Sophos Training:
Sophos Central Architect

This course provides an in-depth study of Sophos Central, designed for experienced technical professionals who will be planning, installing, configuring, and supporting deployments in production environments.

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 **3 days (24 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 3 attempts to pass.

Lab Environment

Each trainee is provided 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 complex installations of Sophos Central
- Explain the core configuration concepts of Sophos Central and demonstrate how to configure and implement them
- Perform manual clean up of threats when required
- Proactively investigate suspicious activities and hunt threats
- Perform preliminary troubleshooting and basic support steps

Prerequisites

Prior to taking this training, trainees should:

- Have completed and passed the **Sophos Central Endpoint and Server Protection – Certified Engineer course**
- Have completed any subsequent delta courses up to version 3.0

We recommend that trainees have the following knowledge and experience:

- Windows networking and the ability to troubleshoot issues
- A good understanding of IT security
- Linux command line for common tasks
- 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

1. Sophos Central Overview		
Chapters	▪ Getting started with SURF	15 minutes
Lab tasks	▪ Register and activate Sophos Central	5 minutes
2. Sophos Central User Management		
Chapters	▪ Sophos Central role-based user access ▪ Advanced directory synchronization in Sophos Central ▪ Configuring federated authentication in Sophos Central	25 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	▪ 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 ▪ Migrating from SEC to Sophos Central	40 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. Device Management and Communication		
Chapters	▪ Advanced Sophos Central updating ▪ Controlling Sophos Central updates ▪ Considerations for using Sophos Central Update Caches and Message Relays ▪ Advanced Sophos Central Update Cache and Message Relay deployment	30 minutes
Lab tasks	▪ Create server groups ▪ Manage tamper protection	15 minutes
5. Sophos Central Virtual Protection		
Chapters	▪ Protecting Azure hosted virtual servers with Sophos Central ▪ Protecting AWS hosted virtual servers with Sophos Central	25 minutes

Simulation tasks	▪ Configure automated deployment on Azure hosted virtual servers ▪ Configure automated deployment on AWS hosted virtual servers	30 minutes
6. Sophos Central Policies		
Chapters	▪ Advanced Sophos Central control policies ▪ Advanced Sophos Central data loss prevention ▪ Advanced Sophos Central policies and exclusions ▪ Getting started with Sophos Central partner global policies ▪ Advanced Sophos Central server lockdown	80 minutes
Lab tasks	▪ 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
7. Sophos Central Remediation and Reports		
Chapters	▪ Getting started with SIEM integration with Sophos Central ▪ Advanced Sophos Central threat remediation ▪ Getting started with Sophos Central forensic snapshots	30 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. Sophos Central XDR		
Chapters	▪ Sophos XDR Data Lake APIs ▪ Sophos Central XDR Live Discover query pivoting ▪ Writing queries for Sophos Central XDR Live Discover ▪ Writing scenarios for Sophos Central XDR Live Discover queries ▪ Using Sophos Central XDR for IT operations ▪ Using Sophos Central XDR for threat hunting	60 minutes
Lab tasks	▪ Use Live Discover to locate unauthorized programs ▪ Investigate a detection using Sophos Central XDR	40 minutes
9. 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.