Sophos Endpoint Administrator Course Overview

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

Sophos Academy

SOPHOS

Delivery

This course is available online via the Training Portal, or as an instructor-led classroom course. Please contact your CAM or CAE to find out more about the availability of classroom courses 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 **3 hours** to complete the assessment; the pass mark is **80%** and trainees will have **4 attempts** to pass.

Lab Environment

Each trainee is provided with a pre-configured environment that simulates a company network with two sites, a head office, and a branch office.

Objectives

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

- Plan and deploy installations of Sophos Endpoint
- Explain the core configuration concepts of Sophos Endpoint and demonstrate how to configure and implement them
- Perform manual clean-up 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 prerequisites, please email us at globaltraining@sophos.com and we will be happy to help.

Course Agenda

Module	Chapter	Duration
1. Sophos Central Overview		
Chapters	▪ Introduction to Sophos Central ▪ Sophos Endpoint Overview ▪ Introduction to Sophos Synchronized Security ▪ Getting Started with the Sophos Central Dashboard ▪ Getting Started with Sophos Endpoint General Settings ▪ Sophos Endpoint Licenses and Requirements	45 minutes
Lab Tasks	**Lab Preparation** ▪ Register for a Sophos Central Trial	10 minutes
2. User Management		
Chapters	▪ Introduction to Users in Sophos Central ▪ Getting Started with Sophos Central User Management ▪ Sophos Central Role-Based User Access ▪ Getting Started with Directory Synchronization ▪ Configuring Federated Authentication in Sophos Central	30 minutes
Lab Tasks	▪ Install and Configure AD Sync Utility ▪ Configure role-based user access	25 minutes
3. Sophos Endpoint Agent Deployment		
Chapters	▪ Getting Started with Sophos Endpoint Agent Deployment ▪ Sophs 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** ▪ Install Sophos Endpoint on a Windows Server ▪ Deploy an Update Cache and Message Relay **Sophos Endpoint Agent Deployment** ▪ Install Sophos Endpoint for Linux ▪ Use AD GPO to deploy multiple Windows devices ▪ Enable Server Lockdown	80 minutes
3. Updating and Communication		
Chapters	▪ 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

4. Virtual Protection		
Chapters	▪ Getting Started with Virtual Protection ▪ Protecting Azure hosted virtual servers ▪ Protecting AWS hosted virtual servers	20 minutes
5. Device Management		
Chapters	▪ 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	▪ Create Server Groups ▪ Manage Tamper Protection	15 minutes
6. Policies		
Chapters	▪ 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 ▪ Advanced Server Lockdown ▪ Getting Started with Server File Integrity Monitoring	65 minutes
Lab Tasks	**Investigation Preparation** ▪ Preparation for a later lab task **Policies** ▪ Configure and Test Threat Protection Policies ▪ Configure and Test Web Control ▪ Configure and Test App Control ▪ Configure and Test DLP using CCLs ▪ Configure and Test Exclusions ▪ Manage Server Lockdown ▪ Test Linux Server Protection	90 minutes
7. Remediation and Reports		
Chapters	▪ 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	▪ Configure SIEM with Splunk ▪ Release a file from SafeStore ▪ Remediate a Linux Server ▪ Create a Forensic Snapshot and Interrogate the database	95 minutes
8. Detection and Response		

Chapters	▪ Introduction to Sophos Endpoint Detection and Response ▪ Getting Started with Integrations ▪ Getting Started with Data Lake ▪ Sophos Data Lake APIs ▪ Getting Started with Live Discover ▪ Live Discover Query Scheduling and Editing ▪ Live Discover Query Pivoting ▪ Getting Started with Threat Graphs ▪ Getting Started with Detections and Cases ▪ Getting Started with Live Response	45 minutes
Lab Tasks	▪ Use Live Discover to locate unauthorized programs ▪ Investigate a Detection	40 minutes
12. Course Review		
Chapters	▪ 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.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com