In confidence

Sophos to Defender Antivirus Migration Guide

Reference:	MDAV-install
Version:	6
Date:	Dec 25
Owner(s):	Ash Green

Lancashire County Council

EDUCATION DIGITAL SERVICES

Contents

Executive summary

This guide is a technical document designed for people providing ICT support within Lancashire schools. It details how to remove the Sophos Central endpoint and how to ensure that Microsoft Defender Antivirus (MDAV) has enabled correctly. It also provides instructions on how to configure MDAV to protect against ransomware.

The document is split into two sections:

1) Workgroup computers. These devices are unmanaged and require manual configuration.
2) Domain managed computers. These devices are managed by one or more servers and the majority of configuration is completed centrally. Devices managed in this way typically enable you to log onto any computer and be able to access your files.

This document should only be followed for machines that are running Microsoft Windows operating systems. IOS and Chromebook devices are out of scope for this document. Please ensure that your Microsoft Windows computers are fully up to date, virus free and are accessible before starting.

This document is not describing how to use Microsoft Defender for Endpoint (MDE). Access to that product is included within some Microsoft agreements and provides an enhanced support experience for Defender.

Schools using Entra to manage devices should review the items outlined for Domain schools, and apply Entra policies accordingly.

Please note

Although Defender will become active on Sophos removal, simply removing Sophos and not configuring Windows Defender is not sufficient to provide appropriate protection for school devices. The security of your data is at risk unless you configure the product appropriately.

1 Workgroup computers

The procedure below walks you through the steps required, and the order to complete them in.

There are a number of steps to complete, in the order of:

1. Identify the machines in scope
2. Disable Sophos tamper protection & remove Sophos
3. Configure Defender
4. Check Defender is working

Each computer will need to be configured individually. Most configuration can occur through the security application, although the Attack Surface Reduction rules can only be enabled through Powershell.

Use of our configuration tool (section 1.1) can help you rapidly configure devices.

Task	Notes	Consideration
Identify machines in scope	• include devices that are turned off • do not include known faulty machines that are being decommissioned	Only windows devices should be considered. Include devices that may be off site.
Disable Sophos Tamper protection	• This prevents Sophos from being uninstalled and needs to be completed first • Tamper Protection - Sophos Central Admin	Tamper protection stops malware from preventing Sophos from running correctly. Turning it off and then leaving an extended period to pass before removing Sophos/enabling Defender is not a good idea. Note that a reboot is required after disabling tamper protection before the removal of Sophos can occur.

Task	Notes	Consideration
Uninstall Sophos Endpoint	• Can be triggered via a program on the device • Uninstall Sophos Endpoint - Sophos Endpoint • Functionality to remove Sophos software by using the the Sophos central console does not remove all components • If you deselect the "reboot" box at the end of uninstallation, you can complete the following steps without needing to wait for a reboot to complete.	• Uninstallation will not complete if there is a Sophos update underway. This cannot occur without Sophos tamper protection being first disabled. Defender automatically enables itself when Sophos is removed. If the software fails to uninstall, SophosZap is the next approach to try: SophosZap: Frequently asked questions
Configure Defender Controlled Folder Access folders and processes.	• Identify each share on each/any of your servers • Update controlled folder access to define each of these shares via the Windows Security app. • Enable folder access - Microsoft Defender for Endpoint | Microsoft Learn • Customize controlled folder access - Microsoft Defender for Endpoint | Microsoft Learn	This is the anti ransomware component of Defender and it is essential that it is configured. Each folder defined will only let known applications write into it – applications can be whitelisted. Blocked attempts can be reviewed within Event Viewer. You should ensure that each defined share on any servers are included on all clients. We recommend this is enabled on all devices.
Configure Defender Attack Surface Reduction (ASR) rules	• Can only be added through powershell or group policy • Enables prevention of a	This enables 15 attack surface reduction methods that are commonly used by malware.

Task	Notes	Consideration
	range of known methods that malware commonly exploit • Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn • Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn (contains the GUID and settings for each rule)	These cannot be configured through the user interface. We recommend these are enabled on all devices.
Enable cloud protection	• This improves the detection behaviour of Defender and is required for some ASR rules • Turn on cloud protection in Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn	Should be on by default
Add scanning exclusions to defender as required	• Some applications require folders and files to be exempted from antivirus scanning. Where these are required, vendors typically publish these lists. • Configure custom exclusions for Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn	Only allow exclusions for computers with affected products. See Appendix 1 for how to use the event log to identify items that have been blocked & need to be added as exceptions.

Task	Notes	Consideration
Confirm Defender is functioning correctly	• Use the EICAR test file to trigger a detection • Antivirus detection test for verifying device's onboarding and reporting services - Microsoft Defender for Endpoint | Microsoft Learn	• This is a legitimate 'test' line of text that antivirus programs recognize and detect. It is the industry standard method of completing this

1.1 Defender AV configuration tool

We have developed a configuration tool for schools to help configuring workgroup computers. Use of this script will:

- Import the Lancashire.gov.uk certificate onto the computer
- Run a signed powershell script to:
    - Configure controlled folder access
    - Configure Attack Surface Reduction rules
    - Set antivirus exceptions based on the applications installed on the computer.
- Remove Sophos

This tool:

- is designed as a starting point – you must configure Controlled Folder access to add in any network shares within the school accessible from this computer. Do not attempt to update the script – as it is signed any editing will render it unusable.
- Should be run on each windows computer (if you wish to use it to configure Defender)

To use:

- Download the zip file from the LCC EDS Hub
- Extract the Zip file by right-clicking and selecting "Extract All...". Tick the box to Show extracted files when complete
- Right-click the "configure_defender.bat" and select "run as administrator".

2 Windows Domain computers

2.1 Approach

Our suggested approach to migrating to Defender Antivirus in a domain environment is to:

- Apply group policies to configure Defender and remove Sophos
- Disable Tamper protection in Sophos, thereby permitting removal
- Arrange for each device to reboot several times.

Our observed results through testing identify that:

- Commonly used devices (office devices, staff devices, regularly used student devices) come over reasonably quickly
- Some devices struggle to migrate – not through error but due to usage. Examples are:
    - Staff devices or staff shared devices that are never actually turned off. These are locked, put to sleep etc by the users. As Group policies that trigger software removal only apply when the computer is fully rebooted and can see it's domain server, it is vital that all users understand they need to be turning their devices off at the end of the day.
    - Student devices that are rarely accessed. These could be older devices within the classrooms, or those laptops in charging units that are 'near the bottom' – and so are rarely used by classes.

Due to this - our recommendation to ICT support teams is to:

- Get the GPOs in place / disable Sophos tamper protection/ get Defender onto servers if necessary
- Advise users to fully shut down their computers daily
- Schedule time several days after the GPOs have been applied to chase down the devices that have not been migrated, and manually reboot them. When all computers have been turned on in school, you can use the Sophos Console to identify the exact machines (and the active users on those machines) that still have Sophos on.

2.2 Servers

Windows servers should be checked first in a school. Unlike Windows 11, Defender does not become deactivated when Sophos is installed. However, many servers have Defender disabled at installation, and it may be necessary to enable the Defender feature first before it works. There are a range of ways in which this may present itself, such as:

- Disabled via group policy
- Disabled at installation
- Removed from the OS

To check, run `get-mpcomputerstatus` in powershell. If it errors, Defender is not enabled and further action is needed.

Two approaches can be used to enable Defender:

1. Existing state	Actions
If the GPO option "Turn off Defender" is enabled	1. Change GPO to "disabled" 2. Run `%ProgramFiles%\Windows Defender\MpCmdRun.exe -wdenable` on the device 3. Confirm defender is active via get-mpcomputerstatus: a. Realtime protection enabled (true) b. AmRunningmode (normal) c. Antivirusenabled (true)
Defender service is disabled and will not start	1. Uninstall Defender components with `dism /online /disable-feature /featurename:windows-defender` 2. `reboot` 3. Reinstall Defender using `dism /online /enable-feature /featurename:windows-defender` 4. `reboot`

Note:

- Add the **local paths** to the controlled folder setting as well as any UNC paths. (i.e. if d:\data is shared as \\devicename\data, both d:\data and \\devicename\data should be configured on that server).
- Ensure that you apply the appropriate exceptions for applications and server roles enabled on the servers.
- Tamper protection is not available for servers using Defender AntiVirus.

2.2.1 Update Cache

If you are using Servers as Update Caches within your school, you should remove these before attempting to remove Sophos from a server. You can check to see if these exist – and remove them if they do – from the Sophos dashboard at https://central.sophos.com/manage/overview/settings-list/update-caches-message-relays .

2.2.2 Server 2016

The modern capability of Microsoft Defender Antivirus only appeared within Server 2016 part way through its lifecycle. In order to get the full functionality we require (including controlled folder access and attack surface reduction rules) it may be necessary to take manual steps on your Server 2016 installations.
To check if you need to update, run `get-MpPreference` within powershell. If the headings of AttackSurfaceReductionRules_Ids and ControlledFolderAccessProtectedFolders exist, you're up to date.

If you do need to update Defender:

1. Ensure that all windows updates are on and applied. This must include the latest cumulative update and the latest defender update.
2. Trigger a signature update from an administrative command prompt using the command:
   `c:\program Files\windows Defender\mpcmdRun.exe -signatureupdate -mmpc`
3. Reboot.

4. To confirm, run `get-MpPreference` within powershell. If the headings of AttackSurfaceReductionRules_Ids and ControlledFolderAccessProtectedFolders exist, you're up to date.

2.2.3 Reboots

Reboots are required on all server devices. Take care to plan these to minimise impact on users. You should ensure all updates are applied before starting, then:

1. Reboot after disabling Sophos tamper protection
2. Reboot if you needed to reinstall Defender in section 2.2.

2.3 Client devices

The procedure below walks you through the steps required, and the order to complete them in. It is important to ensure the settings for Defender are in place before removing Sophos.

There are a number of steps to complete, in the order of:

1. Identify the machines in scope
2. Pre-configure Defender by deploying and configuring group policies
3. Disable Sophos Tamper protection
4. Remove Sophos
5. Check Defender is working
6. Repeat steps 4 and 5 on all devices in scope.

Our group policy templates can be obtained from https://educationdigitalservices-lancashire-gov-uk-admin.ad.lancscc.net/anti-virus-and-threat-protection-service-transition-to-microsoft-defender-antivirus.aspx

Task	Notes	Consideration
Identify machines in scope	• include devices that are turned off • do not include known faulty machines that are being decommissioned • include servers	Only windows devices should be considered. Include devices that may be off site. Knowledge exists to help you:

Task	Notes	Consideration
		1) export list of computers from Sophos Central to see when devices last checked in there 2) Export list of devices from domain controller that have contacted the server in the last 90 days.
Configure Defender Controlled Folder Access folders and processes.	Our template GPOs include the default SIMS shared and Docstorage folders. To fully configure: 1. Identify each share on each of your servers 2. Update client group policies to define each of these shares 3. Update server group policies to protect the local paths to the shares • Enable controlled folder access - Microsoft Defender for Endpoint | Microsoft Learn • Customize controlled folder access - Microsoft Defender for Endpoint | Microsoft Learn	This is the anti malware component of defender and it is essential that it is configured. Each folder defined will only let *known* applications write into it – note that applications can be whitelisted. Blocked attempts can be reviewed within Event Viewer. You should ensure that each defined share on any servers are included in your policies. Policies applied to servers should also include the LOCAL paths to the folders. We recommend this is enabled on all devices.

Task	Notes	Consideration
Configure Defender Attack Surface Reduction (ASR) rules	• Enables prevention of a range of known methods that malware commonly exploit • Our template GPOs enable ASR rules • Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn • Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn (contains the GUID and settings for each rule)	This enables 15 attack surface reduction methods that are commonly used by malware. These cannot be configured through the user interface. We recommend these are enabled on all devices.
Enable cloud protection	• This improves the detection behaviour of Defender and is required for some ASR rules • This is enabled in our template group polices • Turn on cloud protection in Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn	Should be on by default
Add scanning exclusions to defender as required	• Some applications require folders and files to be exempted from antivirus scanning. Where these are required, vendors typically publish these lists.	Only allow exclusions for computers with the affected products. See Section 3 for known exceptions, and Section 5 for identifying items that may need adding to the

Task	Notes	Consideration
	• Our template GPOs include our suggested defaults • Configure custom exclusions for Microsoft Defender Antivirus - Microsoft Defender for Endpoint | Microsoft Learn	exception list.
Remove any Sophos deployment policies	• Group Policy Management Console in Windows | Microsoft Learn	Failure to remove any existing Sophos deployment policy will result in computers reinstalling Sophos after you have removed it
Disable Sophos Tamper protection	• This prevents Sophos from being uninstalled and needs to be completed before uninstallations start. • Tamper Protection - Sophos Central Admin	Tamper protection stops malware from preventing Sophos from running correctly. Turning it off and then leaving an extended period to pass before removing Sophos/enabling Defender is not a good idea. • Note that a reboot is required on devices after disabling tamper protection before the removal of Sophos can occur.
Uninstall Sophos Endpoint	• Can be triggered via a program on the device • Our template GPOs have a dedicated sophos removal GPO. • Uninstall Sophos Endpoint - Sophos Endpoint • Functionality to remove	• Uninstallation will not complete if there is a Sophos update underway. • This can be automated for domains and Intune sites. • This cannot occur without Sophos tamper

Task	Notes	Consideration
	Sophos software by using the the Sophos central console does not remove all components	protection being first disabled.
Confirm Defender is functioning correctly	• Use the EICAR test file to trigger a detection • Antivirus detection test for verifying device's onboarding and reporting services - Microsoft Defender for Endpoint | Microsoft Learn	• This is a legitimate 'test' line of text that antivirus programs recognize and detect. It is the industry standard method of completing this

2.4 Group policies

We have created some Group policy templates to aid schools in migrating to Defender. These will configure Defender AV by:

- Enabling and configuring Defender with AV exclusions
- Enabling and configuring Controlled Folder access with some exceptions
- Enabling and configuring Attack Surface Reduction rules
  These are all provided as templates and act as a 'starting point' to work from. The Controlled Folder Access rules will certainly need updating for your school with entries for each network share within the school. We strongly recommend you review the contents of each and update as necessary.

Name	**Configuration**
Computers – enable remote management	Enables the WinRM service on clients, enabling powershell to be used over the network to retrieve Defender status information
Computers – remove Sophos and set wait time for startup scripts	Triggers the common "SophosUninstall.exe" utility on a device if it is found when the computer starts. This can take a while, so the policy removes the default 10 minute timeout for startup scripts.

Computers – windows defender antivirus settings - servers	• Adds exceptions for:
	  ○ Solus, sims & FMS
	  ○ MECM
	  ○ RBUSS
	  ○ SQL 2019

	• Configures attack surface rules. Sets all to "warn" mode where possible. • Adds ASR exception for RBUSS instantdata process • Enables controlled folder access • Adds sims/fms/solus processes as allowed controlled folder access applications. • Adds default paths for shared$ and Docstorage paths. • Configures a quick scan to run each day at midday

Computers – windows defender antivirus settings – workstations	• Adds exceptions for:
	  ○ Solus, sims & FMS
	  ○ MECM
	• Configures attack surface rules. Sets all to "warn" mode where possible.
	• Enables controlled folder access
	• Adds sims/fms/solus processes as allowed controlled folder access applications.
	• Configures a quick scan to run each day at midday

2.5 SIMS Servers

Sims servers should have c:\windows\temp\GLB*.tmp excluded from controlled folder access. Without this, SIMS deployments will fail.

2.6 MECM devices

Devices that are running the EDS MECM client (typically SIMS servers and devices either installed or supported by EDS) require removal of the ASR rule "Block process creations originating from PSExec and WMI commands". The Workgroup scripts account for this, but GPOs may need to be edited accordingly. The corresponding ASR rule is **d1e49aac-8f56-4280-b9ba-993a6d77406c**

Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn
Back Up and Restore Group Policy in Windows | Microsoft Learn

3 Exception lists

You should only add exceptions based on the applications and roles installed on a given computer. The links below are only a starting point and you should consult the vendor websites for any other applications that you use.

Try to ensure that only appropriate exceptions are allocated to your devices, and to each appropriate part of functionality. Types of Defender feature that can have exceptions set include:

- Antivirus
- Attack Surface Reduction
- Controlled Folder Access

Our GPOs include suggested exclusions that were correct at the time of submission.

Product	URL / exception
Redstor (Remote Backup)	• 008 - Antivirus exclusions : Redstor Help Center
SIMS / SOLUS	**Global Exception List** Trusted Windows Program List •S:\SIMS\Setups\SIMSAMPARKSetup.exe •S:\SIMS\Setups\SIMSApplicationSetup.exe •S:\SIMS\Setups\SIMSManualSetup.exe •D:\SIMS\Sims\Setups\SIMSManualSetup.exe •D:\SIMS\Sims\Setups\SIMSApplicationSetup.exe •D:\SIMS\Sims\Setups\SIMSAMPARKSetup.exe •C:\Program Files\Solus3\AgentService\Sims.Solus3.Agent.OfflineDeployer.exe •C:\Program Files\Solus3\AgentService\Sims.Solus3.Agent.PackageDeployer.exe •C:\Program Files\Solus3\AgentService\Sims.Solus3.Agent.UI.exe •C:\Program Files\Solus3\AgentService\Sims.Solus3.Agent.AgentService.exe **Local Policy Level (Real-Time Scan ONLY Exclusions)** Folders •C:\Program Files\Solus3

Product	URL / exception
	•C:\Program Files (x86)\SIMS\SIMS .net •C:\Program Files (x86)\SIMS\FMSSQL •C:\ProgramData\Capita •C:\ProgramData\Solus 3 Files •C:\Windows\SIMS.INI Controlled folder access:
Windows server roles	• Microsoft Defender Antivirus exclusions on Windows Server - Microsoft Defender for Endpoint | Microsoft Learn (This details the exclusions that are automatically enabled when roles are installed)
SQL Server	• Configure antivirus software to work with SQL Server - SQL Server | Microsoft Learn

4 Glossary

Item	Description
Microsoft Defender AntiVirus (MDAV)	The endpoint protection product that is built into Windows operating systems.
Microsoft Defender for Endpoint (MDE)	A cloud-managed endpoint protection product that provides additional protections and manageability over Microsoft defender antivirus. Available to schools using our cloudschool service.
Controlled folder access	The anti ransomware component of Microsoft Defender antivirus. When enabled this controls access to the system files as well as some user profile areas. Additional folders need to be specified, including any and all network paths that may be written to by any user of that computer. May require additional configuration to add in trusted executable programmes.
Attack surface reduction rules	These provide around 15 additional protections for actions that are commonly compromised by viruses.
Cloud protection	This is required in order for the attack surface reduction rules to work correctly, and improves the functionality of Microsoft defender for antivirus. When Defender antivirus requires additional information about a file it can use cloud systems to improve its knowledge and management of that file.

5 Identifying items that require exception

If you believe that Defender is incorrectly blocking valid applications from working:

1. Review the event logs for Defender. These contain detail regarding the precise programs/paths that have been blocked from conducting activities. They also detail which feature of Defender stopped it (controlled folder access, ASR rules or antivirus). See Microsoft Defender Antivirus event IDs and error codes - Microsoft Defender for Endpoint | Microsoft Learn for detail.
2. Assess the log result and decide whether or not this item requires adding as an exception. This requires technical expertise and contextual knowledge of the application generating the log.
3. To add exceptions:
    a. Antivirus : Configure exclusions for files opened by specific processes - Microsoft Defender for Endpoint | Microsoft Learn
    b. Attack Surface Reduction rules : Enable attack surface reduction rules - Microsoft Defender for Endpoint | Microsoft Learn
    c. Controlled Folder Access : Customize controlled folder access - Microsoft Defender for Endpoint | Microsoft Learn

6 Known issues

1. On uninstallation of Sophos, the device may need a restart before Windows defender becomes fully operational. In testing we have observed:
    a. Defender Tamper protection not enable until the reboot
    b. Defender antivirus did not become active until a reboot.
2. Sophos central cannot uninstall if there is a Sophos update underway. This can be confirmed by running the Sophos endpoint client and selectin the about link. This may affect devices being unable to remove Sophos through a group policy script if Sophos is not up to date. Please ensure that all your computers are up to date and have processed Sophos updates before attempting removal.
3. Computers may fail to add exceptions before Sophos is uninstalled. Running get-computerstatus gives an error. In this circumstance:
    a. Ensure tamper protection is off for Sophos
    b. Disconnect the device from the network (unplug from ethernet lead and/or activate airplane mode)
    c. Uninstall Sophos via add/remove programs

    This should then activate Defender and exclusions can be added. If Sophos won't uninstall, add it back to the network and remove using SophosZap, then go through steps a-c again. Note that SophosZap can leave elements behind.
4. Windows Server 2016 installations that have not been running Windows update correctly may not have upgraded to the modern version of Defender. It is important that the steps in section 2.2.2 are followed – It is not appropriate to just apply the group policy template to such devices unless they have correctly upgraded prior to this point.