

SOPHOS ENDPOINT ADMINISTRATOR

COURSE OVERVIEW

This course is designed for technical professionals who will be administering Sophos Endpoint and provides the skills necessary to manage common day-to-day tasks.

DELIVERY

This course is available online via the Training Portal, or as an instructor-led classroom course. Please contact your Sophos Partner to find out more about the availability of classroom training in your region. Electronic copies of the supporting documents for the course are provided to each trainee via the training portal.

DURATION

This course will take approximately **4 days (32 hours)** to complete.

ASSESSMENT

To complete this course, trainees must take and pass an online assessment. Trainees will have **2.5 hours** to complete the assessment; the pass mark is **80%** and trainees will have **3 attempts** to pass.

OBJECTIVES

On completion of this course, trainees will be able to:

- Plan and deploy complex installations of Sophos Endpoint
- Explain the core configuration concepts of Sophos Endpoint and demonstrate how to configure and implement them
- Perform manual cleanup of threats
- Proactively investigate suspicious activities
- Perform preliminary troubleshooting and basic support steps

PREREQUISITES

There are no prerequisites for this course; however, we recommend that trainees have the following knowledge and experience:

- A good understanding of IT security
- Experience of Windows networking and the ability to troubleshoot issues
- Configuring Active Directory group policies

If you are uncertain whether you meet the necessary requirements, please email us at globaltraining@sophos.com and we will be happy to help.

COURSE AGENDA

Module	Chapter	Duration
1. Sophos Central Overview		
Chapters	<ul style="list-style-type: none"> Introduction to Sophos Endpoint Introduction to Sophos Synchronized Security Getting Started with the Sophos Central Dashboard Getting Started with Global Settings Sophos Endpoint Protection Features and Requirements 	45 minutes
Lab Tasks	Lab Preparation <ul style="list-style-type: none"> Register for a Sophos Central Trial 	10 minutes
2. User Management		
Chapters	<ul style="list-style-type: none"> Introduction to Users in Sophos Central Getting Started with Sophos Central User Management Role-Based User Access Getting Started with Directory Synchronization Configuring Federated Authentication in Sophos Central 	30 minutes
Lab Tasks	<ul style="list-style-type: none"> Install and Configure AD Sync Utility Configure role-based user access 	25 minutes
3. Sophos Endpoint Agent Deployment		
Chapters	<ul style="list-style-type: none"> Getting Started with Sophos Endpoint Agent Deployment Sophos Endpoint Agent Deployment Strategy Getting Started with Sophos Endpoint for Linux Automating Sophos Endpoint Agent Deployment on Windows Automating Sophos Endpoint Agent Deployment on macOS Automating Sophos Endpoint Agent Deployment on Linux 	35 minutes
Lab Tasks	Preparation <ul style="list-style-type: none"> Install Sophos Endpoint on a Windows Server Deploy an Update Cache and Message Relay Sophos Endpoint Agent Deployment <ul style="list-style-type: none"> Install Sophos Endpoint for Linux Use AD GPO to deploy multiple Windows devices 	80 minutes
4. Updating and Communication		
Chapters	<ul style="list-style-type: none"> Getting Started with Sophos Endpoint Updating Advanced Sophos Endpoint Updating Controlling Sophos Endpoint Updates Introduction to Update Caches and Message Relays Getting Started with Update Cache and Message Relay Deployment Considerations when using Sophos Endpoint Update Caches and Message Relays 	30 minutes
5. Virtual Protection		

Chapters	<ul style="list-style-type: none"> Getting Started with Virtual Protection Protecting Azure Hosted Virtual Servers Protecting AWS Hosted Virtual Servers 	20 minutes
6. Device Management		
Chapters	<ul style="list-style-type: none"> Getting Started with Sophos Central Device Management Getting Started with Sophos Central Device Communication Managing Server Protection for Linux Sophos Central Tamper Protection Deleting Devices from Sophos Central 	25 minutes
Lab Tasks	<ul style="list-style-type: none"> Create Server Groups Manage Tamper Protection 	15 minutes
7. Policies		
Chapters	<ul style="list-style-type: none"> Getting Started with Sophos Endpoint Policies Getting Started with the Threat Protection Policy Getting Started with the Peripheral Control Policy Getting Started with the Application Control Policy Getting Started with the Web Control Policy Getting Started with the Data Loss Prevention policy Getting Started with the Sophos Endpoint Exclusions Getting Started with Server File Integrity Monitoring 	65 minutes
Lab Tasks	<p>Investigation Preparation</p> <ul style="list-style-type: none"> Preparation for a later lab task <p>Policies</p> <ul style="list-style-type: none"> Configure and Test Threat Protection Policies Configure and Test Web Control Configure and Test Application Control Configure and Test DLP using CCLs Configure and Test Exclusions Test Linux Server Protection 	90 minutes
8. Remediation and Reports		
Chapters	<ul style="list-style-type: none"> Getting Started with Sophos Endpoint Logs and Reports Getting Started with Sophos Central Health Checks Getting Started with SIEM Integration with Sophos Central Getting Started with Sophos Endpoint Alerts and Events Getting Started with Sophos Endpoint Threat Remediation Getting Started with Sophos Endpoint SafeStore Linux Server Protection threat Detection and Remediation 	50 minutes
Lab Tasks	<ul style="list-style-type: none"> Configure SIEM with Splunk Release a File from SafeStore Remediate a Linux Server Create a Forensic Snapshot and Interrogate the Database 	95 minutes

9. Detection and Response

Chapters	<ul style="list-style-type: none"> ▪ Introduction to Detection and Response ▪ Getting Started with Integrations ▪ Understanding the Unified Context Lake ▪ Investigation Techniques and Search Methods ▪ Getting Started with Detections and Cases ▪ Response Actions and Live Response 	45 minutes
Lab Tasks	<ul style="list-style-type: none"> ▪ Use Data Lake Search to Locate Unauthorized Software ▪ Investigate a Detection 	40 minutes
10. Course Review		
Chapters	<ul style="list-style-type: none"> ▪ How to Find Help from Sophos ▪ Course Review 	10 minutes

FURTHER INFORMATION

If you require any further information on this course, please contact us at globaltraining@sophos.com