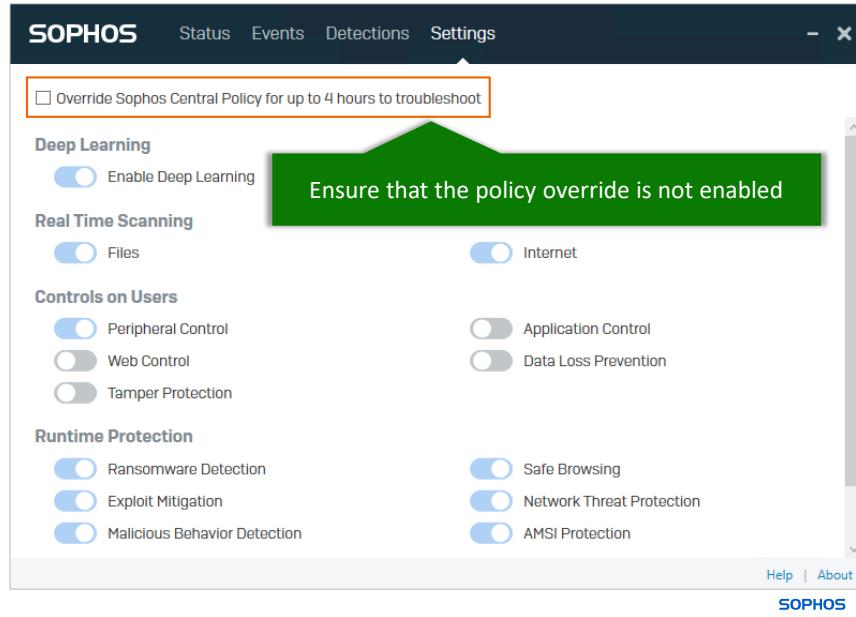
When troubleshooting communication issues, you may need to force management communication to test policy changes, or to verify issue resolution. The most common reason to force management communication is when a change has been applied to a Sophos Central policy and you want to ensure that the device has received the updated policy. A device will eventually receive the policy changes, however, this can take up to 5 minutes. Typically you want to apply and test changes quickly.

There are two ways to force management communication. The first is to click the **Update Now** button in the Sophos Endpoint Agent. This is an indirect communication. Once the device finishes updating, it will tell Sophos Central that an update has succeeded. Should a device require numerous updates, it may take some time to complete before the management communication is established. The benefit of this method is that it does not require you to disable tamper protection on the device.

# Forcing Management Communication

## How?

- Disable tamper protection for the specific device
- Stop the MCS Client and Agent Services
- Restart the MCS Client service
- Restart the MCS Agent service



The second method to force management communication is to disable tamper protection for the specific device and then stop the MCS Client and Agent services.

Then restart the services, the MCS Client service must be started first, followed by the MCS Agent service.

We recommend that you ensure that the policy override in the Sophos Endpoint Agent is not enabled once the services have restarted as this will prevent the device from receiving updated policies from Sophos Central.

# Policy Communication

	Last Time Policy Received
AMSI	Not since 16:54:28 Feb 24, 2021 (UTC +00:00)
Heartbeat	10:28:49 Jun 16, 2021 (UTC+00:00)
HitmanPro.Alert	09:57:42 May 18, 2021 (UTC+00:00)
LiveQuery	09:57:42 May 18, 2021 (UTC+00:00)
Management Communication System	09:57:43 May 18, 2021 (UTC+00:00)
Network Threat Protection	10:30:42 Jun 16, 2021 (UTC+00:00)
Sophos Anti Virus	10:38:05 Jun 16, 2021 (UTC+00:00)
Sophos AutoUpdate	09:57:42 May 18, 2021 (UTC+00:00)
Sophos Core	Not since 16:54:28 Feb 24, 2021 (UTC +00:00)
Sophos Core Customer	10:38:04 Jun 16, 2021 (UTC+00:00)
Sophos Endpoint Firewall	Not since 16:54:28 Feb 24, 2021 (UTC +00:00)
Sophos User Interface	10:38:05 Jun 16, 2021 (UTC+00:00)
Sophos Web Control	Not since 16:54:28 Feb 24, 2021 (UTC +00:00)

SOPHOS

The **Policy** tab in the ESH tool displays the last date and time policies were received for each component. A change made to a policy in Sophos Central should result in a new date and time for the policy shown here following a refresh.

# Endpoint Self Help Components

Component	Policy Details
Hitmanpro alert	Threat protection   runtime protection   mitigation exploits in vulnerable applications   protect media applications
Network threat protection	Threat protection   runtime protection   detect network traffic to command-and-control servers
Sophos anti-virus	Threat protection   real-time scanning Internet   detect low reputation files
Sophos web control	Web control

SOPHOS

This table display some of the components and the corresponding policy in Sophos Central.

# Policy Communication

How to test that a policy is being received:

1 In Sophos Central Admin go to **Configure > Policies**

2 **Modify** a policy

3 **Save** the policy to trigger a policy refresh

4 Click **Refresh** in ESH and check for an updated time-stamp

SOPHOS

You can test that policies are being received by completing these steps:

1. In Sophos Central navigate to **CONFIGURE > Policies**
2. **Modify** a policy
3. **Save** the policy to trigger a policy refresh
4. Wait up to 130 seconds, click **Refresh** in ESH and check for an updated time stamp

We recommend making these changes only as a test and reverting the settings once you have confirmed that a device is receiving the policy.



Additional information in  
the notes

# Policy Communication

The screenshot shows a Windows File Explorer window with the following details:

- Path:** C:\ProgramData\Sophos\Remote Management System\3\Agent\AdapterStorage
- File Explorer View:** Details
- Items:** 14 items, 1 item selected (CORC)
- Table Headers:** Name, Date modified, Type, Size
- Table Data:** A list of 14 file folders, all named with acronyms (ALC, AMSI, CORC, CORE, EFW, FIM, HBT, HMPA, LiveTerminal, MCS, NTP, SDU, SHS, UI). The 'CORC' folder is highlighted.

C:\ProgramData\Sophos\Remote Management System\3\Agent\AdapterStorage\

SOPHOS

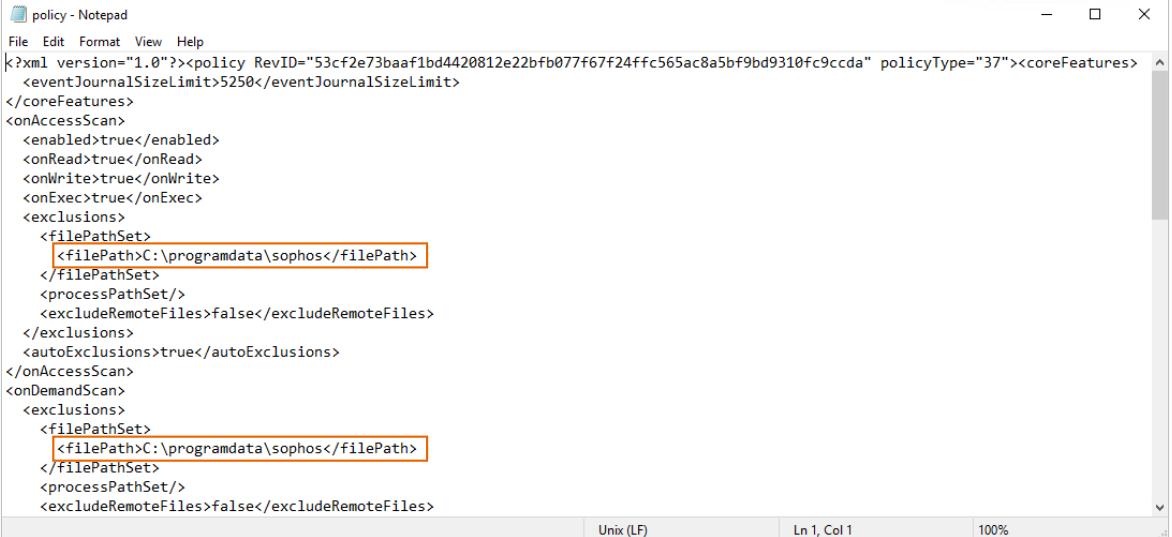
Policy changes are logged to a single policy file for each component. These files can be checked to ensure a policy change has been applied to a device.

Remote management system is a legacy communication component, within this folder you will find single folders that branch into the different components using acronyms, the MCS folder contains the management communication policy configuration and information.

## [Additional Information]

Remote management system file location: C:\ProgramData\Sophos\Remote Management System\3\Agent\AdapterStorage\

# Policy Communication



A screenshot of a Windows Notepad window titled "policy - Notepad". The window displays an XML configuration file for a threat protection policy. Two specific sections of the XML code are highlighted with orange boxes:

```
<?xml version="1.0"?><policy RevID="53cf2e73baaf1bd4420812e22bfb077f67f24ffc565ac8a5bf9bd9310fc9ccda" policyType="37"><coreFeatures>
</coreFeatures>
<onAccessScan>
<enabled>true</enabled>
<onRead>true</onRead>
<onWrite>true</onWrite>
<onExec>true</onExec>
<exclusions>
<filePathSet>
<filePath>C:\programdata\sophos</filePath>
</filePathSet>
</processPathSet>
<excludeRemoteFiles>false</excludeRemoteFiles>
</exclusions>
<autoExclusions>true</autoExclusions>
</onAccessScan>
<onDemandScan>
<exclusions>
<filePathSet>
<filePath>C:\programdata\sophos</filePath>
</filePathSet>
</processPathSet>
<excludeRemoteFiles>false</excludeRemoteFiles>
```

The Notepad window includes standard status bars at the bottom: "Unix (LF)", "Ln 1, Col 1", and "100%". A "SOPHOS" logo is visible on the right side of the window.

In this example, we have added an exclusion to the threat protection policy and want to ensure that the device has received the policy including the exclusion. Opening the policy file in a text editor will display the configuration of the policy.

We have highlighted a file exclusion that was added to the threat protection policy. This indicates that the policy has been received successfully.

# MCS Logs



## Additional information in the notes

## MCS Log Location

C:\ProgramData\Sophos\Management Communications System\Endpoint\Logs

The MCS logs can be used to check the policy communication between Sophos Central and a managed device. MCS creates two log files.

The MCS Client log which details the communication between a device and Sophos Central.

The MCS Agent Log which details the application of policies and other communications from Sophos Central.

### [Additional Information]

MCS logs are located in C:\ProgramData\Sophos\Management Communication System\Endpoint\Logs\MCSClient.log

# MCS Client Log



```
McsClient - Notepad
File Edit Format View Help
2022-07-29T13:54:58.917Z [ 3112: 3964] I POST https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep/v2/data_feed/device/fe5d3799-5083 ^-4850-9e57-19c816f21812/feed_id/scheduled_query
2022-07-29T13:54:58.944Z [ 3112: 3964] I 200 : sent=551 rcvd=0 elapsed=26ms
2022-07-29T13:54:58.944Z [ 3112: 3964] I Feed channel scheduled_query: uploading file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\scheduled-20220729135453871.json result 0 purge false
2022-07-29T13:54:58.944Z [ 3112: 3964] I Feed channel scheduled_query: uploaded file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\Incoming\scheduled-20220729135453871.json
2022-07-29T13:55:08.401Z [ 3112: 3872] I (async) 200 : chunk=286 rcvd=7 comtime=17100829ms
2022-07-29T13:55:08.401Z [ 3112: 3964] I GET https://mcs2-cloudstation-eu-west-
1.prod.hydra.sophos.com:443/sophos/management/ep/commands/applications/ALC;AMSI;CORC;CORE;EFW;HBT;HMPA;LiveQuery;LiveTerminal;MCS;NTP;SAV;SDU;SHS;SWC;UI;APPSPROXY/endpoint/efd57399-0538-8485-e975-918c612f8121
2022-07-29T13:55:28.107Z [ 3112: 3964] I 200 : sent=0 rcvd=140 elapsed=25ms
2022-07-29T13:55:28.109Z [ 3112: 3964] I POST https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep/v2/data_feed/device/fe5d3799-5083^-4850-9e57-19c816f21812/feed_id/scheduled_query
2022-07-29T13:55:28.140Z [ 3112: 3964] I 200 : sent=480 rcvd=0 elapsed=30ms
2022-07-29T13:55:28.140Z [ 3112: 3964] I Feed channel scheduled_query: uploading file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\Incoming\scheduled-20220729135523047.json result 0 purge false
2022-07-29T13:55:28.140Z [ 3112: 3964] I Feed channel scheduled_query: uploaded file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\Incoming\scheduled-20220729135523047.json
2022-07-29T13:56:08.405Z [ 3112: 1996] I (async) 200 : chunk=287 rcvd=7 comtime=17160832ms
2022-07-29T13:56:29.071Z [ 3112: 3964] I GET https://mcs2-cloudstation-eu-west-
1.prod.hydra.sophos.com:443/sophos/management/ep/commands/applications/ALC;AMSI;CORC;CORE;EFW;HBT;HMPA;LiveQuery;LiveTerminal;MCS;NTP;SAV;SDU;SHS;SWC;UI;APPSPROXY/endpoint/efd57399-0538-8485-e975-918c612f8121
2022-07-29T13:56:29.109Z [ 3112: 3964] I 200 : sent=0 rcvd=140 elapsed=107ms
2022-07-29T13:56:29.182Z [ 3112: 3964] I POST https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep/v2/data_feed/device/fe5d3799-5083^-4850-9e57-19c816f21812/feed_id/scheduled_query
2022-07-29T13:56:29.212Z [ 3112: 3964] I 200 : sent=509 rcvd=0 elapsed=29ms
2022-07-29T13:56:29.212Z [ 3112: 3964] I Feed channel scheduled_query: uploading file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\Incoming\scheduled-20220729135624044.json result 0 purge false
2022-07-29T13:56:29.212Z [ 3112: 3964] I Feed channel scheduled_query: uploaded file C:\ProgramData\Sophos\Management Communications System\Endpoint\Channels\LiveQueryScheduled\Incoming\scheduled-20220729135624044.json
```

SOPHOS

The format of each line in the log consists of the data, time, process ID, thread ID, severity, and log event.

The z in the timestamp indicates Zulu or UTC time. The MCS Client log contains HTTPS status codes which are important for troubleshooting MCS issues.

In this example, we have highlighted these codes in green which indicate that the 'GET' request was successful.

# MCS Agent Log

```
File Edit Format View Help
2022-07-29T09:15:32.924Z [ 3128: 5064] I [SHS] SHS adapter: Status changed - sending new status message
2022-07-29T09:41:59.817Z [ 3128: 1088] I UserInfo has changed: saving and broadcasting to listening adapters
2022-07-29T09:41:59.822Z [ 3128: 1088] I [AMSI] Received property changed from: APPSPROXY
2022-07-29T09:41:59.822Z [ 3128: 1088] I [HBT] Heartbeat adapter: AdapterPropertiesChanged notification received from APPSPROXY, check user info
2022-07-29T09:41:59.822Z [ 3128: 1088] I [HBT] Heartbeat adapter: Set user info
2022-07-29T09:41:59.822Z [ 3128: 1088] I [UI] UI: AdapterPropertiesChanged notification received from APPSPROXY
2022-07-29T09:41:59.822Z [ 3128: 1088] I [UI] UI: Set key to SOFTWARE\Sophos\Sophos UI\AdapterNotifications, trying to match adapter APPSPROXY
2022-07-29T09:41:59.822Z [ 3128: 1088] I [UI] UI: Updating registry key SOFTWARE\Sophos\Sophos UI\AdapterNotifications\APPSPROXY
2022-07-29T10:15:43.130Z [ 3128: 4196] I [ALC] Update completed: code=0, message='', details=''
2022-07-29T10:33:17.299Z [ 3128: 3132] I Session Change Notification: Remote session disconnected
2022-07-29T10:33:17.530Z [ 3128: 1088] I UserInfo has changed: saving and broadcasting to listening adapters
2022-07-29T10:33:17.539Z [ 3128: 1088] I [AMSI] Received property changed from: APPSPROXY
2022-07-29T10:33:17.539Z [ 3128: 1088] I [HBT] Heartbeat adapter: AdapterPropertiesChanged notification received from APPSPROXY, check user info
2022-07-29T10:33:17.539Z [ 3128: 1088] I [HBT] Heartbeat adapter: Clear user info
2022-07-29T10:33:17.540Z [ 3128: 1088] I [UI] UI: AdapterPropertiesChanged notification received from APPSPROXY
2022-07-29T10:33:17.540Z [ 3128: 1088] I [UI] UI: Set key to SOFTWARE\Sophos\Sophos UI\AdapterNotifications, trying to match adapter APPSPROXY
2022-07-29T10:33:17.540Z [ 3128: 1088] I [UI] UI: Updating registry key SOFTWARE\Sophos\Sophos UI\AdapterNotifications\APPSPROXY
2022-07-29T10:33:17.540Z [ 3128: 1088] I [UI] UI: UpdateAdapterNotification registry updated for adapter APPSPROXY
2022-07-29T12:21:11.740Z [ 3128: 3132] I Session Change Notification: Remote session connected
2022-07-29T12:21:12.059Z [ 3128: 1088] I UserInfo has changed: saving and broadcasting to listening adapters
2022-07-29T12:21:12.090Z [ 3128: 1088] I [AMSI] Received property changed from: APPSPROXY
2022-07-29T12:21:12.090Z [ 3128: 1088] I [HBT] Heartbeat adapter: AdapterPropertiesChanged notification received from APPSPROXY, check user info
2022-07-29T12:21:12.090Z [ 3128: 1088] I [HBT] Heartbeat adapter: Set user info
2022-07-29T12:21:12.090Z [ 3128: 1088] I [UI] UI: AdapterPropertiesChanged notification received from APPSPROXY
2022-07-29T12:21:12.090Z [ 3128: 1088] I [UI] UI: Set key to SOFTWARE\Sophos\Sophos UI\AdapterNotifications, trying to match adapter APPSPROXY
2022-07-29T12:21:12.090Z [ 3128: 1088] I [UI] UI: Updating registry key SOFTWARE\Sophos\Sophos UI\AdapterNotifications\APPSPROXY
2022-07-29T12:21:12.091Z [ 3128: 1088] I [UI] UI: UpdateAdapterNotification registry updated for adapter APPSPROXY
2022-07-29T13:15:18.459Z [ 3128: 5064] I [SHS] SHS adapter: Status changed - sending new status message
2022-07-29T13:15:33.472Z [ 3128: 5064] I [SHS] SHS adapter: Status changed - sending new status message
```

SOPHOS

The MCS Agent log details the application of policies from Sophos Central. This log should be checked to confirm that a device has received a policy.



# HTTPS Status Codes

STATUS CODE	REASON	DESCRIPTION
200	OK	Successful request
201	Created	Optionally used if event resources created
204	No Content	Optionally used if no commands are available
304	Not Modified	Different version of policy not available
400	Bad Request	Invalid request
401	Unauthorized	Authentication failed
404	Not found	Requested resource currently unavailable
500	Internal server error	Some unexpected problem on the server
501	Not Implemented	Client makes a request that is not supported
503	Service Unavailable	Server is unable to service the request. Possibly because the requested resource is temporarily unavailable

SOPHOS

HTTP status codes that are significant to the MCS protocol are seen in the MCS Client log. Knowing what these codes are can be useful in troubleshooting MCS communication issues.

An example of some of the codes are shown here. The most common codes are 200 and 503.

## [Additional Information]

<https://www.restapitutorial.com/httpstatuscodes.html>

# Logging Level

Enable detailed logging by changing the logging level for MCS logs

1 Turn off tamper protection for the device

2 Stop the MCS Client and Agent services

3 Navigate to the config.xml file and open it

config.xml

C:\ProgramData\Sophos\Management Communications System\Endpoint\Config

SOPHOS

There may be circumstances when it is necessary to enable more detailed logging to troubleshoot an issue. Sophos support may request that you change the logging level for the MCS logs, reproduce an issue, and then check the logs.

We recommend that you take a backup of the config.xml file before you make changes to the current file. To change the logging level for MCS logs:

1. Turn off tamper protection for the device
2. Stop the MCS Agent and MCS Client services on the device
3. Navigate to **config.xml** and open it



Additional information in  
the notes

# Logging Level

```
<?xml version="1.0"?>
<Configuration>
    <McsClient>
        <loglevel>0</loglevel>
        <logPath />
        <servers>
            <server>https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep</server>
        </servers>
        <proxies />
        <proxyCredentials />
        <messageRelays>
            <messageRelay address="dc.sophos.local" id="9237d0e5-1c91-44a5-ad93-a75af933879" port="8190" priority="0" />
            <messageRelay address="reading3" id="66b81eda-b601-4efb-8641-316c7ebe85de" port="8190" priority="0" />
        </messageRelays>
        <useSystemProxy>1</useSystemProxy>
        <useAutomaticProxy>1</useAutomaticProxy>
        <commandPollingInterval>120</commandPollingInterval>
        <v2Apis>
            <api><responses></api>
        </v2Apis>
        <presignedUrlServiceUrl>https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com/sophos/management/ep/presignedUrls</presignedUrlServiceUrl>
        <presignedUrlServiceCredentials>CCDjdEHfI0Lxfx2zhL7CYeBPTdyLNDHCz8InQkyZTBUs/mmCrDVQ6+wZh3SfFB34tQdFP+Kyj+WP6HdyfnUbfH0gbQ+jhNU69K8V2uZzYLvxjaXzLVxjPsxkEp0I=</presignedUrlServiceCredentials>
        <registrationToken>5149ba2bb687ee03c981388ca4a7a7e7a4599bf9f53d0ce7a1ae09b818b3943</registrationToken>
        <useDirect>1</useDirect>
        <flagsPollingInterval>14400</flagsPollingInterval>
        <randomSkewFactor>1</randomSkewFactor>
        <pushServers>
            <pushServer>https://mcs-push-server-eu-west-1.prod.hydra.sophos.com/ps</pushServer>
        </pushServers>
        <pushPingTimeout>90</pushPingTimeout>
        <pushFallbackPollInterval>120</pushFallbackPollInterval>
    </McsClient>
    <McsAgent>
        <loglevel>0</loglevel>
    </McsAgent>
</Configuration>
```

4. Within the McsClient tag, create a new line to change the log level to zero

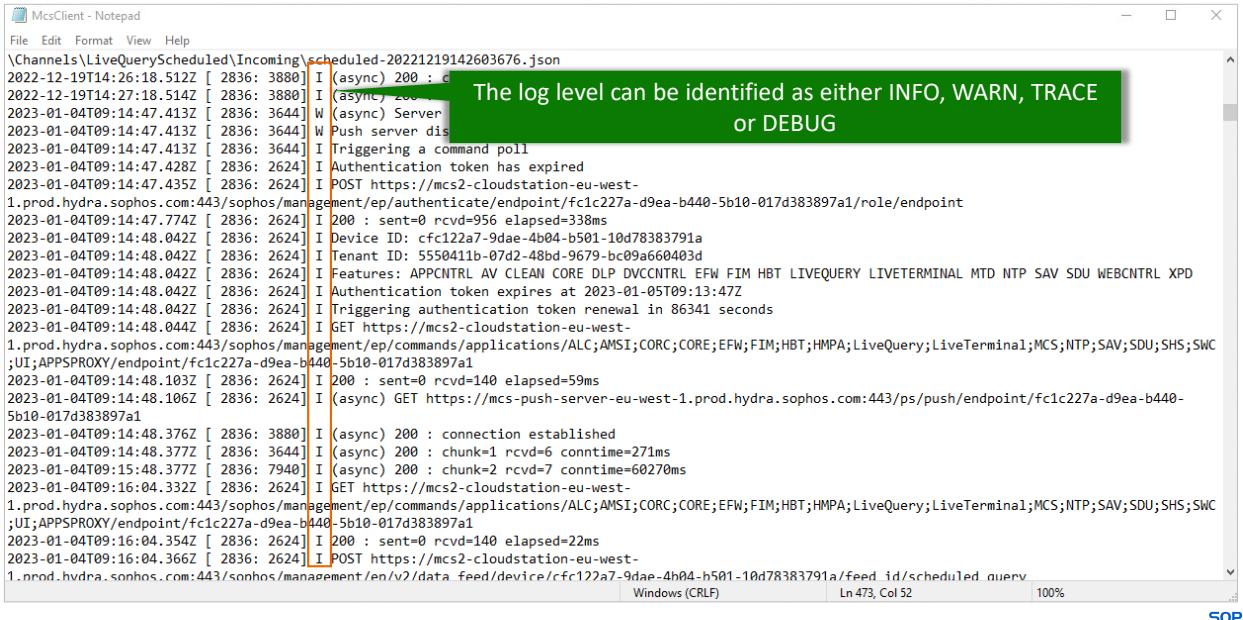
5. Configure logging for the McsAgent tag, you may need to create the McsAgent tag

An example of the amended config.xml file is displayed here. Remember to save the changes you make to this file.

## [Additional Information]

How to change logging level **KB-000034874**. <https://support.sophos.com/support/s/article/KB-000034874>

# Logging Level



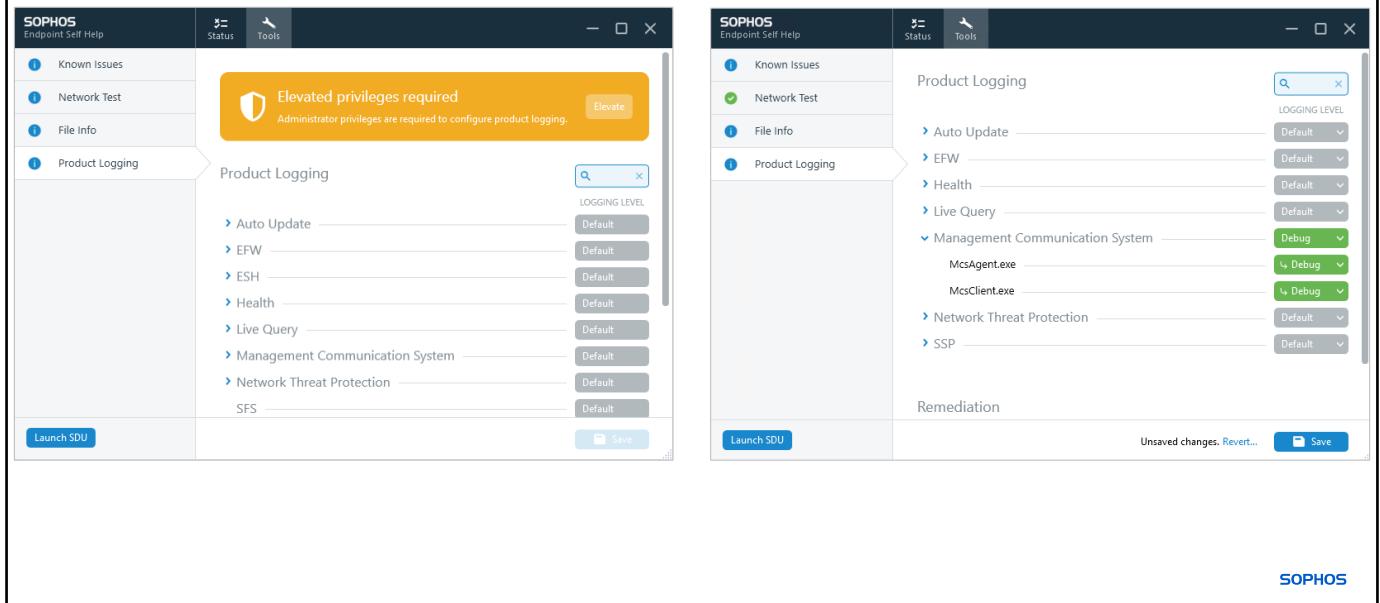
```
\Channels\LiveQueryScheduled\Incoming\scheduled-20221219142603676.json
2022-12-19T14:26:18.512Z [ 2836: 3880] I (async) 200 : sent=0 rcvd=956 elapsed=338ms
2022-12-19T14:27:18.514Z [ 2836: 3880] I (async) 200 : 
2023-01-04T09:14:47.413Z [ 2836: 3644] W (async) Server
2023-01-04T09:14:47.413Z [ 2836: 3644] W Push server dis
2023-01-04T09:14:47.413Z [ 2836: 3644] I Triggering a command poll
2023-01-04T09:14:47.428Z [ 2836: 2624] I Authentication token has expired
2023-01-04T09:14:47.435Z [ 2836: 2624] I POST https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep/authenticate/endpoint/fc1c227a-d9ea-b440-5b10-017d383897a1/role/endpoint
2023-01-04T09:14:47.774Z [ 2836: 2624] I 200 : sent=0 rcvd=956 elapsed=338ms
2023-01-04T09:14:48.042Z [ 2836: 2624] I Device ID: cfc122a7-9dae-4b04-b501-10d78383791a
2023-01-04T09:14:48.042Z [ 2836: 2624] I Tenant ID: 5550411b-07d2-48bd-9679-bc09a660403d
2023-01-04T09:14:48.042Z [ 2836: 2624] I Features: APPCNTRL AV CLEAN CORE DLP DVCCNTRL EFW FIM HBT LIVEQUERY LIVETERMINAL MTD NTP SAV SDU WEBCNTRL XPD
2023-01-04T09:14:48.042Z [ 2836: 2624] I Authentication token expires at 2023-01-05T09:13:47Z
2023-01-04T09:14:48.042Z [ 2836: 2624] I Triggering authentication token renewal in 86341 seconds
2023-01-04T09:14:48.044Z [ 2836: 2624] I GET https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/ps/push/endpoint/fc1c227a-d9ea-b440-5b10-017d383897a1
2023-01-04T09:14:48.376Z [ 2836: 3880] I (async) 200 : connection established
2023-01-04T09:14:48.377Z [ 2836: 3644] I (async) 200 : chunk=1 rcvd=6 conntime=271ms
2023-01-04T09:15:48.377Z [ 2836: 7940] I (async) 200 : chunk=2 rcvd=7 conntime=60270ms
2023-01-04T09:16:04.332Z [ 2836: 2624] I GET https://mcs2-cloudstation-eu-west-1.prod.hydra.sophos.com:443/sophos/management/ep/commands/applications/ALC;AMSI;CORC;CORE;EFW;FIM;HBT;HMPA;LiveQuery;LiveTerminal;MCS;NTP;SAV;SDU;SHS;SWC;UI;APPSPROXY/endpoint/fc1c227a-d9ea-b440-5b10-017d383897a1
2023-01-04T09:16:04.354Z [ 2836: 2624] I 200 : sent=0 rcvd=140 elapsed=59ms
2023-01-04T09:16:04.366Z [ 2836: 2624] I POST https://mcs2-cloudstation-eu-west-1.nrnd.hvdr.a.sonhos.com:443/sonhos/management/en/v2/data_feed/device/cfc122a7-9dae-4b04-h501-10d78383791a/feed_id/scheduled_aquery
Windows (CRLF) | Ln 473, Col 52 | 100%
```

Once the config.xml has been saved, re-start the MCS Client and Agent services.

Confirm the changes have been successful by opening the MCS Agent and Client logs in a text editor. The level of logging can be identified before the message as either TRACE, WARN, DEBUG or INFO. This example log file displays the extra details that are recorded when the logging level has been modified.

We recommend that the log level is returned to the original value once troubleshooting has been completed.

# Logging Level



The Endpoint Self Help tool also provides a way to change the logging level of the management communication system. You can select to enable debug logging for example. Once the changes are saved, re-produce the issue and then check the relevant log files.

You will be prompted to change the log level back to default when you close the Endpoint Self Help tool.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!

# Question 1 of 4



In which two places can you change the logging level for Sophos log files?

In the device record in  
Sophos Central

Assign the logging level in  
the threat protection policy

Editing the config.xml

In the MCS client log

Endpoint Self Help tool

In the Windows services

SOPHOS

## Question 2 of 4

**True or False:** Base policies can be disabled.

True

False

## Question 3 of 4

Which file contains the management communication configuration information?

\_\_\_\_\_

## Question 4 of 4

Match the component with its function.

MCS Client

DROP

Handles the communication between Sophos Central and a protected device

MCS Agent

DROP

Handles the local application of policies once the device has received them

# Chapter Review

**Management traffic** is communicated between Sophos Central and protected devices using the **Management Communication System** on **TCP port 443**.

**MCS has an adaptor** that is installed for each component of the Sophos Endpoint Agent that allows for the **exchange of messages, policy application, and event information** including the detection of malware or a change in the endpoint health status.

**Troubleshooting** management communication issues can be aided by checking the **Endpoint Self Help tool**, configuring the **logging level** and checking the **MCS Client and Agent logs**.

SOPHOS

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

Management traffic is communicated between Sophos Central and protected devices using the management communication system on TCP port 443.

MCS has an adapter that is installed for each component of the Sophos Endpoint Agent that allows for the exchange of messages, policy application, and event information including the detection of malware or a change in the endpoint health status.

Troubleshooting management communication issues can be aided by checking the Endpoint Self Help tool, configuring the logging level and checking the MCS Client and Agent logs.



# Getting Started with SIEM Integration with Sophos Central

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4015: Getting Started with SIEM Integration with 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 SIEM Integration with Sophos Central

In this chapter you will learn how to integrate Sophos Central with third party tools using Security Information and Event Management (SIEM) technology.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

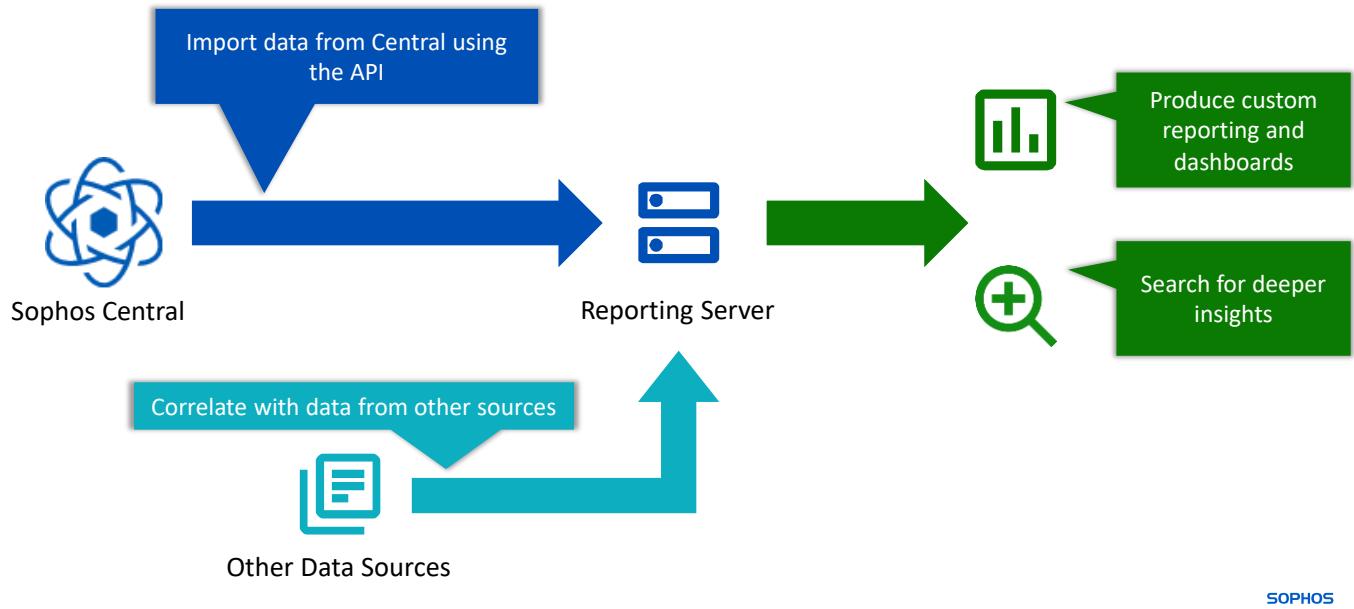
- ✓ Working with Sophos Central global settings
- ✓ Configuring APIs in Sophos Central

DURATION **6 minutes**

SOPHOS

In this chapter you will learn how to integrate Sophos Central with third party tools using Security Information and Event Management technology.

# Security Information and Event Management (SIEM)



Whilst Sophos Central provides several reporting options, you may want to link your Sophos Central data with other data sources. Security Information and Event Management (SIEM) technology collects logs and other security-related documentation for analysis.

The Sophos Central SIEM integration API enables new event and alert data to be pulled from Sophos Central. This data can be used to identify behaviour with threat potential which would not be apparent based on alerts alone.

For example, a series of failed logins to a server might not be noteworthy, however, visibility of this information along with additional sequential data from the network could give a strong indication that a hacking attempt is in progress.

## [Additional Information]

A short video shows the benefits of SIEM integration: <https://youtu.be/1MPwbfoldBk>

# Configuring SIEM Integration

Create an API Token



Download and configure the Sophos SIEM script



Import the data into your preferred tool

SOPHOS

Configuration of SIEM with Sophos Central can be split into three steps:

1. Create an API token that will be used to export the data
2. Download and configure the Sophos SIEM script that will export the data
3. Configure your preferred tool to import the data

# Application Programming Interface (API) Token

The screenshot shows the Sophos Central interface. On the left, a dark sidebar menu includes 'Dashboard', 'Alerts', 'Threat Analysis Center', 'Logs & Reports', 'People', 'Devices', and 'Global Settings' (which is highlighted in blue). Below these are sections for 'MY PRODUCTS' with links to 'Endpoint Protection', 'Server Protection', and 'Mobile'. The main content area is titled 'SIEM' under 'Global Settings / API Token Management / SIEM'. It displays an 'API Token Summary' for a token named 'SIEM' that expires on 'Sep 09, 2023'. It shows the 'API Access URL' as 'https://api3.central.sophos.com/gateway' and the 'Headers' as 'x-api-key: OTTliaUMct... eJbh4'. There are 'Copy' buttons next to both fields. A third field, 'API Access URL + Headers', contains the combined information: 'url: https://api3.central.sophos.com/gateway, x-api-key: OTTliaUM... eJbh4, Authorization: Basic OGI4Mz... UwzSUIVIII... DQ='.

SIEM integration uses an Application Programming Interface (API) to extract data from Sophos Central. API tokens provide credentials that allow access to Sophos Central from SIEM interfaces. All tokens are assigned a read-only role by default.

API tokens are managed in **Global Settings**. When you create the token, we recommend that you give it a descriptive name. You should create separate tokens for each device or application that will be accessing Sophos Central in case the access is compromised.

The API token will be displayed in two formats, the API access URL, and the API headers. The last data field displayed combines both the URL and the header to make copying the information easier.



Additional information in  
the notes

# SIEM Script

<https://github.com/sophos/Sophos-Central-SIEM-Integration>

The screenshot shows a Windows File Explorer window on the left and a Notepad++ window on the right. The File Explorer window shows a folder structure under 'This PC > SYS (C) > siem'. Inside the 'siem' folder, there are several files: config (Python File), config (Compiled Python File), LICENSE-2.0 (Text Document), name\_mapping (Python File), name\_mapping (Compiled Python File), README.md (MD File), siem (Python File), and test\_regression (Python File). The Notepad++ window displays the 'config.ini' file with the following content:

```
[login]
# API Access URL + Headers
# API token setup steps: https://community.sophos.com/kb/en-us/125169
token_info = <Copy API Access URL + Headers block from Sophos Central here>

# format can be json, cef or keyvalue
format = json

# filename can be syslog, stdout, any custom filename
filename = result.txt

# endpoint can be event, alert or all
endpoint = event

# syslog properties
# for remote address use <remoteServerIp>:<port>, for e.g. 192.1.2.3:514
# for linux local systems use /dev/log
# for MAC OSX use /var/run/syslog
address = /var/run/syslog
facility = daemon
socktype = udp
```

SOPHOS

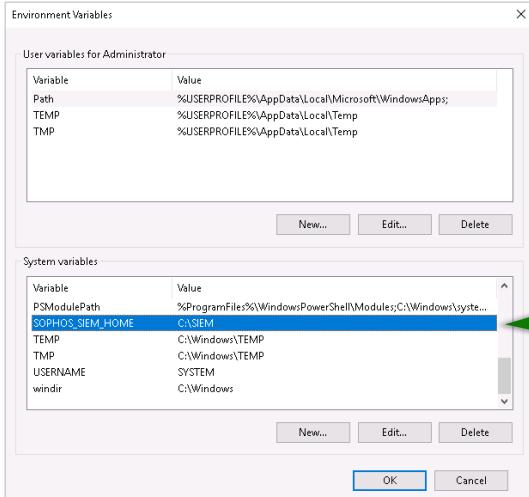
Sophos has created a script that provides a simple means to configure SIEM integration which is available on GitHub. You can download a zip file that contains the script and its configuration files. The config.ini file needs to be modified to include the API token copied from Sophos Central. There are several options that can also be configured in this file:

- The preferred output format, which can be JSON, CEF or keyvalue
- The output filename. For example, the name of a file, syslog or stdout
- If you are using syslog, you need to configure the server details

## [Additional Information]

The script is available here: <https://github.com/sophos/Sophos-Central-SIEM-Integration>

# SIEM Script



Location of config.ini and  
siem\_cef\_mapping.txt

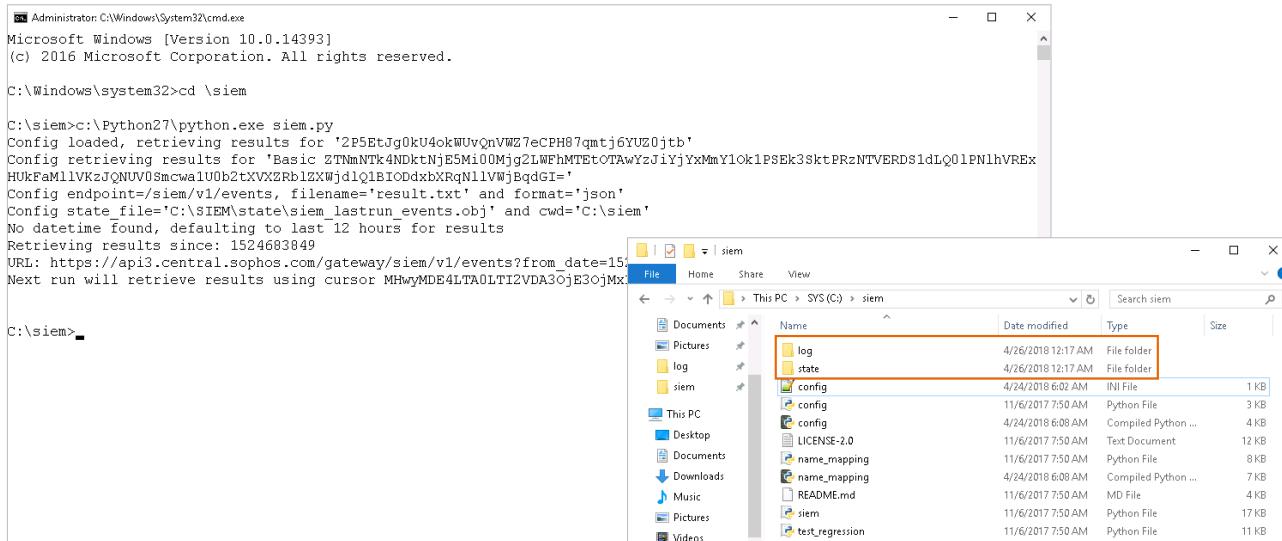
Log and state folders will be created in  
this location

SOPHOS

The script will use the SOPHOS\_SIEM\_HOME environment variable to determine where the log files will be located. You can either set this environment variable each time before calling the script, or set it globally.

The log and state folders will be created the first time the script is run.

# SIEM Script



```
C:\Administrator:C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \siem

C:\siem>c:\Python27\python.exe siem.py
Config loaded, retrieving results for '2P5EtJg0kU4okWWUvQnVWZ7eCPH87qmtj6YUZ0jtb'
Config retrieving results for 'Basic ZTNmNtk4NDktNjE5Mi00Mjg2LWFhMTExOTAwYzJiYjYxMmYlOk1PSEk3SktrPRzNTVERDS1dLQ01PNlhVREx
HUKEm11VKzJQNUV0Smcwa1U0h2tXVXZRB1ZXWjd1p1B1ODdxhXRqN1IVWjbqGt='
Config endpoints='/siem/v1/events', filename='result.txt' and format='json'
Config state file='C:\SIEM\state\siem_lastrun_events.obj' and cwd='C:\siem'
No datetime found, defaulting to last 12 hours for results
Retrieving results since: 1524683849
URL: https://api3.central.sophos.com/gateway/siem/v1/events?from_date=1524683849&size=1000
Next run will retrieve results using cursor MHwyMDE4LTa0LTIZVDA3OjB3OjMx

C:\siem>
```

Name	Date modified	Type	Size
log	4/26/2018 12:17 AM	File folder	
state	4/26/2018 12:17 AM	File folder	
config	4/24/2018 6:02 AM	INI File	1 KB
config	11/6/2017 7:50 AM	Python File	3 KB
config	4/24/2018 6:08 AM	Compiled Python ...	4 KB
LICENSE-2.0	11/6/2017 7:50 AM	Text Document	12 KB
name_mapping	11/6/2017 7:50 AM	Python File	8 KB
name_mapping	4/24/2018 6:08 AM	Compiled Python ...	7 KB
README.mnd	11/6/2017 7:50 AM	MD File	4 KB
siem	11/6/2017 7:50 AM	Python File	17 KB
test_regression	11/6/2017 7:50 AM	Python File	11 KB

SOPHOS

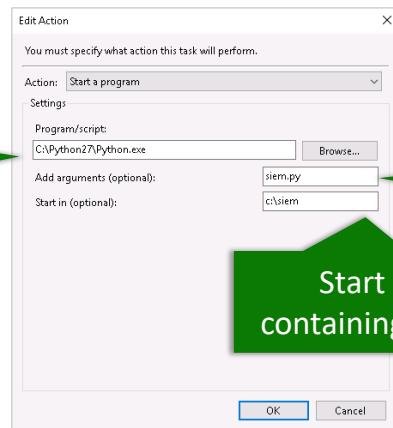
The script will retrieve the last twelve hours of events on its initial run, and a maximum of twenty four hours of historical data can be retrieved. The script keeps track of its state so that it can always continue from where it left off, based on a state file stored in the state folder.

The script calls the server until there are no more events available. There is also a built-in registry mechanism if there are any network issues. The script exits if there are no more events available or when a re-try fails. In this case, the next scheduled run of the script will pick-up the state from the last run, using the state file.

Here you can see an example of the script being run for the first time. The log and state folders are created in the SIEM folder and contain the results.txt file with the data exported from Sophos Central.

# SIEM Script

Call Python



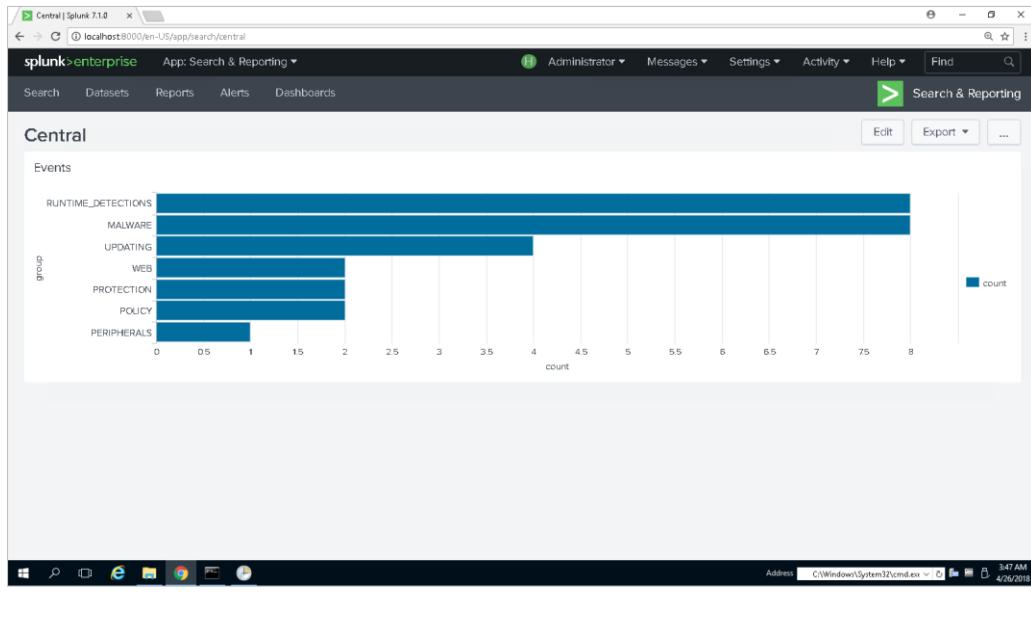
Pass the SIEM script

Start in the folder  
containing the SIEM script

SOPHOS

To schedule the script to run, you need to call Python and pass the SIEM script as an argument. The start folder should be the location of the SIEM script.

# Import Data

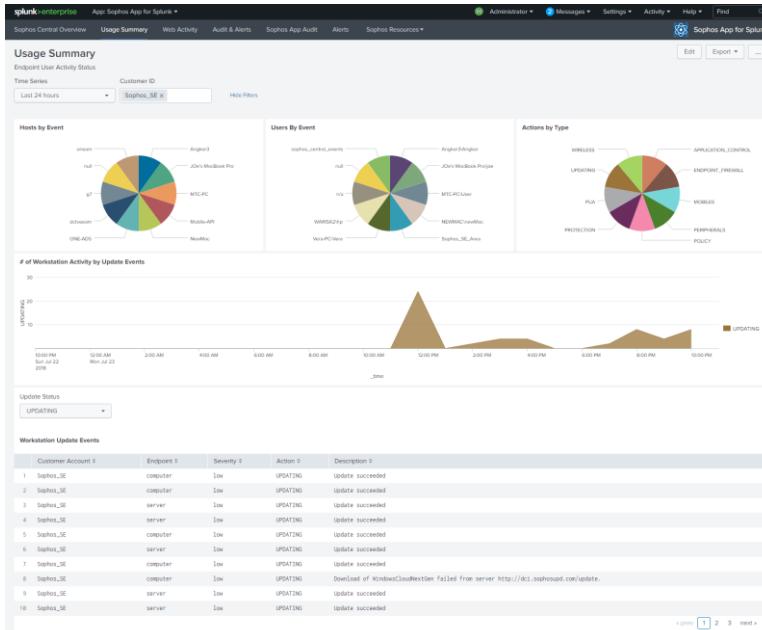


SOPHOS

With the script running, you can configure your preferred tool to import and use the data.

For example, you can use it to create custom views and dashboards, correlate it with other security data or trigger actions.

# Import Data



■ <https://splunkbase.splunk.com/app/4096/>

■ <https://splunkbase.splunk.com/app/4097/>

For demonstration, here is a Splunk dashboard that was developed by Sophos.

The Splunk app has been installed and configured to pull data from a Sophos Central account.

## [Additional Information]

<https://splunkbase.splunk.com/app/4096/>

<https://splunkbase.splunk.com/app/4097/>

SOPHOS

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 1

How does the Central SIEM Integration script authenticate to access Sophos Central?

With an admin username  
and password

With an API token

Using Active Directory for  
SSO

Using SAML for SSO

SOPHOS

# Chapter Review

SIEM technology collects logs and other security-related documentation for analysis.

Sophos Central API enables new event and alert data to be pulled from Sophos Central.

API tokens provide credentials that allow access to Sophos Central from SIEM interfaces. All tokens are assigned a read-only role by default.

SOPHOS

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

Security Information and Event Management (SIEM) technology collects logs and other security-related documentation for analysis.

The Sophos Central integration API enables new event and alert data to be pulled from Sophos Central. This data can be used to identify behaviour with threat potential which would not be apparent based on alerts alone.

API tokens provide credentials that allow access to Sophos Central from SIEM interfaces. All tokens are assigned a read-only role by default.



# Advanced Sophos Central Threat Remediation

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4035: Advanced 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.

# Advanced Sophos Central Threat Remediation

In this chapter you will learn how to remediate threats manually when automatic clean up fails and how to isolate devices during threat investigations.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ Protect and manage devices with Sophos Central
- ✓ Use Sophos Central and Sophos Endpoint Agent to view and manage threats

DURATION

14 minutes

SOPHOS

In this chapter you will learn how to remediate threats manually when automatic clean up fails and how to isolate devices during threat investigations.

## Sophos Clean Logs

- When automatic clean up is run on a device you can view the following logs in Sophos Central

Log file	Location	Description
Clean.txt	C:\ProgramData\Sophos\Clean\Logs	Contains SafeStore verification, threat count, restoration commands, and command process flow logging. Service information is also included.
Scan_<date>_<id>.txt	C:\ProgramData\Sophos\Clean\Logs	This file contains the task process flow, volume information, detection triggering the clean operation, the corresponding action, and the time to complete the scan.

SOPHOS

When an item is detected, Sophos Clean is used to clean up the item. When removing a file, Sophos Clean checks all the references to that file and removes them as well. This means any other links such as registry entries are removed. All items are moved to the SafeStore which stores and encrypts detected items.

The Clean log will display threat count and restoration information if a file has been allowed following detection. The scan logs include the detection triggers and the action taken. You will see multiple scan logs for a device that correspond to the scans run on a device.

# Manual Clean Up

## Why manual clean up may be required

- The detection identity does not have a clean up routine
- The permissions on the file do not permit clean up
- A threat is found in an archive and the Sophos Endpoint Agent will not remove the archive file, as it may contain legitimate files

SOPHOS

It is rare that threats are not automatically cleaned up on protected devices. However, there may be occasions when automatic clean up is unable to take place. An alert will display in Sophos Central indicating that malware was not cleaned up and that manual clean up is required.

A detection may require manual clean up if the detection identity does not have a clean up routine, or the permissions on the file do not permit clean up.

Another example could be if a threat is found in an archive. The Sophos Endpoint Agent will not remove the archive file, as it may contain legitimate files. You will need to determine if the archive is safe and remove the detected malicious file manually from the archive.

# Manual Clean Up

## Why manual clean up may be required

- The path the threat has been detected in is a mailbox, meaning the threat cannot be automatically remediated
- The threat was detected in a temporary Internet file, the file may no longer exist on the device.
- The threat was detected on a removal device which has since been ejected, the file will not be accessible on the device for clean up

SOPHOS

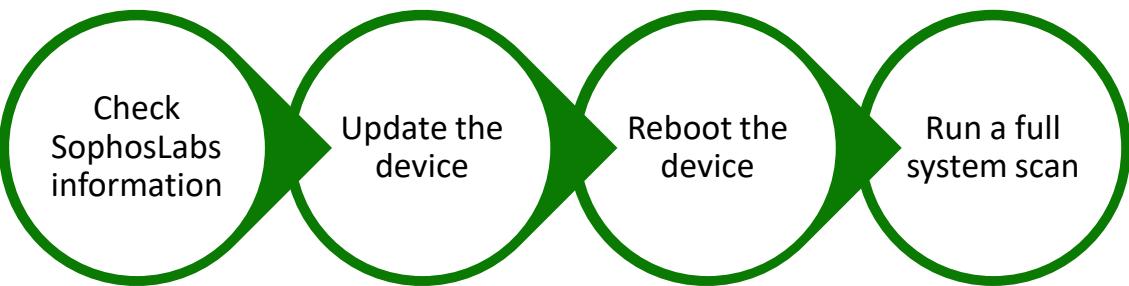
Further examples of when manual clean up could be required are:

If the path the threat has been detected in is a mailbox, the threat cannot be automatically remediated. We recommend that you use your email client to find and delete the item. Typically, it will be an attachment, therefore you need to locate the email with the attachment and delete the email including removing it from all trash locations.

If the threat was detected in a temporary Internet file, the file may no longer exist on the device.

If the threat was detected on a removal device which has since been ejected, the file will not be accessible on the device for clean up.

# Manual Clean Up



Most Recent Alerts

<span style="color: red;">!</span> Apr 3, 2019 1:13 PM	Manual cleanup required: 'EICAR-AV-Test' at '/home/sysadmin/eicar.com'	n/a	linux
--	--	-----	-------

[View All Alerts](#)

Click the threat information for view the latest information from SophosLabs

SOPHOS

We recommend the following steps for manually cleaning up detected threats.

1. Check the SophosLabs page for the threat details. The threat name is linked to SophosLabs from Sophos Central which details all known information about the detected threat. The 'more information' page may give specific remediation instructions
2. Ensure that the device where the threat was detected is up-to-date
3. Reboot the device
4. Run a full system scan on the updated device

Once the scan has completed, check the alerts page in Sophos Central. If the threat is removed, no further action is required.



Additional information in  
the notes

## Manual Clean Up

The detection alert still exists in Sophos Central

- Look for the detected file on the device
- Acknowledge the alert in Sophos Central
- Run an additional full system scan

The detected file still exists on the device

- Delete the file from the detected location manually
- Run a full system scan to ensure the file has been removed and is not re-detected

The detected file is unable to be deleted manually from the device

- Submit file sample to Sophos for analysis
- Create a support case with Sophos Support

SOPHOS

So what happens if the detection alert is still showing in Sophos Central? Let's consider the following scenarios.

The detection alert is still displayed in Sophos Central and in the Sophos Endpoint Agent. In this scenario, look for the detected file on the device. Does it still exist? If not, mark the alert as acknowledged in Sophos Central and run a full system scan to ensure the device is clean.

The detected file still exists on the device. In this scenario, delete the file from the detected location manually and run a full system scan to ensure the file has been removed and is not re-detected.

The detected file is unable to be deleted manually on the device. In this scenario, submit the file to Sophos for analysis and create a support case with Sophos Support for further investigation

### [Additional Information]

For further information about malware that is not cleaned up and alerts that remain in Sophos Central, please see knowledge base article **KB-000035335**. <https://support.sophos.com/support/s/article/KB-000035335>

## Device Isolation

Allows devices to be isolated while investigating a threat ensuring the network is protected whilst threats are cleaned up.

Administrators can choose to isolate a device during or following an investigation into detected threats.

Devices can isolate themselves automatically if their health status is red. This is configured in the threat protection policy and is not available for Server Protection.

SOPHOS

If you are investigating a detection that requires manual clean up, you want to ensure that the device where a threat has been detected cannot compromise any other devices on the network.

Isolating a device provides a way to remove a device from the network while investigation can be completed. This ensures that the network is protected whilst a threat is cleaned up on a specific device. You can still manage a computer from Sophos Central when it is isolated.

Isolation can be performed in two ways:

- An administrator can choose to isolate a device during, or following, an investigation into detected threats
- Devices can isolate themselves if their health status is red. This is configured using the Threat Protection policy. This is not available for Server Protection

Please note that the device isolation feature in Sophos Central is not currently supported for Linux or macOS devices.

# Admin Initiated Isolation

The screenshot shows the Sophos Central interface for a server named READING3. In the left sidebar, under 'Actions', the 'Isolate' button is highlighted with an orange box. A tooltip window titled 'Isolate server' appears, explaining that isolating limits network access but allows management from Sophos Central. It also provides a reason for isolation ('Investigate large number of threats') and two buttons: 'Cancel' and 'Isolate'.

**Server Protection - READING3**

Overview / Server Protection Dashboard / Servers / READING3

Sophos UK - Super Admin

**SUMMARY** EVENTS STATUS EXCLUSIONS APPLICATIONS POLICIES

Recent Events

Nov 2, 2022 6:35 PM Malware cleaned up: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1\_HighScore (1).zip\HighScore.exe'

Nov 2, 2022 6:35 PM Malware detected: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1\_HighScore (1).zip\HighScore.exe'

Nov 2, 2022 6:35 PM Malware cleaned up: 'EICAR-AV-Test' at 'http://www.sophos.com/eicar/index.html'

Nov 2, 2022 6:35 PM Malware detected: 'EICAR-AV-Test' at 'http://www.sophos.com/eicar/index.html' (Technical Support reference)

Nov 2, 2022 6:35 PM Malware cleaned up: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1\_HighScore.zip\HighScore.exe'

Scan Now Lock Down Diagnose Reset health status Live Response

READING3 Windows Server 2022 Standard Edition

Isolate Agent Summary Last Sophos Central Agent Scan

Isolate server

You're about to isolate this server. This limits its access to the network.

You can still manage the server from Sophos Central and you can remove it from isolation at any time.

Why are you isolating it?

Investigate large number of threats

35 of 400 characters.

Cancel Isolate

There are multiple ways to initiate device isolation. In this example, the device page is displayed, in the left-hand pane, the option to 'Isolate' the device is shown. The device needs to be online for the isolation request to be successful. You can still manage the device from Sophos Central when it is isolated.

# Admin Initiated Isolation

The screenshot shows the Sophos Threat Analysis Center interface for a detection named 'ML/PE-A'. The flow is visualized as a series of nodes connected by arrows:

- Device node: READING3, 192.168.1.166
- Root Cause node: Windows Explorer
- Beacon node: highscoore.exe
- Detection Status node: Detected on Nov 2, 2022 6:35 PM
- Cleaned status

**Summary** section 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 6:35 PM

**Suggested next steps** section:

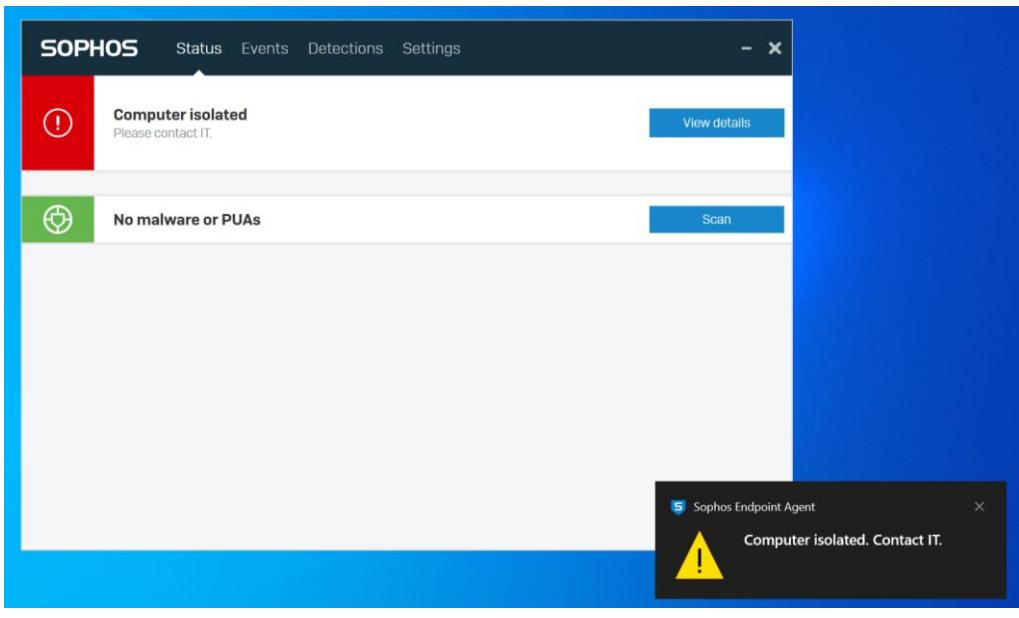
- Set a status for the threat graph
- Priority: Medium
- Status: New
- Isolate this device while you investigate (highlighted)
- Scan the device
- Run a Live Discover query

A green callout box highlights the 'Isolate this device while you investigate' option.

It is also possible to isolate a device from the 'Suggested next steps' section in a threat graph.

To access a threat graph, navigate to **Threat Analysis Center > Threat Graphs**.

## Admin Initiated Isolation



SOPHOS

The user of the device will see a toast message to notify them that their device has been isolated and the **Status** tab in the Sophos Endpoint Agent will also show 'Computer isolated'.

When device isolation is removed, the health status of the device will return to what it would have been before the administrator selected isolation. This may not be a green health status, depending on what was detected.

# Admin Initiated Isolation

The screenshot shows the Sophos Central interface for a server named 'READING3'. The top navigation bar includes 'Help', 'Training', and a user account for 'Sophos UK - Super Admin'. The main content area is titled 'Server Protection - READING3' with tabs for 'SUMMARY', 'EVENTS', 'STATUS', 'EXCLUSIONS', 'APPLICATIONS', and 'POLICIES'. On the left, there's a summary card for 'READING3 Windows Server 2022' showing 'Isolated by Admin' with a red exclamation mark icon. A green button labeled 'Remove from Isolation' is overlaid on this card. Below the card, a green callout box contains the text 'Remove a device from isolation on the device page'. The right side of the screen displays a 'Recent Events' log with the following entries:

Date	Action	Details
Nov 6, 2022 1:45 PM	Computer isolated by Training	
Nov 6, 2022 1:38 PM	Update succeeded	
Nov 2, 2022 6:35 PM	Malware cleaned up: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1_HighScore (1).zip\HighScore.exe'	D
Nov 2, 2022 6:35 PM	Malware detected: 'ML/PE-A' at 'C:\Users\Administrator\AppData\Local\Temp\2\Temp1_HighScore (1).zip\HighScore.exe'	D
Nov 2, 2022 6:35 PM	Malware cleaned up: 'EICAR-AV-Test' at 'http://www.sophostest.com/eicar/index.html'	D

SOPHOS

When a device is isolated, the health status of the device is set to red in Sophos Central. This status is shared with other Sophos Central products if Sophos Synchronized Security is enabled.

When investigations are complete, the device isolation can be removed.



Additional information in  
the notes

# Automatic Isolation

The screenshot shows the Sophos Central interface under the Threat Protection policy. The 'Device Isolation' section has a note: 'Allow computers to isolate themselves on red health' with a note: 'If a computer has red health, it will isolate itself from the network. It will still communicate with Sophos Central.' The 'Scheduled Scanning' section shows a schedule set for 02:00 PM on Saturday. The 'Exclusions' section shows no exclusions listed. A green callout box highlights the automatic isolation feature with the text: 'Configure automatic device isolation in the Threat Protection policy' and 'If a device health status changes to red, it is automatically isolated'.

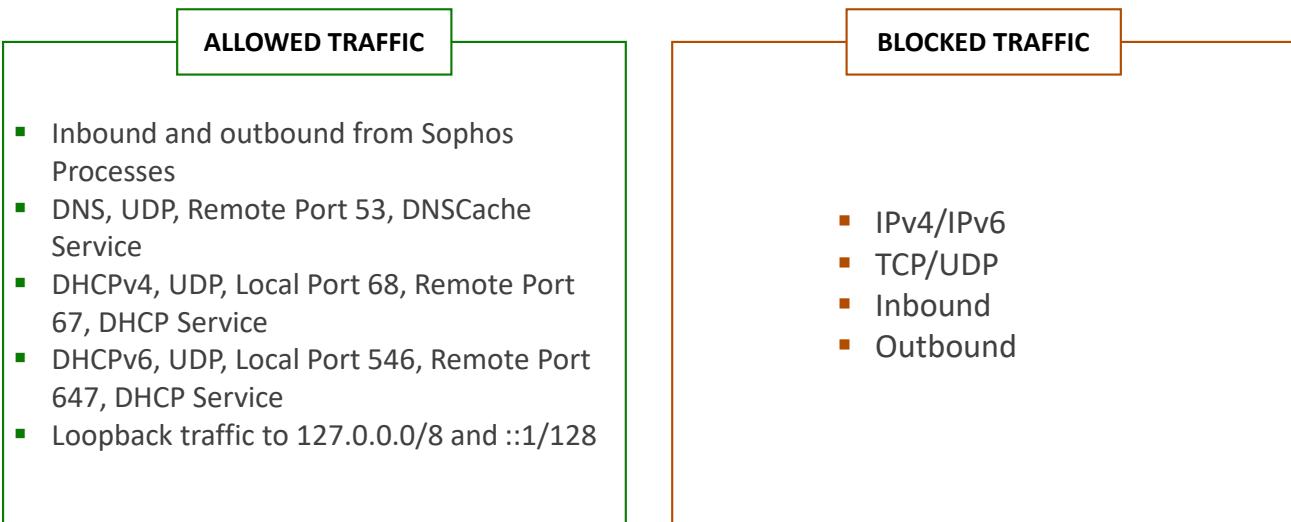
Devices can automatically isolate themselves based on their health status. If a device's health status is red, the device is automatically isolated from the network.

This setting is configured in the threat protection policy. To remove automatic isolation, the cause of the red health status on the device needs to be resolved.

## [Additional Information]

To view more information on what would cause a device's health status to change please see knowledge base article **KB-000035572**. <https://support.sophos.com/support/s/article/KB-000035572>

# Automatic Isolation Rules



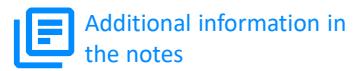
SOPHOS

Automatic isolation is designed so that Sophos processes are allowed for both inbound and outbound traffic. This allows communication between Sophos Central and an isolated device.

All DNS, DHCP and local loopback traffic is allowed, however, all other IPv4 and IPv6 TCP and UDP traffic is blocked.

Please note that ICMP traffic is not blocked, which means that ping will still work should this be required.

# Automatic Isolation Rules



```
C:\> netsh wfp show filters
```



```
<filterKey>(a17e9460-04bf-488e-be24-9e1dad021b29)</filterKey>
<displayData>
    <name>Self-Isolation exclusion IPv4 inbound</name>
    <description></description>
</displayData>
<flags numItems="1">
    <item>FWPM_FILTER_FLAG_INDEXED</item>
</flags>
<providerKey>(5680ca01-44a9-4726-b518-f3c295cf463c)</providerKey>
<providerData>
<layerKey>FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4</layerKey>
<subLayerKey>(Fc309a43-bd92-4x3-9a71-a95536beea3)</subLayerKey>
<weight>
    <uint64>65323</uint64>
</weight>
<filterCondition numItems="5">
    <item>
        <fieldKey>FWPM_CONDITION_IP_PROTOCOL</fieldKey>
        <matchType>FWPM_MATCH_EQUAL</matchType>
        <conditionValue>
            <type>FWP_UINT8</type>
            <uint8>17</uint8>
        </conditionValue>
    </item>
    <item>
        <fieldKey>FWPM_CONDITION_IP_LOCAL_PORT</fieldKey>
        <matchType>FWPM_MATCH_EQUAL</matchType>
        <conditionValue>
            <port>80</port>
        </conditionValue>
    </item>
    <item>
        <fieldKey>FWPM_CONDITION_MAC_ADDRESS</fieldKey>
        <matchType>FWPM_MATCH_EQUAL</matchType>
        <conditionValue>
            <macAddress>00:0C:29:00:00:00</macAddress>
        </conditionValue>
    </item>
    <item>
        <fieldKey>FWPM_CONDITION_IP_REMOTE_PORT</fieldKey>
        <matchType>FWPM_MATCH_EQUAL</matchType>
        <conditionValue>
            <port>443</port>
        </conditionValue>
    </item>
</filterCondition>
<conditions>
    <item>
        <name>Self-Isolation exclusion IPv4 inbound</name>
        <description><![CDATA[Self-Isolation Inbound TCP&UDP IPv4 filter]]></description>
    <item>
        <name>Self-Isolation exclusion IPv4 inbound</name>
        <description><![CDATA[Self-Isolation Inbound TCP&UDP IPv4]]></description>
    <item>
        <name>Self-Isolation exclusion IPv4 inbound</name>
        <description><![CDATA[Self-Isolation Inbound TCP&UDP IPv6 filter]]></description>
    <item>
        <name>Self-Isolation exclusion IPv4 outbound</name>
        <description><![CDATA[Self-Isolation Outbound TCP&UDP IPv6]]></description>
    </item>
</conditions>

```

You can review the rules that are applied for automatic isolation by running an elevated command shown here.

This will create a file in the current directory named filters.xml that contains information on all current network filters. You can search for the self-isolation rules to review the relevant rules.

### [Additional Information]

The command to view automatic isolation rules is: netsh wfp show filters



Additional information in  
the notes

## Automatic Isolation Exceptions

The screenshot shows the 'Add Exclusion' dialog box with the following fields:

- EXCLUSION TYPE:** Computer Isolation (Windows)
- DIRECTION:** Both
- LOCAL PORT:** 2
- REMOTE PORT:** 3
- REMOTE ADDRESS (IPv4, IPv6 or CIDR):** (empty field)
- Buttons at the bottom:** Cancel, Add Another, Add

Annotations with green boxes and arrows point to specific fields:

- An arrow points from a green box labeled "Local port" to the LOCAL PORT field.
- An arrow points from a green box labeled "Remote port" to the REMOTE PORT field.
- An arrow points from a green box labeled "Traffic direction" to the DIRECTION field.
- An arrow points from a green box labeled "Remote address or CIDR range" to the REMOTE ADDRESS field.

SOPHOS

Additionally, you can define exclusion rules for automatic isolation. These are configured as scanning exclusions. The rules can be configured based on:

- The traffic direction (inbound/outbound or both)
- The local port
- The remote port
- The remote address or CIDR range

### [Additional Information]

For information on the different options for computer isolation in Sophos Central, and the policy options see **KB-000038424**. <https://support.sophos.com/support/s/article/KB-000038424>

## Reject Network Traffic from Peers

 Requires Synchronized Security to be enabled

 Allowed traffic is based on a device's health status

 Peers reject network connections based on MAC addresses

SOPHOS

If you have a Sophos Firewall and have enabled Sophos Synchronized Security, peers can reject network traffic from any device with a red health status based on their MAC address. This will also include Linux and macOS devices.

The Sophos Firewall shares the list of MAC addresses that have a red health status with all devices that have a heartbeat with it. Those devices will reject traffic from MAC addresses on the list, isolating them from compromised devices.

# Reject Network Traffic from Peers

The screenshot shows the Sophos Central interface with the 'Global Settings' menu selected. Under 'General', the 'Reject Network Connections' setting is being configured. A green callout box highlights a note stating: 'Rejects connections to or from devices with red health or a missing security heartbeat'. Other visible notes include: 'Allow devices to reject connections from other devices with red health' and 'Note: This only applies to devices connected to a Sophos Firewall'. The 'Available' and 'Excluded' lists are shown below.

Available	Excluded
Search	Search
<input type="checkbox"/> AVAILABLE 27	<input type="checkbox"/> EXCLUDED 3
<input type="checkbox"/> AppServer	<input type="checkbox"/> DC
<input type="checkbox"/> DC	<input type="checkbox"/> READING3
<input type="checkbox"/> DESKTOP-CRQDC8A	<input type="checkbox"/> WinServer1
<input type="checkbox"/> linux-av	

This setting is configured as a **Global Setting** in Sophos Central, navigate to **Global Settings > General > Reject Network Connections**. Please note that this setting only applies to devices connected to a Sophos Firewall.

By default, all devices can be isolated. However, if there are specific devices you want to exclude from isolation you can add them to the 'Excluded' list. It is worth noting that any Update Caches and Message Relays are automatically excluded.

## Override the Isolation Status

 Turn off Tamper Protection

 Open Sophos Endpoint Agent and click **Settings**

 Select **Override Sophos Central Policy for up to 4 hours to troubleshoot**

 Turn off Network Threat Protection

SOPHOS

You can select to override the isolation status of a device by completing the following steps:

- Turn off Tamper Protection
- Open the Sophos Endpoint Agent and click **Settings**
- Select **Override Sophos Central Policy for up to 4 hours to troubleshoot**
- Turn off Network Threat Protection

Please note that these steps will remove the device from isolation for up to four hours. If isolation is still turned on by the administrator or the health of the device is still red at this point, it will return to an isolated state.



Additional information in  
the notes

## Sophos Scan & Clean

Get Started  
Download Now

Compatibility: For 32-bit and 64-bit versions of Windows  
Help: [Visit our support forum](#)

<https://www.sophos.com/en-us/free-tools/virus-removal-tool>

SOPHOS

Sophos provides a free tool that can be used as a second-opinion virus removal scanner for Sophos protected devices and for devices that do not have Sophos protection.

### [Additional Information]

Sophos scan & clean available for download here: <https://www.sophos.com/en-us/free-tools/virus-removal-tool>

# Sophos Scan & Clean

## Why use Sophos Scan & Clean?

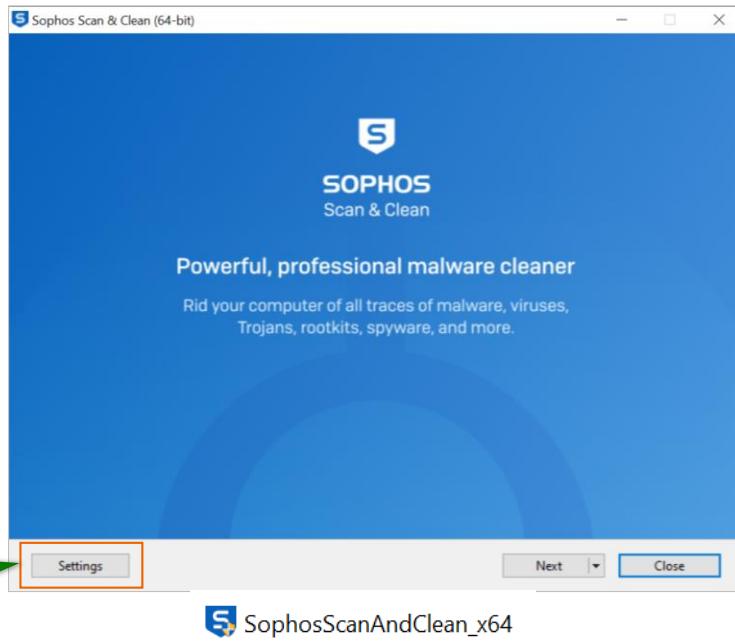
- It can detect and remove threats
- It can be used whilst the operating system is running
- It can block re-infection by protecting registry keys and file locations
- It can be downloaded and run whilst other anti-virus solutions are installed on a device
- No installation required; the downloaded file contains an executable that is run following the download

SOPHOS

For devices without Sophos protection, Sophos Scan & Clean can detect and remove threats. It works alongside existing anti-virus solutions and can remove viruses and threats while the operating system is running and can block re-infection by protecting registry keys and file locations.

There is no installation required; the tool can be downloaded from Sophos. The file contains an executable that is run following the download.

## Sophos Scan & Clean

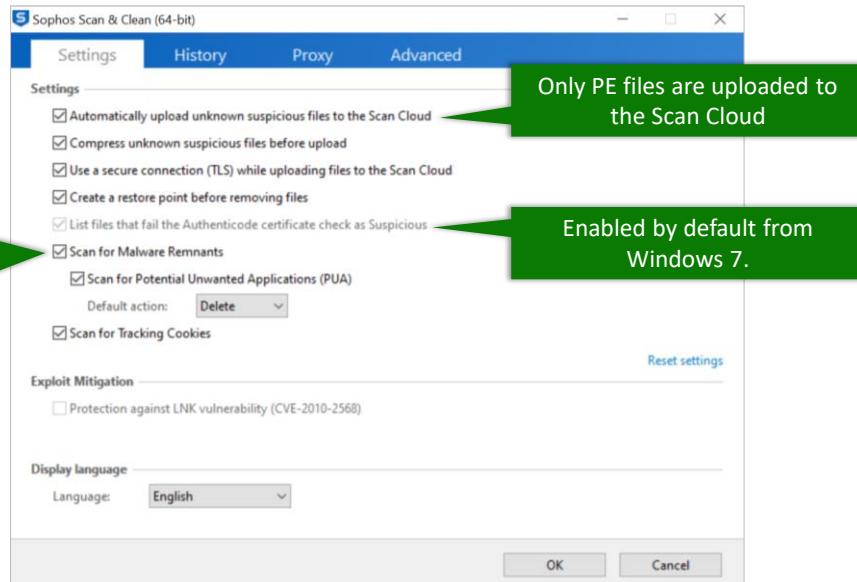


Once downloaded the tool can be launched. You can customize the settings used when running the tool if required.



Additional information in  
the notes

## Sophos Scan & Clean Settings



SOPHOS

The default settings are appropriate for most circumstances but can be modified if required. Some of the settings to note are:

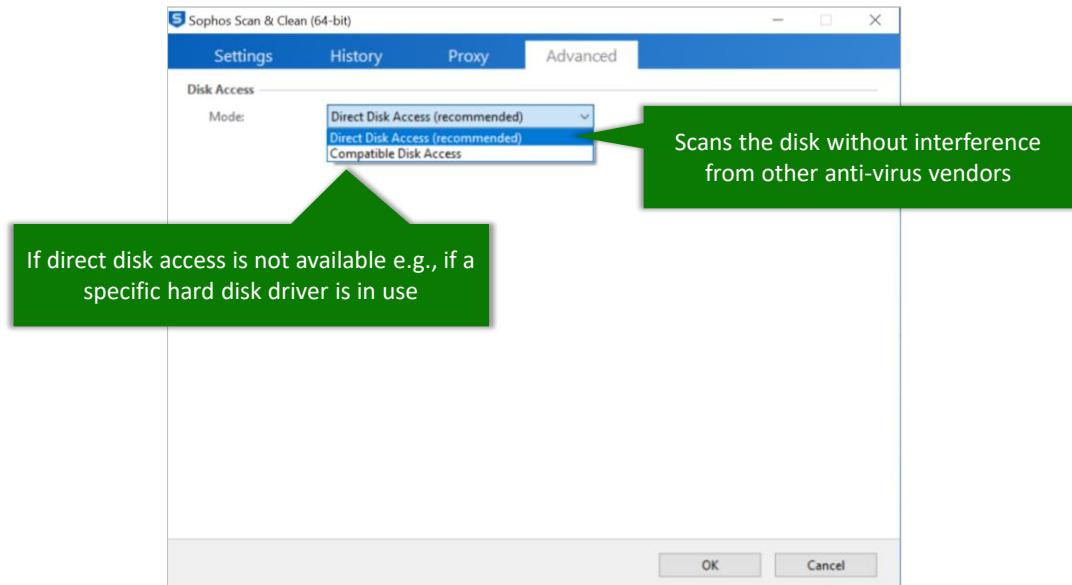
- The automatic upload of unknown suspicious files only includes portable executable files
- The 'List files that fail the Authenticode certificate check as Suspicious' setting is enabled by default for Windows 7 and above versions and cannot be unchecked
- Sometimes there are leftovers from malware like images or text files, 'Scan for Malware Remnants' will remove these

A full description of the settings is included in the quick guide, referenced in the notes and proxy configuration is supported.

### [Additional Information]

<https://community.sophos.com/free-tools/f/recommended-reads/130748/sophos-scan-clean-quick-guide>

## Sophos Scan & Clean Settings

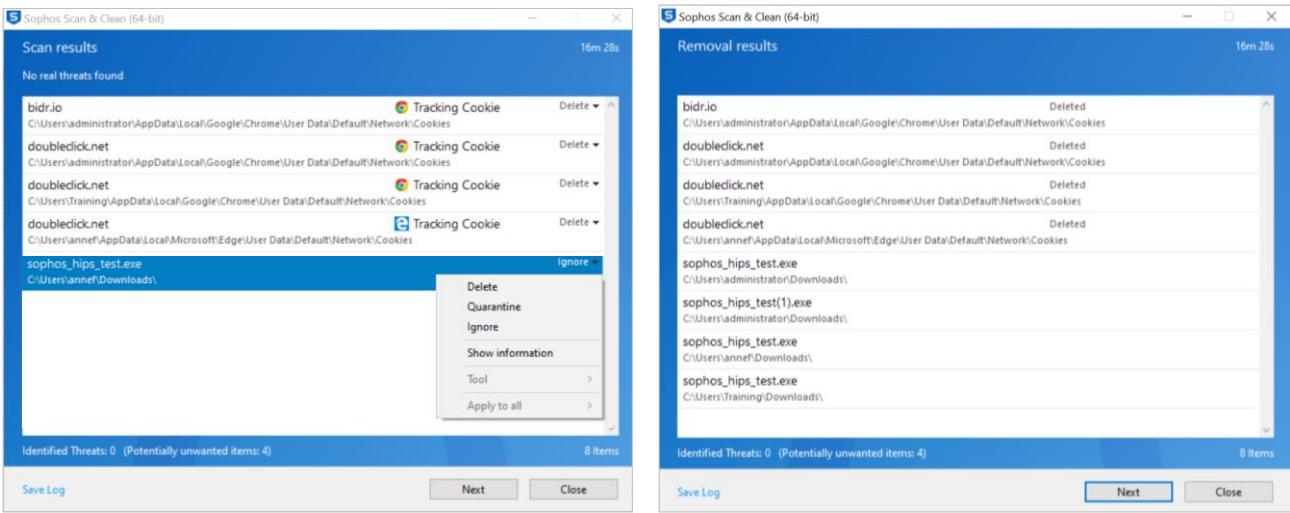


SOPHOS

The **Advanced** tab allows configuration of the disk access mode.

'Direct Disk Access' is recommended which scans the disk without interference from other anti-virus vendors. 'Compatible Disk Access' maybe required if direct disk access does not work on a specific device, for example if a specific hard disk driver is in use.

# Sophos Scan & Clean



SOPHOS

Once a scan is complete, any threats found are displayed with the suggested actions to take. Clicking the drop-down arrow will display an additional menu where you can select additional actions, for example, you can select to quarantine a detected file.

If you select to delete a detected file, it will be displayed in the removal results. A log file from the tool can be saved if required.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 4

Where is automatic device isolation configured in Sophos Central?

Global Settings > Device Isolation

Threat Protection Policy > Device Isolation

Threat Protection Policy > Health Status

Global Settings > Reject Network Connections

SOPHOS



## Question 2 of 4

Which 2 types of traffic are allowed when a device is isolated?

Traffic to Remote Port  
TCP 4444

DNS traffic

Traffic to Remote Port  
TCP 443

Inbound and outbound traffic from  
Sophos Processes

SOPHOS

## Question 3 of 4



All manual clean up steps have failed for a detected file.  
Which 2 steps are recommended?

Reboot the device

Run a full system scan

Submit a file sample to  
Sophos for analysis

Create a support case with  
Sophos Support

SOPHOS



## Question 4 of 4

Which of the following statements is true for Sophos Scan & Clean?

It automatically executes following a reboot

No installation is required

It cannot be used on devices that have existing anti-virus software installed

SOPHOS

# Chapter Review

Devices can be **isolated automatically**, or by an **administrator** whilst a threat is cleaned up. You can still manage the computer from Sophos Central.

A detection may require **manual clean up** if the **permissions** on the file **do not permit clean up** or if a threat is found in an **archive** or **mailbox**.

Sophos Scan & Clean **detects and removes threats**. It works alongside existing anti-virus, and **no installation is required**.

SOPHOS

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

Devices can be isolated automatically, or by an administrator whilst a threat is cleaned up. You can still manage the computer from Sophos Central.

A detection may require manual clean up if the permissions on the file do not permit clean up or if a threat is found in an archive or mailbox.

Sophos Scan & Clean detects and removes threats. It works alongside existing anti-virus, and no installation is required.



# Sophos Central XDR Data Lake APIs

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4520: Sophos Central XDR Data Lake APIs

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 Data Lake APIs

In this chapter you will learn how to make use of a Sophos Central API to run Data Lake queries.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to configure API credentials in Sophos Central
- ✓ How to enable Sophos Data Lake uploads
- ✓ How to access Live Discover queries
- ✓ How to edit and write Live Discover queries

DURATION     **6 minutes**

SOPHOS

In this chapter you will learn how to make use of a Sophos Central API to run Data Lake queries.

## Data Lake API Overview

The data lake can be queried as part of the Sophos Central APIs

Authenticated RESTful API using JSON

Requires API credentials for authentication

SOPHOS

The Sophos Data Lake can be queried using Sophos Central APIs. All the APIs are RESTful using standard authentication, JSON requests and response, and standard HTTP verbs.

The use of APIs requires that you have a set of API credentials configured in Sophos Central, and all communication is over HTTPS.

# Create API Credentials

The screenshot shows the Sophos Central Global Settings page. 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), Protect Devices, and Account Health Check. Under MY PRODUCTS, there are Endpoint Protection, Server Protection, Mobile, and Encryption options. The main content area is titled "Global Settings" with the subtitle "Manage your settings". It contains sections for Administration, Directory service, Role Management, API Token Management, and API Credentials Management (which is highlighted with an orange box). Below these are Sophos sign-in settings and Verify domains. A modal window titled "Add credential" is open, prompting for a "Credential name\*" (set to "Data Lake"), a "Description" (set to "Credentials for Data Lake API"), and a "Role\*" (set to "Service Principal Super Admin"). There's also a "Notes:" section with instructions about generating Client ID and Client Secret, and a note about expiration. At the bottom of the modal are "Cancel" and "Add" buttons.

API Credentials are added in **Global Settings**. When you add a new credential, a 'client ID' and 'client secret' are created which are used by the API for Sophos Central authentication.

# Create API Credentials

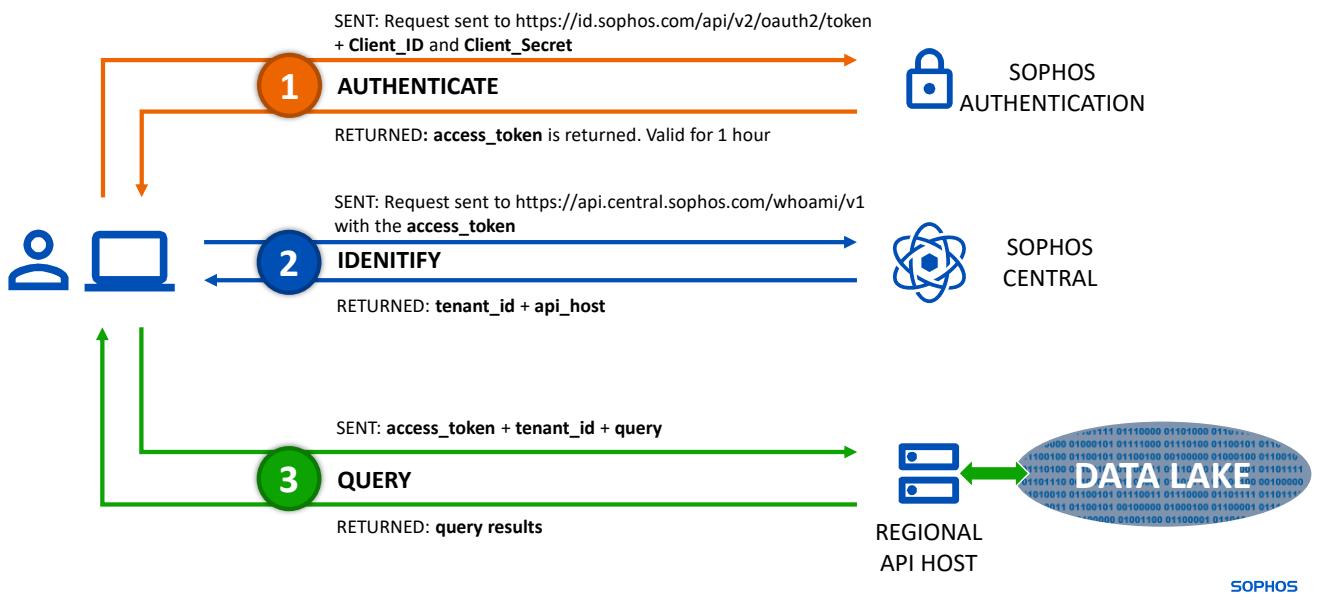
The screenshot shows the Sophos Central interface. On the left is a dark sidebar with various navigation options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings (which is selected), Protect Devices, and Account Health Check. Under MY PRODUCTS, there are links for Endpoint Protection, Server Protection, Mobile, and Encryption. The main content area is titled "Data Lake" and shows the "API Credential Management / Data Lake" page. It displays an "API credential summary" for "Data Lake" with the following details:

Name	Data Lake
Created on	Aug 26, 2022
Expires on	Aug 25, 2025
Last used	Aug 29, 2022
Description	Credentials for Data Lake API
Client ID	6f76d484-[REDACTED]38bdf838
Client Secret	For security purposes, the Client Secret cannot be shown again. If need be, you may create a new API credential.
Role	Service Principal Super Admin

A blue "Delete" button is located in the top right corner of the main content area.

The 'client ID' and 'client secret' are usually required when configuring an API and so the details must be copied from Sophos Central. Remember that the client secret is only shown once. If you did not view the client secret when it was available, you will need to re-create the API to get a new client ID and client secret.

# Data Lake API Overview



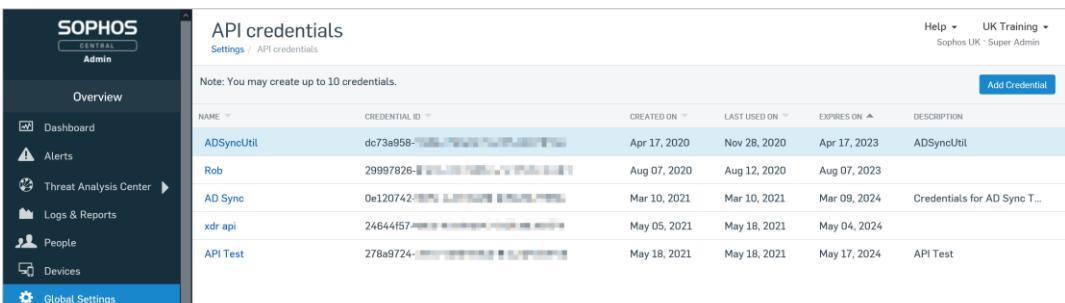
Using the API can be broken down into three phases.

First, you need to authenticate to get an access token. A request is sent for an access token with the client ID and client secret of the API credentials you have created. The access token returned is valid for 1 hour, after that you need to request a new token. Please note that the access token can also be referred to as a 'JWT', a JSON Web Token.

Next, you need to identify your tenant ID and the API host. A request is sent with the access token. The tenant ID and API host information are returned from Sophos Central. Please note that the tenant ID and API host do not change, so this step only needs to be completed once.

Finally, you can start to query the Data Lake. The access token and tenant ID are sent with every request. Following the first request, the response will contain a run ID. You can make subsequent requests to check on the progress of the query. Once the query is complete you can request the results. Queries are available for two hours from when they are first made, and the expiration time can be found in the status of the run ID.

# Step One: Authenticate



The screenshot shows the Sophos Central Admin interface with the 'API credentials' page selected. The table lists five entries:

NAME	CREDENTIAL_ID	CREATED ON	LAST USED ON	EXPIRES ON	DESCRIPTION
ADSyncUtil	dc73a958-[REDACTED]	Apr 17, 2020	Nov 28, 2020	Apr 17, 2023	ADSyncUtil
Rob	29997826-[REDACTED]	Aug 07, 2020	Aug 12, 2020	Aug 07, 2023	
AD Sync	0e120742-[REDACTED]	Mar 10, 2021	Mar 10, 2021	Mar 09, 2024	Credentials for AD Sync T...
xdr api	24644157-[REDACTED]	May 05, 2021	May 18, 2021	May 04, 2024	
API Test	278a9724-[REDACTED]	May 18, 2021	May 18, 2021	May 17, 2024	API Test

Below the table, two command-line examples are shown:

```
curl -XPOST -H "Content-Type:application/x-www-form-urlencoded" -d "grant_type=client_credentials&client_id=<client-id>&client_secret=<client-secret>&scope=token" https://id.sophos.com/api/v2/oauth2/token
```

```
curl -XPOST -H "Content-Type:application/x-www-form-urlencoded" -d "grant_type=client_credentials&client_id=278a9724-[REDACTED]-9d23-95c21e530a46&client_secret=1d0d1519bf3f575261ca62d9f2d511761a8073c9[REDACTED]24d5d203868457b6345702b068d488c6bb3b8cc7e3a81&scope=token" https://id.sophos.com/api/v2/oauth2/token
```

You can make API calls using various tools including cURL and Postman. We will use cURL to demonstrate how an API call works.

In this example, we are running the first API call to request and receive the access token.

## Step One: Authenticate

```
curl -XPOST -H "Content-Type:application/x-www-form-urlencoded" -d  
"grant_type=client_credentials&client_id=278a9724-...-9d23-  
95c21e530a46&client_secret=1d0d1519bf3f575261ca62d9f2d511761a8073c  
24d5d203868457b6345702b068d488c6bb3b8cc7e3a81&scope=token"  
https://id.sophos.com/api/v2/oauth2/token  
{"access_token":  
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjF1aXNtSjFSZmIwRWJqYjJ6dy01LVhTNlFiY  
XBaZWtOcVpsVU51TVdac2cifQ.4WAImHvq81BT4ceeHiiRhH7kb1HQVKpoTuOh5ch_e4AFZ3JRsQHJYRcr  
osn_zrNhGZNi4zZQNcpfSeIFreDDT60udDUnV7IQBrNgtIsJuhoY9lnMtw", "errorCode":  
"success", "expires_in": 3600, "message": "OK", "refresh_token":  
"8222c75a10270fa2af58f43...999d599074e2fcbbeb780bb2985fb0244bf395", "token_type":  
"bearer", "trackingId": "950f-1840-45d9-aec3-c08fd13eeaed"}
```

The bearer access token is returned for this API call

SOPHOS

The authentication API call returns the access token that is valid for one hour. This can be used as many times as required within the one-hour period.

Please note that we have truncated the response in this example.

## Step Two: Identify

```
curl -XGET -H "Authorization: Bearer <jwt>" https://api.central.sophos.com/whoami/v1
```

<jwt> is replaced with the access token

```
curl -XGET -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjFIaXNtSjFSZmIwRWJqYjJ6dy01LVhTN1FiYXBaZWt0cVpsVU51TVdac2cifQ.4WAImHvq81BT4ceeHiiRhH7kblHQVKpoTuOh5ch_e4AFZ3JRsQHJYRcrosn_zrNhGZNi4zzQNcpfSeIFreDDT60udDUnV7IQBrNgtIsJuhoY9lnMtw"  
https://api.central.sophos.com/whoami/v1  
{"id":"0123456a-78b9-012cd-3456-ef78g9012345h","idType":"tenant","apiHosts":{"global":"https://api.central.sophos.co  
m","dataRegion":"https://api-eu01.central.sophos.com"}}
```

The tenant ID and data region are returned.

SOPHOS

Now we have the access token, we can discover the tenant ID. Please note that 'jwt' is used in this example as a representation of the access token.

The tenant ID and the data region API host are highlighted in orange in the results. We can now start running queries.

## Step Three: Query

```
python -c 'import json;  
print(json.dumps(dict(adHocQuery=dict(template=open("query.sql").read().strip()))),in  
dent=2))' > request.json
```

```
$ curl -XPOST -H "Content-Type:application/json" -H "Authorization:bearer <jwt>" -H  
"X-Tenant-ID:<tenant-id>" -d @request.json <data-region>/xdr-query/v1/queries/runs  
{"id":"6e1b4a36-e61a-46ca-937f-473840d08b4a",  
"createdAt":"2021-05-18T09:40:18.181Z",  
"createdBy":"24644f57-4a63-4016-aa49-6d7bed989f74",  
"expiresAt":"2021-05-18T11:40:18.202Z",  
"result":"notAvailable",  
"status":"pending"
```

The converted SQL query is used to return the run ID. The expiry date and time of the request is returned along with the status

SOPHOS

Any SQL queries you use will need to be converted to JSON to be used with the API. Python can be used to read the SQL query from ‘query.sql’ and create a JSON request. In our example, the file is named ‘request.json’.

In the second command shown here, we are requesting the run ID.

## Step Three: Query

```
curl -XGET -H 'Content-Type: application/json' -H 'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtp' -H 'X-Tenant-ID: 0123456a-78b9-012cd-3456-ef78g9012345h' https://api-eu01.central.sophos.com/xdr-query/v1/queries/runs/6e1b4a36-e61a-46ca-937f-473840d08b4a
{
  "id": "6e1b4a36-e61a-46ca-937f-473840d08b4a",
  "createdAt": "2021-05-18T09:40:18.181Z",
  "createdBy": {"id": "24644f57-4a63-4016-aa49-6d7bed989f74"},
  "type": "user",
  "accountId": "0123456a-78b9-012cd-3456-ef78g9012345h",
  "accountType": "tenant",
  "expiresAt": "2021-05-18T11:40:18.527Z",
  "finishedAt": "2021-05-18T09:40:19.044Z",
  "result": "succeeded",
  "status": "finished",
}
```

Check the status of a query using the run ID

SOPHOS

Now we have the run ID, it can be used to check if the request has finished and also to return the results of the query.

To check on the status of the request, we run the API call shown here. In our example, the status is 'finished'.



Additional information in  
the notes

## Step Three: Query

```
curl -XGET -H 'Content-Type: application/json' -H 'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtp' -H 'X-Tenant-ID: 0123456a-78b9-012cd-3456-ef78g9012345h' https://api-eu01.central.sophos.com/xdr-query/v1/queries/runs/6e1b4a36-e61a-46ca-937f-473840d08b4a/results
{"items": [{"broadcast": "", "meta_mac_address": "00:0d:3a:25:7f:fb", "meta_public_ip": "20.86.157.251", "upload_size": 860, "osquery_action": "added", "unix_time": "2021-05-18T15:29:48.000Z", "endpoint_id": "c2beda92-1893-4d40-b263-ea08970a939f", "epoch": 1621329207, "interface": "5", "mac": "00:0d:3a:25:7f:fb", "meta_boot_time": 1621329097, "query_name": "network_interfaces", "meta_ip_mask": "255.255.255.0", "obytes": 81428307, "meta_query_pack_version": "1.2.1.15", "mask": "ffff:ffff:ffff:fff:f:", "address": "fe80::1d15:d232:490f:ac1", "meta_os_version": "10.0.17763", "meta_ip_address": "10.0.9.6", "ibytes": 886310121, "meta_endpoint_type": "server", "counter": 0, "meta_eid": "c2beda92-1893-4d40-b263-ea08970a939f", "calendar_time": "2021-05-18T15:29:48.000Z", "meta_os_name": "Microsoft Windows Server 2019 Datacenter", "mtu": 1500, "host_identifier": "A11DC8D4-B68B-4CFC-A822-85684717A883", "meta_os_platform": "windows", "numerics": false, "customer_id": "5550411b-07d2-48bd-9679-bc09a660403d", "ep_name": "Server1"}},
```

SOPHOS

We return the results of the query by running the API call and appending it with /results. You can optionally add a maximum size statement so that the query will only return a specified amount of data.

The results of any query run are kept for 2 hours. In our example, the results of one endpoint are displayed.

### [Additional Information]

Use ?maxSize=1000 to minimize the amount of data returned

Use /results to return the results of a query

## Learn More

The screenshot shows the Sophos Central APIs landing page. At the top, there's a blue header bar with the Sophos logo on the left and navigation links for 'GETTING STARTED', 'DOCS', 'APIS', and 'WHAT'S NEW?' on the right. Below the header is a large title 'Sophos Central APIs' with a subtitle 'Automate Your Security & Management Workflows'. There are three main call-to-action boxes: 'Getting Started' (with a 'READ THE GETTING STARTED GUIDE' button), 'How Our APIs Work' (with a 'READ BACKGROUND DOCS' button), and 'API Documentation' (with a 'VIEW API REFERENCE' button). The background features a stylized gear and circuit board pattern.

Sophos have a dedicated site with information about Sophos Central APIs. You can also view a webinar where we introduce coding against the Data Lake API.



Additional information in  
the notes

## Learn More

See the **Sophos Central API** on-demand technical training course

On Demand Technical Training

Courses		Type	Status
<input type="checkbox"/> Cybersecurity Essentials			
<input type="checkbox"/> Email			
<input type="checkbox"/> Encryption			
<input type="checkbox"/> Endpoint Protection	<input type="checkbox"/> ET06 - Intercept X Advanced with EDR <input checked="" type="checkbox"/> ET07 - Sophos Central API v1.0 <input type="checkbox"/> ET08 - Sophos Enterprise Console to Sophos Central Migration <input type="checkbox"/> ET09 - EDR v3.0	Elective	In Progress
<input type="checkbox"/> Firewall			
<input type="checkbox"/> Mobile			
<input type="checkbox"/> Wireless			

SOPHOS

You can find more information on getting started with our Sophos Central APIs in the on demand technical training course in the portal.

### [Additional Information]

Sophos Central API site: <https://developer.sophos.com/intro>

Introduction to XDR API webinar: <https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/b/announcements/posts/edr-data-lake-api-intro-webinar>

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

Which 2 pieces of information are required for an API to authenticate with Sophos Central?

Client ID

Client Secret

Tenant ID

Access Token

SOPHOS



## Question 2 of 2

How long is an API access token valid for?

30 minutes

1 hour

1 day

Indefinitely

SOPHOS

# Chapter Review

The Sophos Data Lake can be queried using Sophos Central APIs. All APIs are JSON requests using standard HTTP verbs.

The use of APIs requires a set of API credentials configured in Sophos Central and all communication is over HTTPS.

The results of an API Data Lake query are retained for 2 hours.

SOPHOS

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

The Sophos Data Lake can be queried using Sophos Central APIs. All APIs are JSON requests using standard HTTP verbs.

The use of APIs requires a set of API credentials configured in Sophos Central and all communication is over HTTPS

The results of an API Data Lake query are retained for 2 hours.



# Sophos Central XDR Live Discover Query Pivoting

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4535: Sophos Central XDR Live Discover Query Pivoting

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 Pivoting

In this chapter you will learn what the results of a Live Discover query look like and how you can pivot these results to gain further information and insight.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to select and run Live Discover queries

DURATION     **5 minutes**

SOPHOS

In this chapter you will learn what the results of a Live Discover query look like and how you can pivot these results to gain further information and insight

# Query Results

**SOPHOS**

Threat Analysis Center

DETECTION AND REMEDIATION

- Dashboard
- Threat Graphs
- Live Discover**
- Detections
- Investigations
- Integrations
- Preferences

Detections (Windows) query results

6 / 6 Devices completed

Export

epName	date_time	detection_name	threat_type	threat_source	item_type	detector
WinClient5	2022-10-03T09:17:...	EICAR-AV-Test	Malware	VDL	File	C:\Users\...
WinClient5	2022-10-01T13:02:...	Eventing Command...	App	VDL	File	C:\Wind...
WinClient5	2022-10-01T13:03:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:07:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:09:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:09:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:52:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:54:...	Eventing Command...	App			

Run Query

The query results for any Live Discover query run are grouped and presented in a table which can be exported if required.

Let's have a look at how these results can be used to gain further insight.

# Pivoting Options

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, there's a sidebar with navigation links: Dashboard, Threat Graphs, Live Discover (which is selected and highlighted in blue), Detections, Investigations, Integrations, and Preferences. The main area is titled "Detections (Windows) query results" and shows a table of data. The table has columns: epName, date\_time, detection\_name, threat\_type, threat\_source, item\_type, and detectorid. There are 6 devices completed. A tooltip with a green background and white text appears over the ellipsis menu in the first row of the table, stating: "The ellipsis indicates that pivot options are available". The table contains 10 rows of data, mostly from WinClient5 and WinClient2, with various detection details like EICAR-AV-Test, Eventing Command..., Malware, VDL, File, and specific file paths.

epName	date_time	detection_name	threat_type	threat_source	item_type	detectorid
WinClient5	2022-10-03T09:17:...	EICAR-AV-Test	Malware	VDL	File	C:\Users\...
WinClient5	2022-10-01T13:02:...	Eventing Command...	App	VDL	File	C:\Wind...
WinClient5	2022-10-01T13:07:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:09:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:09:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:15:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:52:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:54:...	Eventing Command...	App			

Additional options available in the results are referred to as pivoting options. Pivoting allows administrators to look at the contents of a returned set of data and identify if it's something they want to perform additional actions on.

In the results table, the ellipsis menu indicates that there are pivoting options available.

# Pivoting Options

SOPHOS

Threat Analysis Center

DETECTION AND REMEDIATION

- Dashboard
- Threat Graphs
- Live Discover**
- Detections
- Investigations
- Integrations
- Preferences

Detections (Windows) query results

6 / 6 Devices completed

Export

epName	date_time	detection_name	threat_type	threat_source	item_type	detector
WinClient5	2022-10-03T09:17:...	EICAR-AV-Test	Malware	VDL	File	C:\Users\...
WinClient5	2022-10-01T13:02:...	Eventing Command...	App	VDL	File	C:\Wind...
WinClient5	2022-10-01T13:03:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:07:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:09:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient5	2022-10-01T13:15:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:52:...	Eventing Command...	App	VDL	File	C:\Windo...
WinClient2	2022-10-06T14:54:...	Eventing Command...	App			

Run Query

The pivoting options are context aware and will only display options that are available for the variable. In this example, the options for the endpoint name allow the administrator to select from a list of Data Lake queries. They can also scan the device or start a Live Response session.

# Pivoting Options

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists navigation options: Threat Analysis Center, DETECTION AND REMEDIATION (Dashboard, Threat Graphs, Live Discover, Investigations, Integrations, Preferences), and a general Sophos logo. The 'Live Discover' option is currently selected and highlighted in blue. The main content area is titled 'Detections (Windows) query results' and shows a table of query results. The table has columns: detection\_item, status, sophos\_pid, cmd\_line, detection\_thumbprint, username, sid, monitor\_mode, and priority. A tooltip is displayed over the 'detection\_thumbprint' column, providing information about enrichment links to third-party websites like VirusTotal. The tooltip content is as follows:

detection_item	status	sophos_pid	cmd_line	detection_thumbprint	username	sid	monitor_mode	priority
C:\Program File...	Not Cleaned			391c0dee0067...			0	{"c"
C:\Windows\Sy...	Not Cleaned			a7354b9c6297...			0	{"c"
C:\Windows\Sy...	Not Cleaned						0	{"c"
C:\Windows\Wi...							0	{"c"
C:\Windows\Wi...							0	{"c"
C:\Windows\Sy...							0	{"c"
C:\Windows\Sy...							0	{"c"
C:\Windows\Sy...							0	{"c"
C:\Windows\Sy...							0	{"c"
C:\Users\Traini...	Cleaned			275a021bbfb64...	SYSTEM	S-1-5-18	0	{"c"
C:\Windows\Sy...	Not Cleaned			1256a1e89815a...				

Queries

- Data lake queries
  - Find Emails with a specific Attachment - SHA256 (Data Lake)
  - Find Emails with Attachments (Data Lake)
  - Firewall: Threats detected and their location
- Live Discover queries
  - Events involving a SHA-256
  - Processes matching SHA-256 hashes in the last 30 days
  - Search for processes (Windows)

Enrichments

Third party

These links go to third-party websites, and Sophos isn't responsible for any product, service or content at these websites.

VirusTotal lookup

Run Query

Pivoting actions also allow administrators to navigate from the result of one query to either initiate a new query or enrich the data in the results.

Enrichments are a list of links to third-party websites like VirusTotal which can provide additional information about a potential threat you've found.



Additional information in  
the notes

## Pivoting Options

The screenshot shows the 'Queries' section of the Live Discover interface. It displays two main sections: 'Data lake queries' and 'Live Discover queries'. Under 'Data lake queries', there is one entry: 'Process activity (Data Lake)'. Under 'Live Discover queries', there are four entries: 'File system interactions for a SophosP...', 'Network interactions for a SophosP...', 'Process activity history', and 'Process details for a Sophos PID'. A green callout box points to the 'Live Discover queries' section with the text: 'In this example, the available pivots displayed are those that can use the Sophos PID'. Another green callout box points to the 'Process details for a Sophos PID' entry with the text: 'Available pivots are determined by the variable type of the query being run'. At the top of the interface, there is a configuration panel for a variable named 'sophos\_pid'.

Descriptive name	Variable type	SQL variable name	Note
sophos_pid	sophosPID	\$\$sophos_pid\$\$	*Enter value to use when query runs 5000

The list of available queries is determined by the variables used in queries already in the system, both queries provided by Sophos and those created by you. This works by associating the variable to one of the available pivot types. When a query is edited or created, the variables used are automatically updated.

For example, if you have a query that will identify the Sophos Process ID, this value can be set as a variable which will become available as a pivotable value.

Over time, Sophos will add additional pivot types, and these will be displayed as available variables. Along with this, as many queries and pivot types are developed, we will also introduce a pivot management function.

### [Additional Information]

A video explaining these new features can be found here: <https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/b/announcements/posts/live-discover-pivoting>

# Pivoting

The screenshot shows the Threat Analysis Center - Live Discover interface. On the left, a sidebar titled 'Queries' lists various pivoting options, including 'Data lake queries indicators (Data Lake)', 'Find common privilege escalation threat indicators (Data Lake)', 'Linux runtime detection details by detection ID (Data Lake)', 'Linux runtime detections by MITRE tactic (Data Lake)', 'MITRE impact threats (Data Lake)', 'Process activity on a device (Data Lake)', 'Process tree from Sophos PID (Windows)', and 'Windows detections (Data Lake)'. A green callout box points to this sidebar with the text: 'The pivot query is launched in a new Internet browser tab'. In the main area, the title 'Threat Analysis Center - Live Discover' is displayed above the 'Live Discover' section. The query 'Process activity on a device (Data Lake)' is selected. A green callout box points to the 'device\_name' variable input field with the text: 'The value for device\_name has been automatically inserted into the query'. The input field contains 'Training-W10'. The bottom right corner of the interface features the 'SOPHOS' logo.

When you select a query to run from the available pivoting options, a new Internet browser tab will be opened.

If you select a Data Lake pivoting query, in the new browser tab you will see the new query is ready to run. The variable data is automatically populated in the query.

# Pivoting

## Threat Analysis Center - Live Discover

Overview Threat Analysis Center Dashboard / Live Discover

Designer Mode  
Lets you create or edit queries

Query :  Search for processes (Windows)

[Back to categories / Processes](#)

Search for processes (Windows)

Processes: Search for processes (Windows)

Lists processes that match entries in your specified search terms

Created by Sophos

Sources  
 Windows

Expected system impact

No system impact data available.. To get system impact data, run the query on one device to test it.

Variables

Descriptive name	Enter value to use when query runs
parent_sophos_pid	You can use % as a wildcard 275a021bbfb6489e54d47189f
sha256	You can use % as a wildcard
user_name	You can use % as a wildcard
search_term	You can use % as a wildcard
start_time	<input type="text"/>
end_time	<input type="text"/>

Device selector (14 Endpoints available)

3 Endpoints selected

[Available devices](#) [Selected devices](#)

[Run Query](#)

SOPHOS

Variable values may have to be entered to run the query  
% can be used as a wildcard

This shows an example of a Live Discover pivot query. Again, a new Internet browser tab is opened.

The variable data is automatically added for you; however, additional variable information may be required. For example, dates or limit conditions. The percent symbol can be used as a wildcard.

For Endpoint Live Discover queries, the devices that were selected for the original query can be modified if required.

## Enrichments

**Enrichments**  
These links go to third-party websites, and Sophos isn't responsible for any product, service or content at these websites.

[VirusTotal lookup](#)

The screenshot shows the VirusTotal analysis interface for a specific file hash. At the top, a large red circle displays a score of 63 out of 67. Below the score, the file's SHA-256 hash is listed: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f. To the right, the file size is 68 B, the upload date is 2022-08-27 17:30:06 UTC, and it was uploaded 1 minute ago. A 'TXT' button is available for viewing the raw report. Below the main information, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 30+ entries). The DETECTION tab is selected, showing 'Security Vendors' Analysis' with the following table:

Vendor	Detection	Engine	Details
Ad-Aware	EICAR-Test-File (not A Virus)	AhnLab-V3	Virus/EICAR_Test_File
Alibaba	Trojan:MacOS/eicar.com	ALYac	Misc.Eicar-Test-File
Antiy-AVL	Trojan/Generic.ASMalwRG.118	Arcabit	EICAR-Test-File (not A Virus)
Avast	EICAR Test-NOT Virus!!!	Avast-Mobile	Eicar

If you select an available enrichment, you will be re-directed to a third-party website.

In this example, a new Internet browser tab was opened to the virustotal.com website that provides additional information on the detection.

Please note that Sophos is not responsible for any product, service or content on these websites.

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!

## Question 1 of 2

What symbol can be used as a wildcard entry for a query variable?

\_\_\_\_\_



## Question 2 of 2

Which 2 of the following are actions that can be performed from pivot options?

Scan this device

Wipe a device

Uninstall the Sophos  
Endpoint Agent

Start a Live Response  
session

SOPHOS

# Chapter Review

Pivoting options are context aware based on the type of data requested in the query.

The pivoting options include running Endpoint Live Discover and Data Lake queries and linking to third party websites to gain more insight into a detection or behaviour.

Actions can be taken using the pivoting actions available like scanning a device or starting a Live Response session.

SOPHOS

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

Pivoting options are context aware based on the type of data requested in the query.

The pivoting options include running Endpoint Live Discover and Data Lake queries and linking to third party websites to gain more insight into a detection or behaviour.

Actions can be taken using the pivoting actions available like scanning a device or starting a Live Response session.



# Writing Queries for Sophos Central XDR Live Discover

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4540: Writing Queries for Sophos Central XDR Live Discover

September 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.

# Writing Queries for Sophos Central XDR Live Discover

In this chapter you will learn how to create new Live Discover queries including how to find the available data and construct, save, and run a simple SQL query.

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ What Live Discover is
- ✓ How to run a Data Lake and Endpoint Live Discover query
- ✓ How to edit an existing query

DURATION **7 minutes**

SOPHOS

In this chapter you will learn how to create new Live Discover queries including how to find the available data and construct, save, and run a simple SQL query.

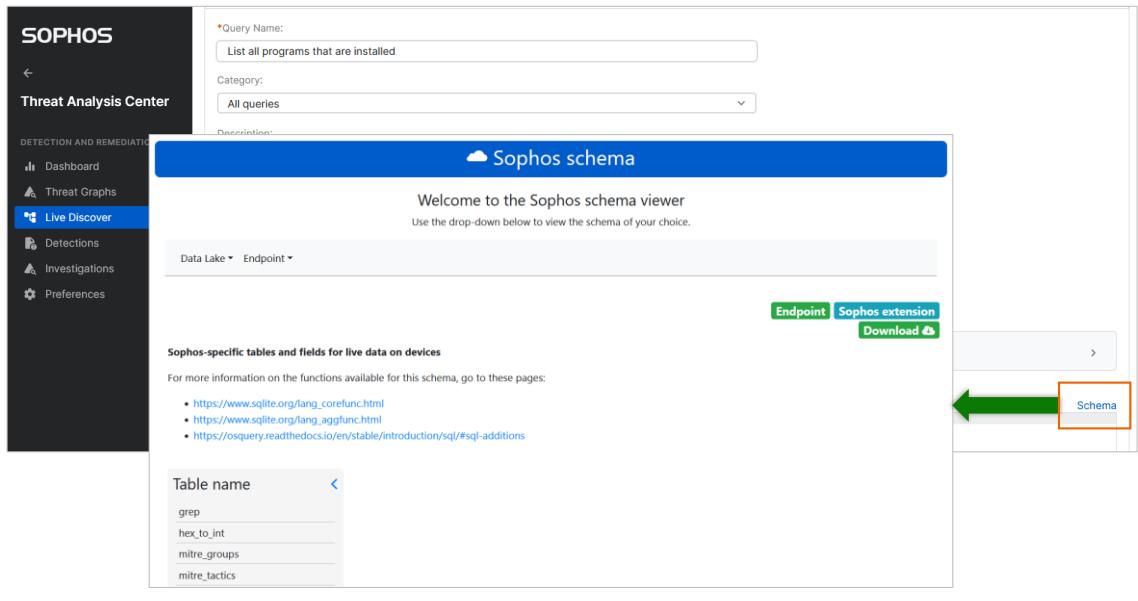
# Get To Know Your Data

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. The left sidebar has a dark theme with white text. It includes sections for DETECTION AND REMEDIATION: Dashboard, Threat Graphs, Live Discover (selected), Detections, Investigations, and Preferences. The main content area is titled "Threat Analysis Center - Live Discover" and shows a "Designer Mode" toggle switch which is turned on. Below it, there's a search bar and a message: "Query : Select One - 18 Categories, 335 Queries". There are three tabs: All Queries (selected), Endpoint Queries, and Data Lake Queries. A note says: "Queries that get data from devices or from the Data Lake. 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." The main area is divided into several sections with icons and counts: All queries [335] (All available queries), Recent queries [18] (Queries run recently), Anomalies [0] (Unexpected activity or network connections), ATT&CK [26] (Queries based on attack tactics and techniques), Cloud Optix [0] (Public cloud activity logs), Compliance [44] (Compliance with security standards), Device [44] (Device OS, patches, services and more), Email [7] (Email and messaging activity), Events [28] (Events in the system events logs), Files [9] (File details and file accesses), Microsoft 365 [10] (Audit logs from Microsoft 365), Mobile [20] (Mobile devices and apps), Network [56] (Network connections and data transfers), Other queries [32] (All other queries), and Processes [89] (Process activity and reputations). A "Run Query" button is at the bottom right.

There may be circumstances where you want to create your own Live Discover queries. Before you begin writing queries, it is useful to understand what data is available to you.

The first step is to enable designer mode as this is how you can edit queries and view the SQL used for each query.

# Get To Know Your Data



When you create a new query or edit an existing query, you can access the Sophos schema viewer. To do this, click **Schema**. This option will be in the top-right corner of the SQL used for the query.

Here you can view the available data tables for both Data Lake and Endpoint queries.



Additional information in  
the notes

# Get To Know Your Data

The screenshot shows the Sophos schema viewer interface. At the top, there's a blue header bar with the text "Sophos schema" and a cloud icon. Below it, a welcome message says "Welcome to the Sophos schema viewer" and "Use the drop-down below to view the schema of your choice." A dropdown menu is open, showing "Data Lake" and "Endpoint" with "Endpoint" selected. A sidebar on the left lists categories: Endpoint, Detection, Email, Firewall, Cloud Optix, Mobile, and M365. A specific section titled "Sophos Endpoint data in the Data Lake" is highlighted with a red box. It contains a link to "https://trino.io/docs/current/functions/list.html". On the right, there's a "General info" panel for the "changed\_files\_windows\_sophos" schema, which includes fields for Name, interval, platforms, description, and example. There are also "Data Lake" and "Endpoint" buttons, and a "Download" button with a file icon.

The Sophos schema viewer allows you to browse the schemas used for Data Lake and Endpoint queries. The Data Lake schema is grouped into Sophos product categories. Endpoint queries make use of two schemas; osquery and Sophos extension.

Viewing what data is available allows for a better understanding of how the data can be used to answer specific questions about your environment.

## [Additional Information]

PDF containing the OSQuery and Sophos Extension Schemas can be downloaded from the following links.

OSQuery Schema (<https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/m/files/9511>)

Sophos Extension Schema (<https://community.sophos.com/intercept-x-endpoint/edr-data-lake-eap/m/files/9512>)

# Get To Know Your Data

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists 'DETECTION AND REMEDIATION' options: Dashboard, Threat Graphs, Live Discover (which is selected and highlighted in blue), Detections, Investigations, and Preferences. The main content area is titled 'Threat Analysis Center - Live Discover' and includes a 'Designer Mode' toggle switch. Below it, a search bar contains the query 'Query : Table schema'. A section titled 'Device selector (14 Endpoints available)' follows. Underneath, a table titled 'Table schema query results' displays 15 rows of data. The columns are labeled A, B, C, D, and E. The data is as follows:

A	B	C	D	E
1 epName	table	column	type	extension
2 Training-W10	appcompat_shims	executable	TEXT	core
3 Training-W10	appcompat_shims	path	TEXT	core
4 Training-W10	appcompat_shims	description	TEXT	core
5 Training-W10	appcompat_shims	install_time	INTEGER	core
6 Training-W10	appcompat_shims	type	TEXT	core
7 Training-W10	appcompat_shims	sdb_id	TEXT	core
8 Training-W10	arp_cache	address	TEXT	core
9 Training-W10	arp_cache	mac	TEXT	core
10 Training-W10	arp_cache	interface	TEXT	core
11 Training-W10	arp_cache	permanent	TEXT	core
12 Training-W10	atom_packages	name	TEXT	core
13 Training-W10	atom_packages	version	TEXT	core
14 Training-W10	atom_packages	description	TEXT	core
15 Training-W10	atom_packages	path	TEXT	core

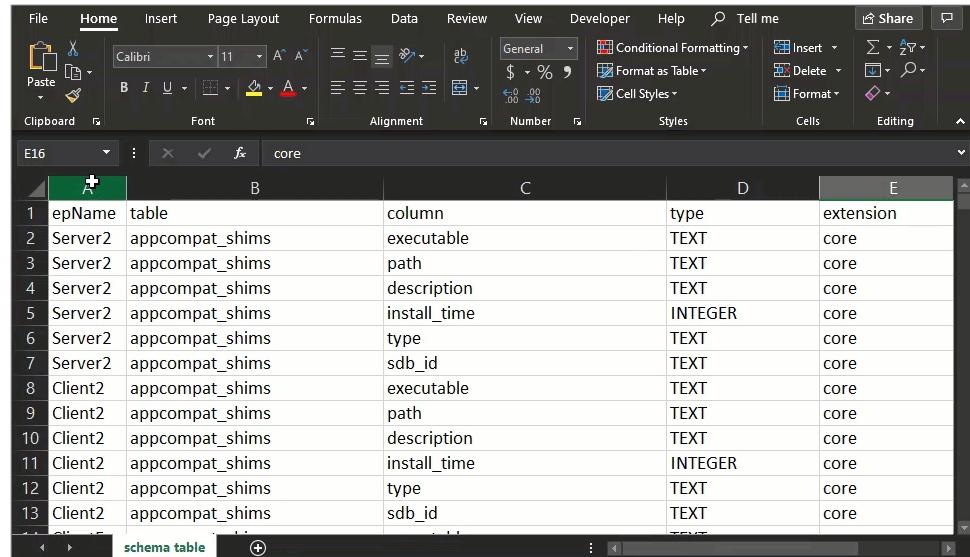
On the right side of the table, there is a progress indicator '3 / 3 Devices completed' and an 'Export' button.

Using the schema table canned query, you can determine the tables that are available for you to return the data you need. This can be exported to a .csv file.

# Get To Know Your Data

Sort and filter the exported data.

View the table names and available data



The screenshot shows a Microsoft Excel spreadsheet titled 'schema table'. The table has five columns labeled A through E. Column A contains row numbers from 1 to 13. Column B contains table names like 'appcompat\_shims' and 'core'. Column C contains column names such as 'column', 'executable', 'path', 'description', 'install\_time', 'type', 'sdb\_id', and 'path'. Column D contains data types including 'TEXT' and 'INTEGER'. Column E contains values like 'extension' and 'core'. The 'core' table entry in column B is highlighted in yellow.

	A	B	C	D	E
1	epName	table	column	type	extension
2	Server2	appcompat_shims	executable	TEXT	core
3	Server2	appcompat_shims	path	TEXT	core
4	Server2	appcompat_shims	description	TEXT	core
5	Server2	appcompat_shims	install_time	INTEGER	core
6	Server2	appcompat_shims	type	TEXT	core
7	Server2	appcompat_shims	sdb_id	TEXT	core
8	Client2	appcompat_shims	executable	TEXT	core
9	Client2	appcompat_shims	path	TEXT	core
10	Client2	appcompat_shims	description	TEXT	core
11	Client2	appcompat_shims	install_time	INTEGER	core
12	Client2	appcompat_shims	type	TEXT	core
13	Client2	appcompat_shims	sdb_id	TEXT	core

SOPHOS

If you have exported the data, you can filter and sort the tables to view specific information.

This is especially useful if you want to determine what data is included in a specific table. For example, if you want to determine which tables will include a username, you can filter the column data to show 'username' and identify the tables that data exists in.

# Activity: Sophos Schema Viewer



- Use the link to access Sophos schema viewer
- Use the Data Lake drop down menu to view data in the endpoint category
- Select **changed\_files\_windows\_sophos** and view the information for this table
- From the Endpoint drop down select **osquery** – this will open in new browser tab
- Select **account\_policy\_data** and view the information in the table
- Return to the Sophos schema and From the Endpoint drop down select **Sophos extensions**
- Select **sophos\_detections\_journal** and view the information

[Sophos schema viewer](#)

[CONTINUE](#)

<https://docs.sophos.com/central/References/schemas/index.html>

SOPHOS

Please complete this activity.

Click **Sophos schema viewer** to open the viewer in a new browser window. Once you have finished, click **Continue**.

## [Additional Information]

<https://docs.sophos.com/central/references/schemas/index.html>

# Creating a New Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, a sidebar lists 'DETECTION AND REMEDIATION' options: Dashboard, Threat Graphs, Live Discover (which is selected), Detections, Investigations, and Preferences. The main area is titled 'Threat Analysis Center - Live Discover' and shows a summary: 'Query : Select One - 18 Categories, 335 Queries'. Below this are three tabs: All Queries (selected), Endpoint Queries, and Data Lake Queries. A note says 'Queries that get data from devices or from the Data Lake'. A search bar is present. On the right, there are several categories of queries, each with an icon and a count: All queries [335], Recent queries [18], Anomalies [0], ATT&CK [26], Cloud Optix [0], Compliance [44], Device [44], Email [7], Events [28], Files [9], Microsoft 365 [10], Mobile [20], Network [56], Other queries [32], Processes [89]. A 'Create new query' button is highlighted with a red box. At the bottom right is a 'Run Query' button.

To create a new query, click **Create new query**.

Please note that this option will only be displayed when you have enabled designer mode.

# Creating a New Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with 'Threat Analysis Center' and 'DETECTION AND REMEDIATION' sections. The 'Live Discover' tab is selected. The main area is titled 'Threat Analysis Center - Live Discover' with a sub-section 'Overview / Threat Analysis Center Dashboard / Live Discover'. It shows 'Designer Mode' is turned on. A query card is displayed: 'Query : List All Programs Installed' under 'Category : All queries, Device'. Below it, there's a 'Back to categories' link, 'Edit' and 'Save' buttons, and a 'Cancel' button. The form fields include 'Query Name' (List All Programs Installed), 'Category' (All queries, Device), 'Description' (List all programs that are installed), and 'Source' (Live Endpoint). A note at the bottom says 'Expected system impact: No system impact data available. To get system impact data, save and run the query on one device to test it.' A green callout box on the right contains the text 'Enter the following details:' followed by a bulleted list: '• Query name', '• Category', '• Description', and '• Source'.

Enter a name for the query and optionally select one or more categories the query will be assigned to. The 'all queries' category is automatically applied, however, you can enter additional categories. In this example we have added the 'Device' category.

Enter a description for the query and then select the source of the query. You can choose between Data Lake and Endpoint queries.

You can then select the operating systems the query can support.

# Creating a New Query

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', 'DETECTION AND REMEDIATION' (with 'Dashboard', 'Threat Graphs', and 'Live Discover' selected), 'Detections', 'Investigations', and 'Preferences'. The main area has a title 'SOPHOS Threat Analysis Center' and 'DETECTION AND REMEDIATION' with 'Dashboard', 'Threat Graphs', and 'Live Discover' (selected). Below this is a 'SQL' section with a 'Source' dropdown set to 'Live Endpoint Windows, Linux'. A 'Hide variable editor' button is above a 'variable editor' section. An orange box highlights the '+ Add variable' button. A green callout box points to a dropdown menu for 'Variable type' which includes 'String', 'Date', 'SHA-256', 'IP Address', 'sophosPID', and 'URL'. The 'String' option is selected.

For any new or edited queries you can include up to 6 variables. You can select a variable type of either string, date, SHA 256, IP address, Sophos PID, URL, registry key, file path, and username. Once added, the variable will be given a prefix and postfix.

# Writing a New Query

**SELECT \* FROM certificates**

Return ALL data

Specify which table you want to return data from

This query will return all available data from the certificates table

The screenshot shows a software interface for writing SQL queries. At the top, there's a toggle for 'Designer Mode' (which is turned on) and a dropdown menu set to 'Core table certificates'. Below that is a toolbar with 'Edit', 'Save', and 'Delete' buttons. The main area is titled 'All queries: Core table certificates' and contains a single entry: 'Core table certificates'. It was 'Created by UK Training'. Under 'Sources', it lists 'Linux' and 'macOS'. There's a note about 'Expected system impact' stating 'No system impact data available. To get system impact data, run the query on one device to test it.' At the bottom, the SQL code is shown as 'SELECT \* FROM certificates'. A 'Run Query' button is at the bottom right, and the 'SOPHOS' logo is in the bottom right corner of the window.

To return all data held in a single table, use the **SELECT \*** statement. The asterisk means that you want to return all data available in the table.

The **FROM** statement is used to specify the data table you want to return data from. In this example we have asked for all data to be returned from the certificates table.

Please note that this type of query may not work for all tables due to the amount of data stored in the available data tables.

# Writing a New Query

The screenshot shows a SQL query editor window. In the top-left corner, there is a small icon labeled '\*SQL'. Below it, the word 'SELECT' is typed into the input field. A dropdown menu is open, listing various SQL keywords and system procedures. The 'SELECT' keyword is highlighted in blue. Other visible items in the dropdown include 'sp\_delete\_backuphistory', 'procedure', 'SET CURSOR\_CLOSE\_ON\_COMMIT', 'statement', 'SET TRANSACTION ISOLATION LEVEL READ CO', 'SET TRAN', and 'sys.sp\_>'. Below the dropdown, the query code continues with 'SELECT name, version, install\_location, install\_source, language, publisher, uninstall\_string, install\_date, identifying\_number FROM programs'. The 'FROM programs' part is currently selected, indicated by a vertical cursor bar on its right side.

SOPHOS

To return more specific data, you can list the data rows you want to return. All SQL queries start with a **SELECT** statement. Following this, the data rows required are listed.

In this example, the data rows for name, version, install location, install source, language, and publisher have been added. Additionally, the uninstall string for the program and the date it was installed are added. Lastly, the identifying number is added.

The query is ended with the **FROM** statement that identifies the table the data is returned from.

The example query shown here is asking for data from a single table.

# Writing a New Query

All queries: Auth History of a User

A list of authentication history for the past 90 days for a user for login attempts NOT to their assigned device on the network.

Created by UK Training

Sources      Expected system impact      0.481 Data transferred (Kb)      2.566 sec Execution time

Windows      Smallest impact (Fastest)      Largest impact (Slowest)      Small      Large      Fast      Slow

Hide variable editor

*Descriptive name	Variable type	SQL variable name	*Enter value to use when query runs
UserName	String	\$\$UserName\$\$	admin

SQL

```
SELECT DISTINCT
eventid,
ia.address as local_IP,
datetime (time,'unixepoch') Date_Time,
COUNT (task_message) Logon_Count,
json_extract (swe.data,'$.EventData.LogonType') LogonType,
json_extract (swe.data,'$.EventDataIpAddress') Remote_IP_Address,
json_extract (swe.data,'$.EventData.TargetUserName') TargetUserName,
data
FROM sophos_windows_events swe
JOIN interface_addresses ia
WHERE eventid IN (4672,4624,4625) AND time > strftime ('%s','now','-%90 days') and TargetUserName LIKE '$$UserName$$' and ia.type = 'dhcp'
GROUP BY LogonType;
```

Schema

Include the variable in the SQL command

SOPHOS

Any query created should specify the variable information in the SQL code. When the query is run, the administrator enters the variable information which is automatically substituted for the variable used in the SQL query.

Here is an example. In the variable editor, the username is entered before running the query which replaces the variable placeholder when the query is run.

# Creating a New Query

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, there's a sidebar with 'Threat Analysis Center' and 'DETECTION AND REMEDIATION' sections. Under 'DETECTION AND REMEDIATION', 'Live Discover' is selected and highlighted with a blue background. The main content area is titled 'Threat Analysis Center - Live Discover' and shows 'Designer Mode' is turned on. A query is being created with the following details:

- Query :** List All Programs Installed
- Category :** All queries, Device
- Query Name:** List All Programs Installed
- Category:** All queries, Device
- Description:** List all programs that are installed
- Source:** Live Endpoint (selected)
- Expected system impact:** No system impact data available. To get system impact data, save and run the query on one device to test it.

The 'Save' button is highlighted with an orange box.

Once you are happy with the created query, click **Save**.

We recommend that any new queries are run on a small group of test devices before running the query for all devices.

# Resource Thresholds

SophosOSQuery.exe and SophosOSQueryExtension.exe always run at the lowest CPU priority

A **watchdog** service prevents overloading a device

## Thresholds

- If SophosOSQuery.exe uses more than 250MB ram OR CPU greater than 60%
- If SophosOSQueryExtension.exe uses more than 250MB ram
- If the query response data size is more than 10MB from a single device
- If the query request data size is more than 50KB or less than 15 characters

If a threshold is reached, the query will be stopped, and an error is returned in Live Discover

SOPHOS

Depending on the query you create, you may be asking for a lot of data to be returned. So how does Live Discover prevent queries from overloading a device?

The Sophos OSQuery.exe and SophosOSQueryExtension.exe always run at the lowest CPU priority. There is also a watchdog service that prevents overload, the query will be stopped once a threshold is reached, and an error returned against the query in Live Discover.

The Live Discover query resource thresholds are:

- If SophosOSQuery.exe uses more than 250 MB ram OR CPU greater than 60%
- If SophosOSQueryExtension.exe uses more than 250 MB ram
- If the query response data size is more than 10 MB from a single device
- If the query request data size is more than 50 KB or less than 15 characters

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

Which SQL statement is used to return all data from a single data table?

SELECT \*

GROUP BY

DISTINCT

FROM

SOPHOS

## Question 2 of 2

What is the maximum number of variables that can be added to a single Live Discover query?  
(Enter a numeric value)

\_\_\_\_\_

# Chapter Review

‘Designer Mode’ must be **enabled** to write new Live Discover queries.

To view the **available data tables** use the **Sophos schema viewer** or run the **table schema** canned query.

Any **new queries** should be **run for the first time using a small group of devices**. Resources thresholds are applied to prevent overload.

SOPHOS

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

‘Designer Mode’ must be enabled to write new Live Discover queries.

To view the available data tables, use the Sophos schema viewer or run the table schema canned query.



# Using Sophos Central XDR for IT Operations

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4565: Using Sophos Central XDR for IT Operations

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.

# Using XDR for IT Operations

In this chapter you will learn how to use Live Discover, Live Response and result pivoting to perform IT operational tasks across a network

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access and navigate Sophos Central
- ✓ How to run an Endpoint Live Discover query
- ✓ How to run a Live Response session on a protected device
- ✓ How to pivot Live Discover results

DURATION     **6 minutes**

SOPHOS

In this chapter you will learn how to use Live Discover, Live Response, and result pivoting to perform IT operational tasks across a network.

# IT Operations

Sophos Central XDR



Work faster



Do more with less

SOPHOS

Over twenty percent of a cyber security teams time is spent managing security whilst the budget for people and technology is low. Sophos Central XDR allows IT Teams to work faster and complete more with less resource.

Let's look at a few use case scenarios for completing IT operational tasks across a network.

# Scenario One

SOPHOS

Scenario one.

## Use Case Scenario One



Are the PDQ Deployment and Inventory services running on devices?

SOPHOS

In this scenario, your IT team makes use of the PDQ deployment and Inventory automation tools. The scripted deployments that make use of the PDQ deployment tool are not working as expected.

You want to check that the PDQ deployment and inventory services are running on devices.

# Checking Services

The screenshot shows the Sophos Threat Analysis Center interface. On the left, there's a sidebar with 'DETECTION AND REMEDIATION' options: Dashboard, Threat Graphs, **Live Discover** (which is selected), Detections, Investigations, and Preferences. The main area is titled 'Threat Analysis Center - Live Discover' and shows a query: 'Query : Services installed on the device'. A green callout box points to this query with the text 'Run the canned query 'Services installed on the device''. Below the query, it says 'Services installed on the device' and 'All queries: Services installed on the device'. It lists services with columns for Sources (Windows), Expected system impact (ranging from Smallest Impact (Fastest) to Largest Impact (Slowest)), Data transferred (Kb) (ranging from Small to Large), and Execution time (ranging from Fast to Slow). There's also a 'Device selector (17 Endpoints available)' section with tabs for Available devices and Selected devices, and a 'Filters' section with an Online Status filter and a 'Run Query' button.

You navigate to Live Discover and select to run the canned query that lists all services along with their current status.

# Checking Services

Services installed on the device query results						1 / 1 Devices completed
epName	name	display_name	start_type	path	status	Export
Training-W10	StorSvc	Storage Service	AUTO_START	C:\Windows\Sy...	STOPPED	
Training-W10	WiaRpc	Still Image Acquisiti...	DEMAND_S...			
Training-W10	StateRepository	State Repository Se...	DEMAND_START	C:\Windows\sy...	RUNNING	

Export the query results

Filter the data to look for the PDQ entries

Check the status of the service

	A	B	C	D	E	F	G	H	I
1	epName	name	display_name	start_type	path	status	user_account		
272	Training-W10	PDQDeploy	PDQ Deploy	AUTO_START	"C:\Program Files (x86)\PDQ Deploy"	STOPPED	SOPHOS.LOCAL\Administrator		
273	Training-W10	PDQInventory	PDQ Inventory	AUTO_START	"C:\Program Files (x86)\PDQ Inventory"	RUNNING	SOPHOS.LOCAL\Administrator		

SOPHOS

There is a lot of data returned, therefore, you export the data and then apply a filter to only display the PDQ entries.

Here you can see that for the device Training W10 the PDQ Deploy service is stopped.

# Checking Services

The screenshot shows the Sophos Central XDR interface. On the left, a device card for 'Training-W10' is displayed, showing details like Windows 10, IP: 192.168.1.110, and last user Administrator. A green checkmark icon is present. On the right, a green callout box says 'Start a Live Response session for the device'. Below it, a modal window titled 'Live Response - Training-W10' shows a 'Start new session' section. The 'SESSION PURPOSE' field contains 'Start PDQ Deploy Service|'. An orange box highlights the 'Live Response' button in the device card's actions menu, and an orange arrow points from this button to the 'Start' button in the modal window. The Sophos logo is at the bottom right.

You need to start the service on the device. To do so, you navigate to the **Device** page in Sophos Central and select **Live Response** from the left-hand menu.

To start a new Live Response session, you must enter a reason for the session. This is especially useful for auditing.

## Checking Services

Start the service using the command  
`net start PDQDeploy`

SOPHOS

Live Response - Training-W10

OS: Windows 10 Enterprise IP: 192.168.1.100 Last user: SOPHOS\Administrator Group: Reading Office

```
Microsoft Windows [Version 10.0.19043.1089]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net start PDQDeploy
The PDQ Deploy service is starting.
The PDQ Deploy service was started successfully.

C:\Windows\system32>
```

SOPHOS

Start the service on the server by using the command ‘`net start PDQ Deploy`’.

The command should successfully start the service on the device. The Live Response session can be ended.

# Checking Services

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists 'DETECTION AND REMEDIATION' options: Dashboard, Threat Graphs, Live Discover (selected), Detections, Investigations, and Preferences. The main area displays a query results page titled 'Services installed on the device'. A green callout box highlights the status of the 'PDQDeploy' service.

Query : ✓ Services installed on the device

Back to categories / All queries Services installed on the device

All queries: Services installed on the device

Lists all services installed on the device  
Created by Sophos

Sources: Windows

Expected system impact: Smallest Impact (Fastest) Largest Impact (Slowest)

31.134 Data transferred (Kb): Small Large

0.332 sec Execution time: Fast Slow

Device selector (17 Endpoints)

The PDQDeploy service is successfully RUNNING

Services installed on the device query results 1 / 1 Devices

Export

epName	name	display_name	start_type	path	status
Training-W10	PDQInventory	PDQ Inventory	AUTO_START	"C:\Program Files (x...)	RUNNING
Training-W10	PDQDeploy	PDQ Deploy	AUTO_START	"C:\Program Files (x...)	RUNNING

Re-run the services installed canned query in Live Discover.

In the results for the device, you can see that the PDQ Deploy service is now in a RUNNING state.

# Scenario Two

SOPHOS

Scenario two.

## Use Case Scenario Two



You have a strict VPN policy.

No additional VPN clients are allowed to be installed on Sophos protected devices.

Are any devices running unauthorized VPN clients?

SOPHOS

You have a strict VPN policy. Sophos' VPN client is allowed, no additional VPN clients are allowed to be installed on protected devices.

You are going to use Live Discover to determine if there are any devices running unauthorized VPN clients.

# Simulation: Use Case Scenario Two



This simulation demonstrates how you can use Live Discover to determine unauthorized programs and use Live Response to remove the programs identified.

**LAUNCH SIMULATION**

**CONTINUE**

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

# Scenario Three

SOPHOS

Scenario three.

## Use Case Scenario Three



As part of our security policy, only Sophos password safe can be used to store passwords.

Are there any devices running online unauthorized password managers?

SOPHOS

In this scenario, the IT Team have a security policy where only Sophos password safe can be used to store passwords.

The team want to find out if there are any devices that are running online unauthorized password managers.

## Use Case Scenario Three

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left, a sidebar menu includes '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' and shows a 'Designer Mode' toggle switch. Below it, a search bar displays the query 'Select One - 18 Categories, 336 Queries'. A green callout bubble points to the search bar with the text 'View the FireFox add-ons canned queries'. The results table has columns for 'Name', 'Description', 'Category', 'Sources', 'System Impact', 'Created by', and 'Last modified'. Two entries are listed:

Name	Description	Category	Sources	System Impact	Created by	Last modified
Firefox add-ons	Lists all Firefox add-ons inst...	Other queries	Windows, ...	Larges...	S	Nov 04, 2021
Firefox add-ons (Data La...)	Lists Firefox add-ons on dev...	Other queries	Data Lake			

At the bottom right of the table is a 'Run Query' button.

In the organization you only allow Internet access using the Mozilla FireFox web browser. You use Live Discover to identify the FireFox add-ons that are currently installed on each device.

You find a canned query that will list all add-ons in FireFox.

## Use Case Scenario Three

Enable Designer Mode to edit the query

Designer Mode  
Lets you create or edit queries

Query : Select One - 18 Categories, 336 Queries

All Queries Endpoint Queries Data Lake Queries

Queries that get data from devices or from the Data Lake

firefox

Create new query Create new category

Back to categories

Name	Description	Category	Sources	System Impact	Created by	Last modified
Firefox add-ons	Lists all Firefox add-ons inst...	Other queries	Windows, ...	Larres	S	Nov 04, 2021
Firefox add-ons (Data La...)	Lists Firefox add-ons on dev...	Other queries	Data Lake			

RUN QUERY

You enable 'Designer Mode' to view the SQL being used for the query as you want to amend the query so that it will only return password add-ons.

You select the query from the list.

## Use Case Scenario Three

The WHERE will return any data in firefox\_addons.name data table

```
*SQL
SELECT DISTINCT
    firefox_addons.name,
    users.username,
    firefox_addons.identifier,
    firefox_addons.creator,
    firefox_addons.type,
    firefox_addons.version,
    firefox_addons.description,
    firefox_addons.source_url,
    firefox_addons.visible,
    firefox_addons.active,
    firefox_addons.islisted,
    firefox_addons.autoupdate,
    firefox_addons.native,
    firefox_addons.location,
    firefox_addons.path
FROM users
LEFT JOIN firefox_addons
    USING (uid)
WHERE firefox_addons.name IS NOT NULL
```

Device selector (17 Endpoints available)

Available devices Selected devices

Filters Update selected devices list Run Query

SOPHOS

In designer mode, you can view the SQL being used for the query.

You can see that the WHERE statement is in use which will return data included in the FireFox add-ons name data table.

# Use Case Scenario Three

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. The left sidebar has a dark theme with the following navigation options:

- Dashboard
- Threat Graphs
- Live Discover** (selected)
- Detections
- Investigations
- Preferences

The main content area is titled "Threat Analysis Center - Live Discover" and shows the following details:

- Designer Mode:** A toggle switch is turned off.
- Query:** Firefox add-ons (status: ✓)
- Buttons:** Back to categories / All queries, Edit (highlighted), Save.
- Section:** Firefox add-ons
- All queries: Firefox add-ons:** Lists all Firefox add-ons installed on the device.
- Sources:** Windows, Linux, macOS
- Metrics:**
  - Expected system impact: A slider bar from "Smallest impact (Fastest)" to "Largest impact (Slowest)".
  - 13.876 Data transferred (Kb): A slider bar from "Small" to "Large".
  - 0.16 sec Execution time: A slider bar from "Fast" to "Slow".
- SQL:** SELECT DISTINCT firefox\_addons.name, users.username, firefox\_addons.identifier, firefox\_addons.creator, firefox\_addons.type,
- Run Query** button.

As you want to limit the results to return only password add-ons, you select to edit the query.

## Use Case Scenario Three

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists 'DETECTION AND REMEDIATION' options: Dashboard, Threat Graphs, Live Discover (which is selected), Detections, Investigations, and Preferences. The main area is titled 'Hide variable editor' and contains an 'SQL' section with the following code:

```
SELECT DISTINCT
    firefox_addons.name,
    users.username,
    firefox_addons.identifier,
    firefox_addons.creator,
    firefox_addons.type,
    firefox_addons.version,
    firefox_addons.description,
    firefox.addons.source_url,
    firefox.addons.visible,
    firefox.addons.active,
    firefox.addons.disabled,
    firefox.addons.autoupdate,
    firefox.addons.native,
    firefox.addons.location,
    firefox.addons.path
FROM users
LEFT JOIN firefox_addons
USING (uid)
WHERE firefox_addons.name LIKE '%password%'
```

A large green callout box points to the 'WHERE firefox\_addons.name LIKE '%password%'' line, containing the text: 'Append a LIKE statement to the WHERE statement to return only names that include the word 'password''.

To specify the data you want returned from the table, you append a **LIKE** statement to the **WHERE** statement.

This will return data from the FireFox add-ons name data table if the data matches the word 'password'.

## Use Case Scenario Three

The screenshot shows a table titled "Firefox add-ons (1) query results". The table has columns: epName, name, username, identifier, creator, and type. A single row is present, corresponding to the device "Training-W10". The "name" column contains the value "LastPass: Free Password M...", which is highlighted with an orange border. The "creator" column shows "anoble" and the "type" column shows "extension". The top right corner of the interface shows "3 / 3 Devices completed" and an "Export" button. A green callout box points to the "LastPass" entry in the table, stating: "Password manager addons are listed in the results".

epName	name	username	identifier	creator	type
Training-W10	LastPass: Free Password M...	anoble	support@lastpass.c...	LastPass	extension

>Password manager addons are listed in the results

Once the query is run, you can see in the results that out of the three devices the query was run against, one device has returned data.

Training W10 has the LastPass extension installed. You now know that the user 'anoble' has installed an unauthorized password manager.

SOPHOS

# Video Demo: Use Case Scenario Three



This video demonstrates how to edit a query that lists all devices that have installed a password safe add-on in Firefox

**LAUNCH DEMONSTRATION**

**CONTINUE**

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

## IT Operations - Summary

Sophos XDR can:

- Find known vulnerabilities
- Find out of date applications
- Discover bad certificates
- Identify unknown services
- Determine whether remote sharing is enabled
- Identify unencrypted SSH keys
- Discover if guest accounts have been enabled
- Locate specific file copies

and so much more...

SOPHOS

These scenarios are basic examples of what you can use Sophos XDR features for. Among numerous additional use cases are:

- Finding known vulnerabilities
- Finding out of date applications
- Discovering bad certificates
- Identifying unknown services
- Determining whether remote sharing is enabled
- Identifying unencrypted SSH keys on a device
- Discovering if guest accounts are enabled
- And, locating specific file copies

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!

## Question 1 of 2

Which statement would you add to the WHERE statement to return only names that include the name '**password**'?

IS '%password%'

LIKE '%password%'

= '%password%'

LIKE 'password'



## Question 2 of 2

Which feature can be used to start services remotely on a protected device?

Live Discover

Services can only be started locally on the device

The pivot option 'Start Service'

Live Response

SOPHOS

# Chapter Review

Live Discover allows IT Teams to **work faster** and complete more tasks **with less resource**.

Sophos XDR can be used to **check that services are running** and start them if required.

Sophos XDR can be used to **detect** and remotely remove **unauthorized applications**.

SOPHOS

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

Live Discover allows IT Teams to work faster and complete more tasks with less resource.

Sophos XDR can be used to check that services are running and start them if required.

Sophos XDR can be used to detect and remotely remove unauthorized applications.



# Using Sophos Central XDR for Threat Hunting

Sophos Central Endpoint and Server Protection

Version: 4.0v1



## [Additional Information]

Sophos Central Endpoint and Server Protection

CE4570: Using Sophos Central XDR for Threat Hunting

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.

# Using Sophos Central XDR for Threat Hunting

In this chapter you will learn where to start a threat hunt, how to determine the types of attack activities, and how to use Sophos Central XDR to search for and identify data that could be malicious

## RECOMMENDED KNOWLEDGE AND EXPERIENCE

- ✓ How to access and navigate Sophos Central
- ✓ How to use Live Discover and Live Response
- ✓ How to view threat graphs and perform follow-up actions

DURATION      **13 minutes**

SOPHOS

In this chapter you will learn where to start a threat hunt, how to determine the types of attack activities, and how to use Sophos Central XDR to search for and identify data that could be malicious.

# What is Threat Hunting?

Threat hunting is the process of proactively searching across networks to discover and identify malicious or suspicious threats that have not been detected by existing security solutions



Threat hunting is **proactive**

Discovering something potentially malicious that may be have been missed by automated alerts and detections

SOPHOS

What exactly do we mean by threat hunting?

Threat hunting is part of Sophos' layered approach to cyber security. It is the process of proactively searching across networks to discover and identify malicious or suspicious threats, vulnerabilities, insecurity practices, or anomalies.

Threat hunting is proactive. Discovering something potentially malicious that may have been missed by automated alerts and detections.

## What to Look for

### Determine what you are looking for

- User reports
- Information from a third party
- A high-profile threat in the news
- Threat intelligence reports
- Your own experience or an educated guess

SOPHOS

You can search your network for threats whenever you want to. However, firstly, you need to know what you are looking for.

Any threat search undertaken, is likely to have started because of an event, or information you have received, or come across.

A few examples could be a report from a user, information from a third party or a high-profile threat in the news. You can also view threat intelligence reports or trust your own experience and threat knowledge.



Additional information in  
the notes

## What to Look for

<https://news.sophos.com>

The screenshot shows the Sophos News homepage. At the top, there's a navigation bar with links for 'Products & Services', 'Security Operations', 'Threat Research', 'AI Research', and 'Security News & Tips'. A search icon is also present. Below the navigation, there's a section for 'Featured Articles' with a thumbnail image of a silhouette of a person holding a sword against a dramatic sunset sky. To the right of the thumbnail, the article title 'Winners and losers in the ransomware turf wars' is displayed, along with a small profile picture of a man and a 'THREAT RESEARCH' button. Below the main article, there are two smaller, partially visible images: one showing a document and another showing a software interface.

The 'Sophos News' section, available on the sophos.com website, publishes articles about our products, case studies, and end-user and network specific information. It also hosts SophosLabs uncut articles, which are extremely useful in keeping you up to date with new attacks, how they infect and spread, and what indicators of compromise to look for on your network, should you suspect an infection.

### [Additional Information]

The Sophos News site can be accessed here: <https://news.sophos.com>



Additional information in  
the notes

# What to Look for

<https://sophos.com/labs/technical-papers.aspx>

The screenshot shows the Sophos Technical Papers page. At the top, there's a navigation bar with links for Products, Solutions, Partners, and Support. Below the header, the title "Technical Papers" is centered. A brief introduction follows: "Here you will find a range of papers aimed at system administrators and security specialists on a variety of topical issues. Some of these papers have been presented at security seminars and technical conferences around the world." Three research cards are displayed:

- Cyberthreats: A 20-Year Retrospective**  
In security we spend a lot of time trying to decipher the future. Where's the next technology breakthrough? What are cybercriminals going to do next?  
Annual threat reports provide an opportunity to look back at significant events of the past 12 months and identify trends for future development, action and protection. Looking back in time a
- Sophos 2021 Threat Report**  
As much of the world shifted to remote work in 2020, cybercriminals upped their game, devising ways to use the fears and anxieties of organizations and end users against them.  
[View Research](#)
- An Insider View Into The Increasingly Complex Kingminer Botnet**  
Kingminer is an opportunistic botnet that keeps quiet and flies under the radar. The operators are ambitious and capable, but don't have endless resources – they use any solution and concept that is freely available, getting inspiration from public domain tools as well as techniques used by APT groups.

SOPHOS

Sophos' technical papers offer a range of papers that cover a variety of topical issues. Often you can find information about specific attacks.

## [Additional Information]

You can view all our technical papers here: <https://www.sophos.com/en-us/labs/technical-papers.aspx>



Additional information in  
the notes

## What to Look for

<https://community.sophos.com>

The screenshot shows the Sophos Community homepage. At the top, there's a navigation bar with links like 'Community & Product Forums', 'Community Blogs & Events', 'Getting Started', 'Sophos Partners', 'Member Recognition', 'Sophos Techvids', 'Product Documentation', and 'Support Portal'. Below the navigation is a banner for 'SOPHOS TECHVIDS Configuration and Troubleshooting Videos!' featuring three people and a video thumbnail. To the left, there's a 'Current Central Status' box indicating 'All systems normal' with a green dot. A sidebar on the left shows 'Tweets from @SophosSupport' from 'Sophos S... @So... 11h' with a message about response actions for Sophos Central XDR tools. The main content area includes a 'Welcome to the Sophos Community' message, a 'Latest Community Release Notes & News' section, and a search bar.

We also recommend joining the Sophos Community. From the community you can access the Sophos Support Security Blog and additionally, you can join specific groups.

### [Additional Information]

You can view the community page here: <https://community.sophos.com/>



Additional information in  
the notes

## What to Look for

View third-party sources

Some Government and security agencies provide alerts and services

The image shows two screenshots of government websites. On the left is the official website of the United States Cybersecurity & Infrastructure Security Agency (CISA). It features a search bar, navigation links like 'REPORT', 'SUBSCRIBE', 'CONTACT', and 'SITE MAP', and a prominent 'SHIELDS UP' banner with sub-sections for 'STOP Ransomware' and 'Start preparing now for the transition to post-quantum cryptography'. On the right is the National Cyber Security Centre (NCSC) website, which has a dark blue header with links for 'CSP', 'REPORT AN INCIDENT', and 'CONTACT US'. Below the header is a 'Keep up to date' section featuring a 'NCSC news' card with a list of items, a 'Reports & advisories' card, and a 'Weekly threat reports' card.

SOPHOS

You can obtain information about threats from several other third-party sources. Some government and security agencies provide alert services for new threats, which include indicators of compromise, and hashes that you can use to start a threat hunt.

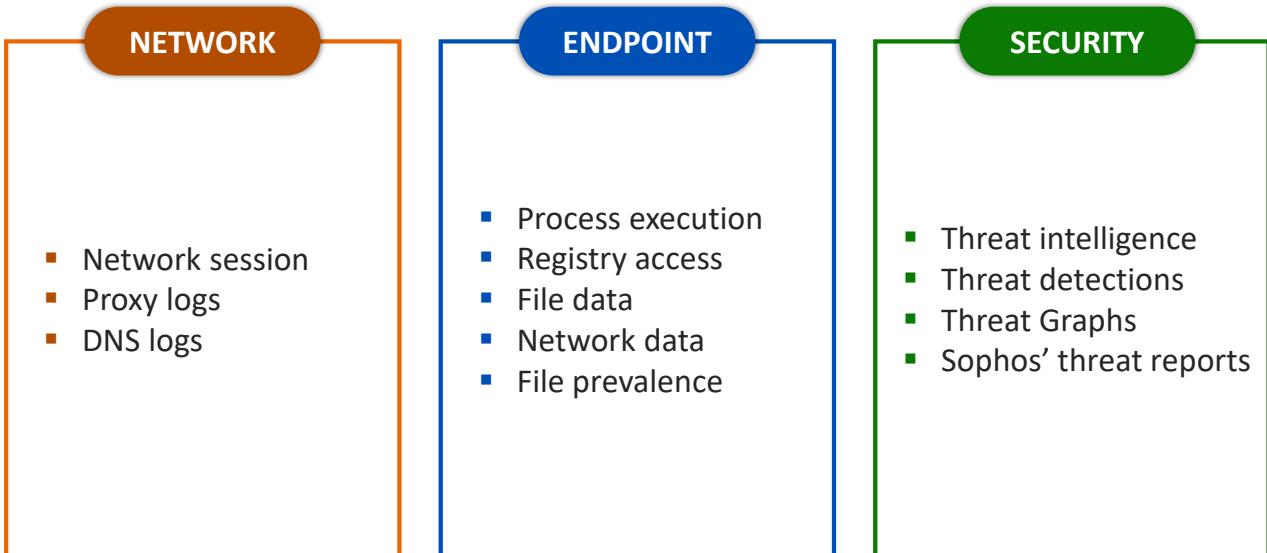
Here are a couple of examples of government agency sites which provide a subscription service to receive up to date news about cyber security threats.

### [Additional Information]

USA you can signup to the cyber security newsletter here: <https://www.cisa.gov/>

UK you can view the Cyber Security centre here: <https://www.ncsc.gov.uk/>

## Determine the Data to Search



SOPHOS

So how do you know where to hunt for a threat on your network?

This will depend on the type of threat you are hunting. To help identify where to start a hunt, you could divide your data into three data sets.

Network data will include information about a network session, the active connections between hosts, including the IP addresses, destination and host ports, and the duration of any active connections. Additionally, network data will contain information about outgoing web requests and data related to DNS activity, including domain to IP address mappings, identification and internal clients.

Endpoint data will contain information about processes, file names and identification definitions of each process. It will also include registry access data, including key and value data. Information about files stored, including file creation and modification dates, size and type are held on an endpoint. You will also be able to identify a parent process for a network connection and how common a file is across your network.

Lastly, security data. This includes threat intelligence data gained from threat detections, threat graphs generated, and Sophos' threat reports.

This is not all the data available, however, it gives you an idea of how you can separate data on your network.

# Identify Attack Activities

## Attack Aim

Remain undetected whilst gaining access to full network

- Take advantage of RPC (Remote Procedure Call)
- DLL injection
- Registry key modification

## Attack Aim

Extract data without detection

- Look like routine network traffic
- Bypass monitored ports
- Use RPC to gain access to a target system
- Path interception

SOPHOS

It is important that you understand your own environment, so you can better anticipate the type of information an attacker might want to target and identify the techniques or activities they may use to get to this information. Once an attacker has access to an endpoint, it is likely that they will want to remain undetected for as long as possible, whilst trying to gain access to the rest of your network. To do so, they could:

- Take advantage of Remote Procedure Call (RPC) to schedule tasks that run at system start-up
- Run malicious code using another process to load and execute the code
- Add a value of RUN and/or RUNONCE to a registry key, to allow malware binaries to execute on system boot and session logon

If an attacker does gain access to your full network, they may try to extract data without detection. They can use a number of techniques to achieve this, for example:

- Hide in plain site by looking like routine network traffic, by using HTTPS, DNS tunnelling or high traffic TCP ports
- Bypassing monitored ports by sending data through uncontrolled or uncommon ports. This means that they can evade detection from routine scans or reports
- If RPC is enabled, they can use user credentials to gain access to and export a target system
- Path interception. They can place an executable file in a specific path, so that it is run by a legitimate application. This technique uses unquoted paths, path environment variable misconfigurations, and search order hijacking

## Determine the Data to Search

### NETWORK

Search the data for:

- Routine network traffic
- Uncommon ports and protocols
- Use of RPC
- Path interception

### ENDPOINT

Search the data for:

- Enablement of RPC
- DLL injections
- Registry key modification

### SECURITY

Search the data for:

- Identified threats
- Threat indicators
- Potential threats

SOPHOS

Now you have separated your data and identified the attacks you may be vulnerable to; you can start hunting for threats in the appropriate places on your network.

For example, to look for an attacker using RPC, you know to look at the scheduled tasks running at start-up on an endpoint. Or to look for processes that are executing outside of expectation. You can also look at the registry values to search for a value of RUNONCE to find anomalies.

You can view the network data to view routine network traffic, counting the number of active connections over DNS for example. You can also search for traffic using uncommon ports and protocols.

These are examples of what you can do. However, the aim is to identify what you are looking for and where to look for it.

# Threat Hunting



## Additional information in the notes

**Threat Analysis Center - Live Discover**

Overview : Threat Analysis Center Dashboard / Live Discover

Designer Mode  
Lets you create or edit queries

Query : Select One - 18 Categories, 336 Queries

< Back to categories All Queries > ATT&CK

All Sources All System Impact types

Name	Description	Sources
Authentication attempts	Lists all authentication attempts (requires Windows event audit logging)	Windows
Detections per detection type (Data Lake)	Shows the number of detections for each detection type on each endpoint	Data Lake
Exfiltration threats (Data Lake)	Uses MITRE techniques to find specific exfiltration threat cases	Data Lake
Find common command and	Searches for common command and usage across endpoints	Windows

Use canned queries to hunt for threats

Use the Community to discover new queries

SOPHOS COMMUNITY =

Community & Product Forums Community Blogs & Events Getting Started Sophos Partners Member Recognition Sophos Tenants Product Lineup Support Portal

Ep Intercept X Endpoint > Live Discover & Response Query Forum + New

Overview

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

New to Live Discover & Response queries?

See Getting Started in Live Discover - From Beginner to Advanced Query Creation

Make sure to also check out:

- Best Practices On Using Live Discover & Response Query Forum and Sophos EDR Threat Hunting Framework.
- Query Corner Announcement and Master Index.

Note: For more information on Live Discover, please check out our Product Documentation

[Sophos Community XDR Queries on GitHub](#)

Navigate to a category below to browse and submit a query

Browse Live Response and Discover Queries by Category

Latest Live Response and Discover Queries [All]

Uncategorized

Anomalies

ATT&CK

Cloud Optix

Compliance

Data Lake

Using Live Discover to determine TPM enabled devices

25 Aug 2022 10:31 PM

Sophos Central XDR provides you with the tools to search for threats across your network.

You can use the canned queries in Live Discover that will, for example, list all remote authentication attempts, or any running process that might be masquerading as a system process.

Alternatively, we highly recommend that you make use of the Sophos Community pages. Here you can view other queries members of the community have created. Often, you may find a query that another member has created that exactly matches what you are looking for.

### **[Additional Information]**

<https://community.sophos.com/intercept-x-endpoint/p/query-forum>



Additional information in  
the notes

# Threat Hunting

<https://vimeo.com/showcase/6972121/video/405009931>

The screenshot shows a collection of video thumbnails from the Sophos Vimeo channel. The thumbnails include:

- IT Operations: Live Discover leveraging canned queries for basic IT Operations
- Hunting part 1: Performing basic hunting with EDR 3.0 EAP (highlighted with an orange border)
- Live Response EAP Introduction: Learn about how Live Response can be used to help with detailed investigations or take prompt action on devices.
- Initial Analysis Center - Live Show: A screenshot of the Sophos XDR interface showing various threat detection and analysis tools.
- Initial Analysis Center - Live Show: Another screenshot of the Sophos XDR interface, likely showing a different view or continuation of the previous one.
- Initial Analysis Center - Live Show: A third screenshot of the Sophos XDR interface, showing a different perspective on the live analysis center.

SOPHOS

A video demonstration that shows how to perform basic hunting with Sophos Central XDR called 'Hunting part 1' is available on Sophos' Vimeo channel.

## [Additional Information]

The Vimeo showcase is available here: <https://vimeo.com/showcase/6972121>

The video to view is called Hunting part 1 and is available here:

<https://vimeo.com/showcase/6972121/video/405009931>

# Threat Hunting Example One

SOPHOS

We'll now look at examples of how Live Discover can be used to proactively hunt for threats across your network.

In the first example, as part of our routine security practice, we want to check our network to ensure that there are no unsigned applications running.

## Example One

We want to check our network to ensure that there are no unsigned applications running

The screenshot shows two side-by-side interfaces. On the left is the 'Threat Analysis Center - Live Discover' dashboard, which includes sections for Designer Mode, a query selector, and canned query categories like All queries, Recent queries, Anomalies, and ATT&CK. A green callout box labeled 'View canned queries' points to the ATT&CK category. On the right is a search results page for 'All Queries > ATT&CK', showing a list of queries with columns for Name, Description, Sources, System Impact, Created by, and Last modified. One specific query, 'Unsigned applications that were run', is highlighted with an orange box and a green callout box labeled 'Identify a query that matches what you want to search for'. The ATT&CK category box and the highlighted query in the search results are both outlined in orange.

Name	Description	Sources	System Impact	Created by	Last modified
SSH root login	Shows whether SSH root login is permitted	Linux	Not Available		May 06, 2022
Unquoted paths in the service registry keys	Lists unquoted paths in the service registry keys. Unquoted paths allow an adversary to place an application in a higher-level directory so that Windows finds that application instead of the intended one. (MITRE category T1034)	Windows	Not Available		Jul 21, 2021
Unsigned applications that were run	Identifies unsigned applications that were run on the device in the last day. Code signing shows this is an authentic binary from the developer and has not been tampered with. (Code signing MITRE ID T1116)	Windows	Smallest impact (Fastest)		May 06, 2022
Windows detections (Data Lake)	Contains Windows detections and indicators of compromise (IOCs)	Data Lake	Not Available		Jun 07, 2022

We check the Live Discover canned queries to see if there is already a query that will search for unsigned applications.

We find a canned query called 'unsigned applications that were run'.

## Example One

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, the navigation menu includes Threat Analysis Center, Detection and Remediation (Dashboard, Threat Graphs, Live Discover, Detections, Investigations, Preferences), and a Sources section for Windows. The 'Live Discover' tab is selected.

In the main pane, under 'Device selector [10 Endpoints available]', it shows 'Unsigned applications that were run query results'. A specific entry for 'WinClient2' is highlighted with an orange box around the 'SuspiciousActivity.exe' process name. A green callout bubble points to this entry with the text: 'This is a suspicious application being run'.

To the right, the 'Queries' pane lists various options like Data lake queries, Live Discover queries, and Process activity history. Under 'Process activity history', there are dropdown menus for 'Process details for a Sophos PID' and 'Process tree for a PID'. A green callout bubble points to the ellipsis menu (three dots) next to the 'sophos\_pid' dropdown with the text: 'Select the ellipsis menu for the sophos\_pid and run another query to provide process details'.

At the bottom right of the interface is the 'SOPHOS' logo.

We select to run the query across all protected endpoints.

In the results there is one unsigned application returned. For the purposes of this training, the application 'suspicious activity' requires investigation.

We select the ellipsis menu for the sophosPID and select to run another query that will provide the process details for the application.

## Example One

The screenshot shows the Sophos Threat Analysis Center - Live Discover interface. On the left sidebar, under 'DETECTION AND REMEDIATION', the 'Live Discover' option is selected. The main content area displays a query: 'Process details for a Sophos PID'. A green callout bubble points to the 'sophos\_pid' variable input field, which contains the value '15328132836197909517937'. The interface includes sections for 'Processes', 'Sources' (Windows), 'Expected system impact' (No system impact data available), and a 'Device selector' (10 Endpoints available). A 'Run Query' button is at the bottom right.

Look for more details about the sophosPID

This query will provide further details about the application process.

## Example One

epName	sophos_pid	process_name	start_time	end_time	path
WinClient2	2664:13314718...	SuspiciousActivity....	2022-12-05T12:55:...	2022-12-05T12:55:...	C:\Users\Sopho...

The results provide the start and end time of the process, the cmdline and file path along with the SHA 256 hash of the file

SOPHOS

In the results we can view the start and end time of the process. The cmdline of where the application was executed from.

Additionally, we can see the SHA 256 of the file.

## Example One

The screenshot shows the Sophos Central XDR Threat Analysis Center interface. On the left, a sidebar lists navigation options: DETECTION AND REMEDIATION (Dashboard, Threat Graphs, Live Discover, Detections, Investigations, Preferences). The 'Live Discover' option is selected and highlighted in blue. The main pane displays a search interface. At the top, under 'Sources', it says 'Windows' and 'Expected system impact: No system impact data available. To get system impact data, run the query on one device to test it.' Below this, the 'Queries' section shows several options: 'Data lake queries' (Firewall: Threats detected and their location, Firewall zero-day protection events, Network activity of a process with a specific SHA-256 (Data Lake)), 'Enrichments' (VirusTotal lookup), and 'Live Discover queries' (Events involving a SHA-256, Processes matching SHA-256 hashes in the last 30 days, Search for processes (Windows)). The 'Processes matching SHA-256 hashes in the last 30 days' query is currently selected and highlighted in blue. The results pane shows a table with columns: app\_id, ml\_score, pua\_score. There are two rows of data. The first row has app\_id 28361970..., ml\_score 9728, and pua\_score 3. The second row has app\_id 12c2d18fbdcadecfc..., ml\_score 22, and pua\_score 10. Below the table is a 'Device Telemetry' section showing 'COMPILETE: 6 - data.sent: 0 - no data sent: 0 - errors: 0 - no response'. A 'Run Query' button is located at the top right of the results pane.

We can use the SHA 256 file hash to search across our network to determine if this file exists on any other endpoints.

To do this, we pivot to another query that will show any processes matching the SHA 256 hash in the last 30 days. The SHA 256 value is automatically added to the query.

## Example One

The screenshot shows the Sophos Central XDR interface. On the left, the 'Threat Analysis Center' sidebar includes options like 'Live Discover' (which is selected), 'Detections', 'Investigations', and 'Preferences'. The main area displays a table titled 'Processes matching SHA-256 hashes in the last 30 days query results'. The table has columns for 'epName', 'sha256', 'path', and 'sophos\_pid'. A green callout bubble with the text 'Select the ellipsis menu for the path' points to the ellipsis menu icon next to the 'path' column of the row for 'WinClient2'. The table shows 6 / 6 Devices completed. A red box highlights the 'Run Query' button at the bottom right of the table.

epName	sha256	path	sophos_pid
WinClient4	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Documents\...	12500:1328214116520076124
WinClient5	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Downloads\S...	3292:132821406803503803
WinClient5	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Downloads\S...	5216:132821407540622138
WinClient5	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Documents\...	6432:132821415411248410
WinClient5	12c2d18fbdcadecfc836addee0ec9738...		5882390649
WinClient1	12c2d18fbdcadecfc836addee0ec9738...		995570773
WinClient2	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Documents\...	9356:132821411408386442
WinClient2	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\anoble\Documents\Suspici...	15328:132836197909517937
WinClient3	12c2d18fbdcadecfc836addee0ec9738...	C:\Users\administrator\Documents\...	1324:132821414767257389

In the results we can see that this file is present on multiple protected endpoints including our server.

Selecting to see the details of WinClient2, which is where we identified the file, we can see that the application was executed by a user.

We select the pivoting options and select to **Generate a threat graph**.

## Example One

The screenshot shows the Threat Analysis Center interface. At the top, it displays "Threat Analysis Center - SuspiciousActivity.exe - WinClient2". Below this, there's a navigation bar with links to "Overview", "Threat Analysis Center Dashboard", "Threat Graphs", and "SuspiciousActivity.exe - WinClient2". On the right, user information is shown: "Help", "Simon Smith", and "Sophos UK - Super Admin".

The main area is divided into two sections: "Summary" on the left and "Suggested next steps" on the right.

**Summary:**

- Threat graph generated by Simon Smith on Dec 10, 2021 2:58 PM
- Named: SuspiciousActivity.exe - WinClient2
- Root cause: [explorer.exe](#) (highlighted with a red box)
- Additional Information: The root cause copied a file from the network.
- Network Location: \\winserver1\ netlogon\suspiciousactivity.exe
- Possible data involved: [1 business file](#)
- Where: On [WinClient2](#) that belongs to [TRAININGDEMO\anoble](#)

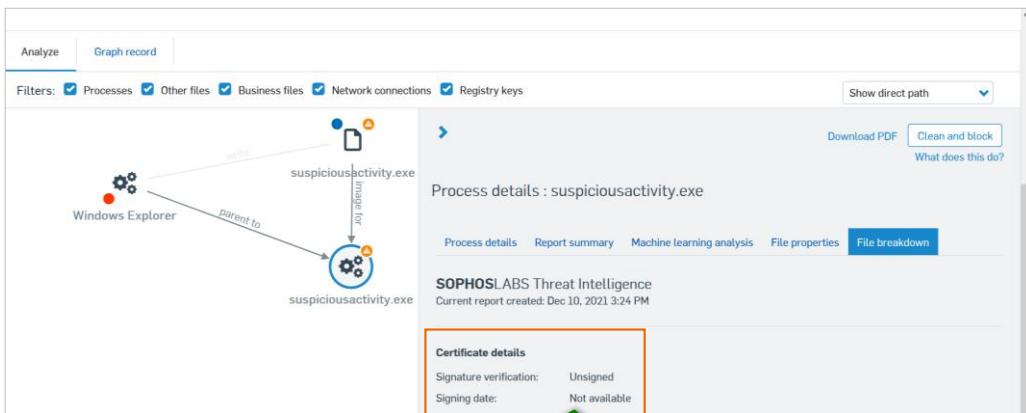
**Suggested next steps:**

- Set a status for the threat graph (Priority: Medium, Status: New)
- Investigate 1 process 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](#)

A green callout box points to the "Root cause" section, containing the text: "When the application was executed, files were copied from the network".

Once the threat graph has been created, we can see that the suspicious activity application was executed locally and copied network files. We can also see that the file is stored on the network.

## Example One

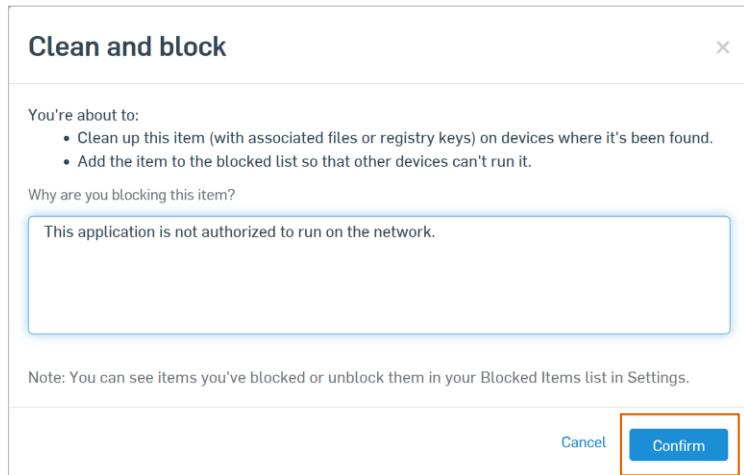


In the file breakdown tab, we can see the application is not signed, which reiterates why we were looking for unsigned applications as part of our security routine.

## Example One

### Summary of Threat Hunt

- Started as a routine security check
- Identified a suspicious unsigned application
- Determined where the application has been run on a network
- Cleaned and blocked the application



We decide to clean up and block this file across our network.

To summarize this threat hunting example:

- This threat hunt started as a routine security check
- We identified an unsigned application that was suspicious
- We determined which endpoints the application was run on
- As a result of this threat hunt, we made the decision to clean and block the application

# Threat Hunting Example Two

SOPHOS

In the second example we want to identify any attack that uses brute force authentication to access networks.

## Example Two

We have read about an attack that uses brute force authentication to compromise networks

We want to view all failed authentication attempts to endpoints in our network

SOPHOS

We want to run a query that will list all failed authentication attempts to our endpoints. If we see over 20 attempts in the same time period, this will indicate a brute force attack.

# Video Demo: Query to List Failed Authentication Attempts



This video demonstrates how to run a query that will list all failed authentication attempts to endpoints

**LAUNCH DEMONSTRATION**

**CONTINUE**

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

SOPHOS

Play this video demonstration.

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

## [Additional Information]

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

## Example Two

### Summary of Threat Hunt

- Identified a potential security issue
- Searched for a query that would identify a possible brute force attack
- Ran the query and identified a possible bad login that required investigation

SOPHOS

In summary we have completed the following:

- Identified a potential security issue
- Searched for a query that would identify a possible brute force attack
- Ran the query and identified a possible bad login that required investigation

# Knowledge Check

SOPHOS

Take a moment to check your knowledge!



## Question 1 of 2

Which 2 of the following could be indications of a threat against the network?

Use of RPC

Multiple users  
authenticating

Path interception

Starting Sophos services

SOPHOS



## Question 2 of 2

Which 2 of the following could be indications of a threat against an endpoint?

Enablement of RPC

DLL Injections

Multiple applications  
running

Allowing traffic on TCP port  
8190

SOPHOS

# Chapter Review

Threat hunting is the process of **proactively searching** across networks **to discover and identify malicious or suspicious threats** that have not been detected by existing security solutions.

To identify where to start a hunt, **divide your data into three data sets: network, endpoint, and security**. This helps to define what to look for when hunting for threats.

You can use the **canned queries in Live Discover** and make use of the **Sophos community pages**, where you can view queries members of the community have created.

SOPHOS

Here are the main things you learned in this chapter.

Threat hunting is the process of proactively searching across networks to discover and identify malicious or suspicious threats that have not been detected by existing security solutions.

To identify where to start a hunt, divide your data into three data sets: network, endpoint, and security. This helps to define what to look for when hunting for threats

You can use the canned queries in Live Discover and make use of the Sophos community pages, where you can view queries members of the community have created.



# 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 at [sophos.com/support](https://www.sophos.com/en-us/support). The page has a blue header with the Sophos logo and navigation links for Services & Products, Solutions, Partners, Support (which is highlighted), Overview, Support Packages, Downloads, Documentation, Training, and Go to Support Portal (which is enclosed in a red box). The main content area features the text "Sophos Support" and a search bar with the placeholder "Search Support". At the bottom, there are links for "Join the Community", "Twitter Support", and 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 overview page with a blue header bar containing the word "Support" and navigation links for Overview, Support Packages, Downloads, Documentation, Training, and Go to Support Portal.

The main content area displays six cards arranged in a grid:

- Read Documentation**: Product Setup and Configuration. Includes a book icon with an orange "i" symbol.
- Knowledge Base**: Solutions to Known Issues. Includes a smartphone icon with a speech bubble containing a question mark.
- Techvids**: Product Support Videos. Includes a video camera icon with a play button.
- Sophos Central Status**: Check Central Downtime & Outages. Includes a laptop icon with a gear symbol.
- Contact Us**: Support Cases & Live Chat. Includes a person icon with a speech bubble.
- Rapid Response**: For Malware and Ransomware. Includes a clock icon with a gear symbol.

A "SOPHOS" logo is visible in the bottom right corner of the page.

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 homepage. At the top, there's a navigation bar with links for PRODUCTS, SOLUTIONS, PARTNERS, and COMPANY. Below the navigation is a search bar with placeholder text "Search..." and a magnifying glass icon. To the right of the search bar is a "LOGIN" button.

The main content area features a search sidebar on the left with filters for "Product" (listing Sophos Mobile, SafeGuard Enterprise, Enterprise Central, Sophos Firewall, Central Admin, etc.) and "Version" (listing NA, 9.708, 9.707, 9.706, 9.705). The main search results show 1-10 of 84,969 results in 0.16 seconds, ordered by RELEVANCE or DATE UPLOADED. A featured article about the Support Certification Program (SCP) is displayed, mentioning Technical Exams and the Support Certification Program.

On the right side, there's a "Current Sophos Status" section indicating "All systems normal" with a green status indicator. It also shows the current status in effect for 3 days, 11 hours, 24 minutes, and 17 seconds. Below this is a "Preferred Language" dropdown set to English [US]. A green button labeled "Click Here To Register" is present.

A "For Critical Cases" section provides instructions for opening support cases, mentioning case numbers and immediate assistance. It includes a dropdown menu for selecting a region. At the bottom right, there's a "LOGIN TO CHAT" button with a speech bubble icon and the word "SOPHOS".

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

Search...



LOGIN

HOME

ALL CONTENT ARTICLES COMMUNITY DOCUMENTATION VIDEOS

Language	Count
English	4,079
French	17
German	17
Spanish	18
Italian	18
+ Search	

Results 1-10 of 6,104 in 0.27 seconds RELEVANCE DATE uploaded

RECOMMENDED

Sophos Central: How to turn on Remote Assistance 4/15/2016

This article provides Sophos Central Admin customers instructions in enabling Remote Assistance in their Sophos Central Admin Dashboard.

RECOMMENDED

Sophos Endpoint: Disable Tamper Protection 4/8/2013

You must 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.

Current Sophos Status

All systems normal

Current status in effect for 8 days, 10 hours, 13 minutes, and 1 seconds.

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'.

For Critical Cases:

You'll receive a case number when you submit your ticket. Once you have this number, call us for immediate assistance. Select your region below to view the correct number to call.

Select your region

LOGIN TO CHAT

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

The screenshot shows the Sophos Community homepage with a blue header and a large banner at the top. The banner features the text 'CONNECT | ENGAGE | EARN REWARDS' and 'JOIN TODAY!' in white and green. Below the banner is a 'Sophos Partner Program' logo. The main content area includes a 'Current Central Status' section showing 'All systems normal' with a green status indicator, a 'Tweets from @SophosSupport' feed, and a 'Welcome to the Sophos Community' message. There's also a 'Latest Community Release Notes & News' section with three cards: one for Sophos Central Endpoint Protection, one for Staff Spotlight featuring Kay Carlos, and one for managing Login Items in macOS 13 Ventura. The bottom right corner of the page has the 'SOPHOS' logo.

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](https://sophos.com/labs)

## Latest Research



Sophos Named 2022  
Emerging Partner of the Year

10/06/2022

**Sophos wins HashiCorp Emerging  
Partner of the Year 2022**



10/04/2022

**Remove All The Callbacks –  
BlackByte Ransomware Disables  
EDR...**



10/03/2022

**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 navigation is a search bar with the placeholder "Viruses and Spyware" and a "Submit" button. To the right of the search bar is a link to download a free Virus Removal Tool. Further down, there's a section titled "Security Solutions" listing various protection services like Endpoint Protection, Cloud Visibility and Security, and Mobile Security. On the left side, there's a sidebar with a "Latest viruses and spyware" section containing a list of threat names, such as "Troj/Inject-IFL" and "Troj/Formboo-DET". The main content area has a heading "Viruses and Spyware" and a sub-section about finding specific threats. The Sophos logo is in the bottom right corner.

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>



Additional information in  
the notes

## Sophos TechVids

The screenshot shows the homepage of techvids.sophos.com. At the top, there's a dark header bar with the URL 'techvids.sophos.com'. Below it is a white navigation bar with the 'SOPHOS TECHVIDS' logo, social media icons (Twitter, LinkedIn, YouTube), a search bar, and links to 'Sophos Community', 'Documentation', and 'Sophos.com'. The main content area has a blue background. It features a large video player placeholder with the text 'Welcome to Sophos TechVids!' and the Sophos TechVids logo. Below this, there's a section titled 'Browse Videos by Categories' with five categories: 'Intercept X Endpoint' (EP icon), 'Sophos (XG) Firewall' (FW icon), 'Sophos Central' (Central icon), 'Sophos Wireless' (Wi icon), and 'All Videos' (play icon). The 'SOPHOS' logo is in the bottom right corner.

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](https://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](https://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/yBi5NcvMQTBNWVyunmm4u1>

## 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

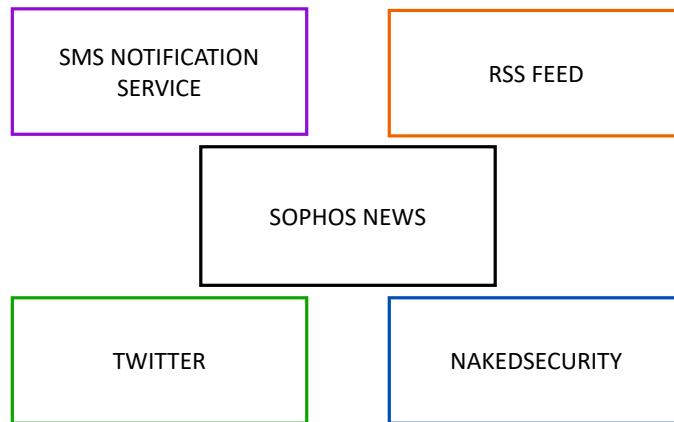
SOPHOS

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>



news.sophos.com

SOPHOS NEWS

Products & Services Security Operations Threat Research AI Research Security News Sophos Life

Featured Articles

RSS



OCTOBER 12, 2022

## Are threat actors turning to archives and disk images as macro usage...

Following Microsoft's announcement that macros from the Internet will be disabled by default, threat actors are using alternative file types for malware delivery. This shift brings both challenges and opportunities for...



THREAT RESEARCH



SOPHOS

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. At the top right is a button labeled "Subscribe to Sophos Notifications". Below the header is a "Current Status" box with a green checkmark and the text "All systems normal". Below this is a "Status Grid" showing the status of various services from October 8 to October 14. Most services are marked as "All systems normal" (green checkmark). The grid includes rows for Central - Partner Dashboard, Central - Admin Dashboard, Central - Enterprise Dashboard, Central - Self Service Portal, Central - Sophos Mail, Phish Threat, Reflexion Mail, Network Related Services, Other Services, and Sophos Home. A "Status Key" at the bottom defines the colors: green for "All systems normal", blue for "Information", orange for "Performance issues", red for "Service disruption", and yellow for "Scheduled maintenance".

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

☰

Overview Press Events Careers Contact Naked Security News

## RSS Feeds

Get our latest updates straight to your computer

We send the breaking news, latest virus alerts, reports of the most prevalent viruses and hoaxes, 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 loading RSS or Atom feeds into a feed reader, you will receive a summary of our latest news, product advisories or virus and hoax 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 as soon as we update our information.

How do I use Sophos info feeds?

- You will need a feed reader to display and subscribe to the feeds. Some news readers are accessed using your browser; some are downloadable applications.
- Drag the RSS or Atom icon for the information feed you want into your feed reader. Or you can click on the RSS or Atom icon and cut and paste the feed's URL into your feed reader.

Can I add these feeds to my website?

Yes! Using an RSS to JavaScript service is a free and very simple way to add our feeds to your own website. After providing a few details, such as the URL of the feed you want to

RSS Feeds

[Sophos Blog](#)

[Naked Security](#)

[Latest virus alerts](#)

[Latest suspicious behavior and file alerts](#)

[Latest PUA alerts](#)

[Latest controlled applications](#)

[Sophos podcasts](#)

[UTM 9 Release Notes](#)

[XG Release 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.

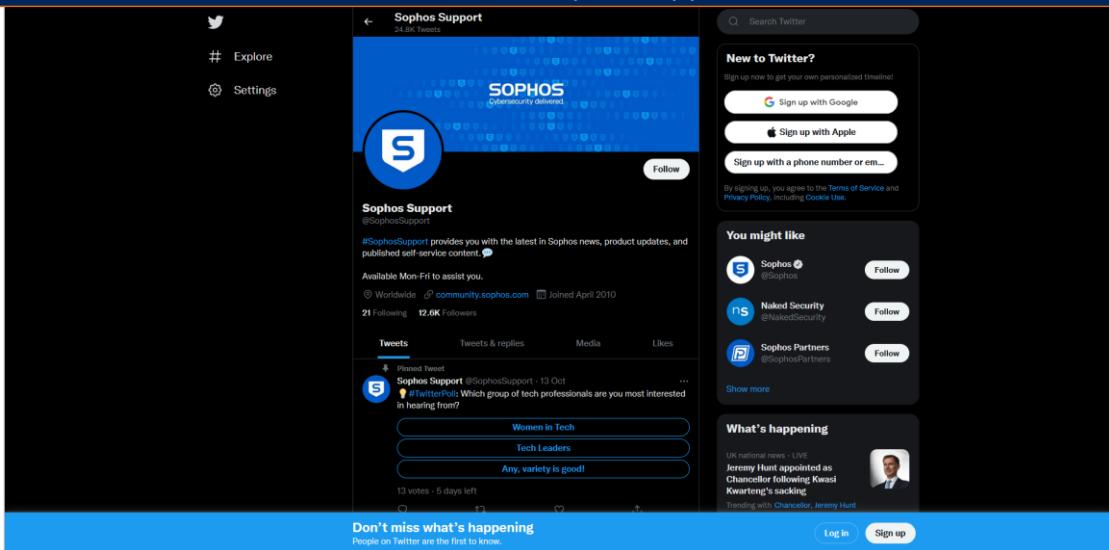
## [Additional Information]

<https://sophos.com/company/rss-feeds>

# Twitter

 Additional information in the notes

twitter.com/sophossupport



The screenshot shows the Twitter profile page for Sophos Support (@SophosSupport). The profile picture is a blue circle with a white 'S'. The bio reads: '#SophosSupport provides you with the latest in Sophos news, product updates, and published self-service content.' It mentions availability 'Available Mon-Fri to assist you.' and location 'Worldwide'. The account has 21 following and 12.6K followers. A pinned tweet from October 13, 2010, asks '#TwitterPoll: Which group of tech professionals are you most interested in hearing from?' with three options: 'Women in Tech', 'Tech Leaders', and 'Any, variety is good!'. The poll has 13 votes and 5 days left. To the right of the profile, there's a 'New to Twitter?' sign-up section, a 'You might like' sidebar with profiles for Sophos (@sophos), Naked Security (@nakedsecurity), and Sophos Partners (@sophospartners), and a 'What's happening' section showing a trending topic about Jeremy Hunt's appointment as Chancellor.

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>

# NakedSecurity



Additional information in  
the notes

nakedsecurity.sophos.com

The screenshot shows the homepage of nakedsecurity.sophos.com. At the top, there's a navigation bar with links for 'PRODUCTS', 'FREE TOOLS', and 'FREE SOPHOS HOME'. Below the navigation is a banner with the text 'Have you listened to our podcast? Listen now' and a link. The main feature is a large article titled 'S3 Ep104: Should hospital ransomware attackers be locked up for life? [Audio + Text]' by Paul Ducklin, dated OCT 13. Below this are three smaller articles: 'Microsoft' (OCT 12), 'Portrait of Ada Lovelace' (OCT 11), and 'Apple' (OCT 11). 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.

`https://www.sophos.com/`

\_\_\_\_\_

SOPHOS

# Chapter Review

Help can be found by navigating to [sophos.com/support](https://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](https://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.

