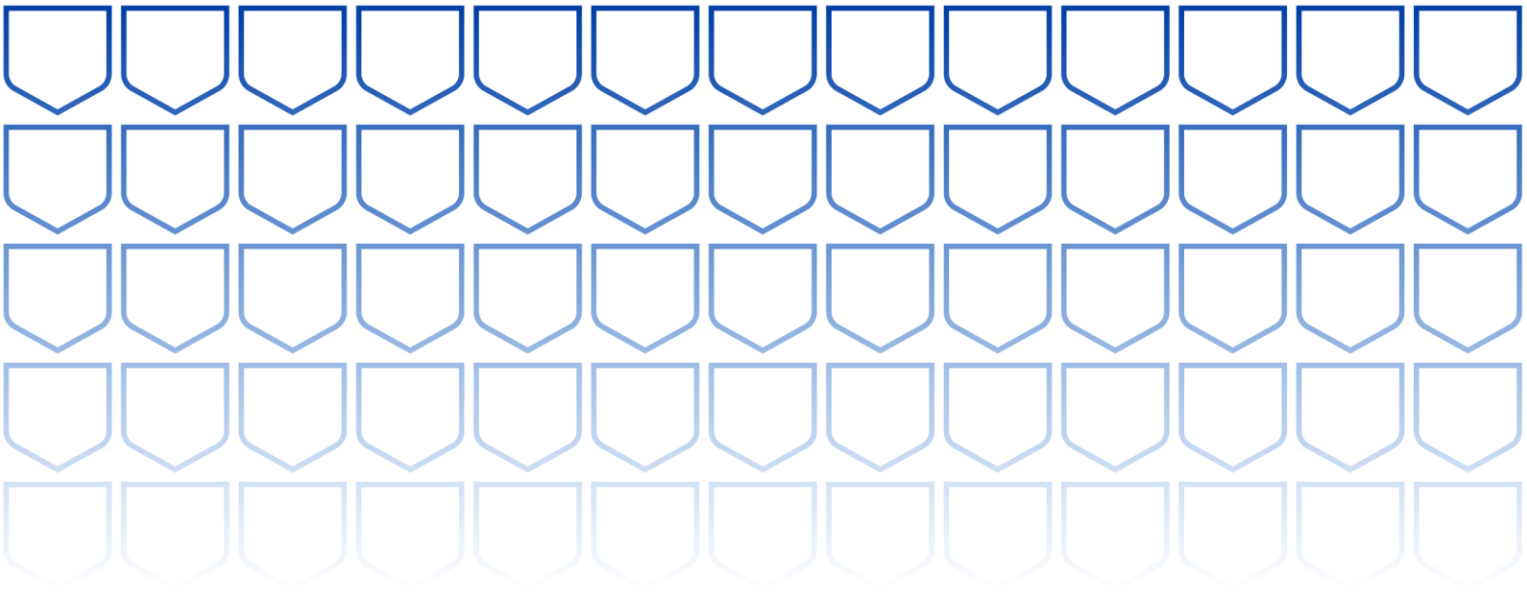

# Sophos Central Administrator Course Overview

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

SOPHOS

## 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 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, which 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 Central
- Explain the core configuration concepts for Sophos Central and demonstrate how to configure and implement them
- Perform manual remediation of threats when required
- Proactively investigate suspicious activities and hunt threats
- 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<br>▪ Sophos Central Protection Overview<br>▪ Introduction to Sophos Synchronized Security<br>▪ Getting Started with the Sophos Central Dashboard<br>▪ Getting Started with Sophos Central General Settings<br>▪ Sophos Central Protection Licenses and Requirements | 55 minutes |
| Lab Tasks | **Lab Preparation**<br><br>▪ Register and activate a Sophos Central Evaluation | 10 minutes |
| **2. Sophos Central User Management** | | |
| Chapters | ▪ Introduction to Users in Sophos Central<br>▪ Getting Started with Sophos Central User Management<br>▪ Sophos Central Role-Based User Access<br>▪ Getting Started with Directory Synchronization<br>▪ Configuring Federated Authentication in Sophos Central | 35 minutes |
| Lab Tasks | **User Management**<br><br>▪ Install and Configure AD Sync Utility<br>▪ Configure Role-Based Access<br><br>**Deployment Preparation**<br><br>▪ Install Sophos Protect on a Windows Server<br>▪ Deploy an Update Cache and Message Relay | 50 minutes |
| **3. Sophos Central Agent Deployment** | | |
| Chapters | ▪ Getting Started with Sophos Central Agent Deployment<br>▪ Sophos Central Agent Deployment Strategy<br>▪ Getting Started with Sophos Server Protection for Linux<br>▪ Automating Sophos Central Agent Deployment on Windows<br>▪ Automating Sophos Central Agent Deployment on macOS<br>▪ Automating Sophos Central Agent Deployment on Linux | 55 minutes |
| Lab Tasks | **Sophos Central Endpoint Agent Deployment**<br><br>▪ Install Sophos Server Protection for Linux<br>▪ Use Active Directory Group Policy to Deploy to Multiple Windows Devices<br>▪ Enable Server Lockdown (preparation for policies lab) | 80 minutes |

| | | |
|---|---|---|
| **4. Sophos Central Updating and Communication** | | |
| Chapters | ▪ Getting Started with Sophos Central Updating<br>▪ Advanced Sophos Central Updating<br>▪ Controlling Sophos Central Updates<br>▪ Introduction to Update Caches and Message Relays<br>▪ Sophos Central Update Cache and Message Relay Deployment<br>▪ Considerations when using Sophos Central Update Caches and Message Relays | 100 minutes |
| **5. Sophos Central Virtual Protection** | | |
| Chapters | ▪ Getting Started with Sophos Central Virtual Protection<br>▪ Protecting Azure hosted virtual servers with Sophos Central<br>▪ Protecting AWS hosted virtual servers with Sophos Central | 25 minutes |
| Simulation Tasks | ▪ Configure Automated Deployment for Azure hosted virtual servers<br>▪ Configure Automated Deployment for AWS hosted virtual servers | 30 minutes |
| **6. Sophos Central Device Management** | | |
| Chapters | ▪ Getting Started with Sophos Central Device Management<br>▪ Getting Started with Sophos Central Device Communication<br>▪ Managing Server Protection for Linux<br>▪ Sophos Central Tamper Protection<br>▪ Deleting devices from Sophos Central | 35 minutes |
| Lab Tasks | **Device Management**<br><br>▪ Create Server Groups<br>▪ Manage Tamper Protection | 45 minutes |
| **7. Sophos Central Policies** | | |
| Chapters | ▪ Getting Started with Sophos Central Policies<br>▪ Getting Started with Sophos Central Threat Protection Policy<br>▪ Getting Started with the Sophos Central Peripheral Control Policy<br>▪ Getting Started with the Sophos Central Application Control Policy<br>▪ Getting Started with the Sophos Central Web Control Policy<br>▪ Getting Started with the Sophos Central Data Loss Prevention Policy<br>▪ Getting Started with Sophos Central Exclusions<br>▪ Getting Started with Sophos Central Server Lockdown<br>▪ Getting Started with Sophos Central Server File Integrity Monitoring | 80 minutes |
| Lab Tasks | **Policies**<br><br>▪ Preparation for a later lab task<br>▪ Configure and Test Threat Protection Policies<br>▪ Configure and Test Web Control<br>▪ Configure and Test Application Control<br>▪ Configure and Test Data Control Using CCLs<br>▪ Configure and Test Exclusions<br>▪ Manage Server Lockdown<br>▪ Test Linux Server Protection | 90 minutes |

| | | |
|---|---|---|
| **8. Sophos Central Remediation and Reports** | | |
| Chapters | ▪ Getting Started with Sophos Central Logs and Reports<br>▪ Getting Started with Sophos Central Health Checks<br>▪ Getting Started with SIEM Integration with Sophos Central<br>▪ Getting Started with Sophos Central Alerts and Events<br>▪ Getting Started with Sophos Central Threat Remediation<br>▪ Getting Started with Sophos Central SafeStore<br>▪ Linux Server Protection Threat Detection and Remediation | 55 minutes |
| Lab Tasks | **Remediation and Reports**<br><br>▪ Configure SIEM with Splunk<br>▪ Release a file from SafeStore<br>▪ Remediate a Linux Server<br>▪ Create a Forensic Snapshot and Interrogate the Database | 95 minutes |
| **9. Sophos Central Detection and Response** | | |
| Chapters | ▪ Introduction to Sophos Central Detection and Response<br>▪ Sophos Central Detection and Response Licensing<br>▪ Getting Started with Integrations<br>▪ Getting Started with Sophos NDR<br>▪ NDR Deployment and Management<br>▪ Getting Started with the Sophos Central Appliance Manager<br>▪ Getting Started with Sophos Central XDR Data Lake<br>▪ Sophos Central XDR Data Lake APIs<br>▪ Getting Started with Sophos Central XDR Live Discover<br>▪ Sophos Central XDR Live Discover Query Scheduling and Editing<br>▪ Sophos Central XDR Live Discover Query Pivoting<br>▪ Getting Started with Sophos Central XDR Threat Graphs<br>▪ Getting Started with Sophos Central XDR Detections and Cases<br>▪ Sophos Central XDR Live Response | 80 minutes |
| Lab Tasks | **Sophos Detection and Response**<br><br>▪ Use Live Discover to Locate Unauthorized Programs<br>▪ Investigate a Detection | 40 minutes |
| **10. Course Review** | | |
| Chapters | ▪ How to find help from Sophos<br>▪ 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



SOPHOS