Sophos Training:

Sophos Central Administrator

This course is designed for technical professionals who will be administering Sophos Central 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 CAM or CAE to find out more about the availability of classroom courses in your region.

Due to the nature of delivery, and the varying experiences of trainees, open discussion is encouraged during this course.

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 a pre-configured lab 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 Central Explain
- the core configuration concepts of 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 training.kenya@clc-africa.com and we will be happy to help.

Course Agenda

1. Sophos Central Overview		
Chapters	▪ An Introduction to Sophos Central ▪ Sophos Central Protection Overview An Introduction to ▪ Sophos Synchronized Security Getting Started with the ▪ Sophos Central Dashboard Getting Started with ▪ Sophos Central Global Settings Sophos Central ▪ Protection Licenses and Requirements	60 minutes
Lab tasks	▪ Register and activate Sophos Central	5 minutes
2. Sophos Central User Management		
Chapters	▪ An introduction to Users in Sophos Central ▪ Getting Started with Sophos Central User Management Sophos ▪ Central role-based user access Getting Started with Directory ▪ Synchronization in Sophos Central Configuring federated ▪ authentication in Sophos Central	40 minutes
Lab tasks	▪ Install and configure Windows AD sync utility ▪ Configure role-based access Deployment preparation tasks ▪ Deploy Sophos protection to a Windows server ▪ Deploy an Update Cache and a Message Relay	80 minutes
3. Sophos Central Agent Deployment		
Chapters	▪ ▪ Getting Started with Sophos Central Agent Deployment ▪ Sophos Central Agent deployment strategy Automating Sophos ▪ Central Agent deployment on Windows Automating Sophos Central ▪ Agent deployment on macOS Automating Sophos Central Agent ▪ deployment on Linux Troubleshooting Manual Deployment on ▪ Windows Troubleshooting Automated Deployment on Windows	70 minutes
Lab tasks	▪ Install Sophos server protection for Linux ▪ Use AD group policy to deploy Sophos protection to multiple devices ▪ Enable server lockdown (preparation for a later lab task)	60 minutes

4. Sophos Central Updating and Communication		
Chapters	▪ Getting Started with Sophos Central Updating ▪ Advanced Sophos Central updating Controlling Sophos Central updates An Introduction to Update Caches and Message Relays ▪ Getting Started with Sophos Central Update Cache and Message Relay Deployment ▪ Considerations for using Sophos Central Update Caches and Message Relays	40 minutes
5. Sophos Central Virtual Protection		
Chapters	▪ Getting Started with Sophos Central Virtual Protection ▪ Protecting Azure hosted virtual servers with Sophos Central ▪ Protecting AWS hosted virtual servers with Sophos Central	30 minutes
Simulation tasks	▪ Configure automated deployment on Azure hosted virtual servers ▪ Configure automated deployment on AWS hosted virtual servers	30 minutes
6. Sophos Central Device Management and Communication		
Chapters	▪ Getting Started with Sophos Central Device Management ▪ Getting Started with Sophos Central Device Communication ▪ Sophos Central Tamper Protection Deleting Devices from Sophos Central	25 minutes
Lab tasks	▪ Create server groups ▪ Manage tamper protection	10 minutes

7. Sophos Central Policies		
Chapters	▪ Getting Started with Sophos Central Policies ▪ Getting Started with the Sophos Central Threat Protection Policy ▪ Getting Started with the Sophos Central Peripheral Control Policy ▪ Getting Started with the Sophos Central Application Control Policy ▪ Getting Started with the Sophos Central Web Control Policy Getting ▪ Started with the Sophos Central Data Loss Prevention Policy Getting ▪ Started with Sophos Central Exclusions Getting Started with Sophos ▪ Central Server Lockdown Getting Started with Sophos Central	80 minutes
Lab tasks	▪ ▪ Server File Integrity Monitoring ▪ Prepare for a later lab task ▪ Configure and test threat protection policies Configure and test web ▪ control Configure and test application control Configure and test ▪ data control using CCLs Configure and text exclusions Manage ▪ server lockdown Test Linux server protection ▪	90 minutes
8. Sophos Central Remediation and Reports		
Chapters	▪ Getting Started with Sophos Central Logs and Reports ▪ Getting Started with Sophos Central Health Checks ▪ Getting Started with SIEM Integration with Sophos Central ▪ Getting Started with Sophos Central Alerts and Events ▪ Getting Started with Sophos Central Threat Remediation ▪ Getting Started with Sophos Central SafeStore Advanced	75 minutes
Lab tasks	▪ Sophso Central Threat Remediation ▪ Configure SIEM with Splunk ▪ Release a file from SafeStore Remediate a Linux server ▪ Create a forensic snapshot and interrogate the database	95 minutes
9. Sophos Central XDR		
Chapters	▪ An Introduction to Sophos Central XDR ▪ Sophos Central XDR Licensing ▪ Getting Started with Sophos Central XDR Data Lake Getting ▪ Started with Sophos Central XDR Live Discover Sophos Central ▪ XDR Live Discover Query Scheduling and Editing Sophos Central ▪ XDR Live Discover query pivoting ▪ Writing queries for Sophos Central XDR Live Discover ▪ ▪ Getting Started with Sophos Central XDR Threat Graphs Getting ▪ Started with Sophos Central XDR Detections and Investigations Getting Started with XDR Live Response	70 minutes

Lab tasks	▪ Use Live Discover to locate unauthorized programs ▪ Investigate a detection using Sophos Central XDR	40 minutes
10. 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 training.kenya@clc-africa.com