



Sophos Central Architect

Course Overview

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 discussions are 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 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 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 course, trainee should:

- Have completed and passed the Sophos **Central Endpoint Protection – Certified Engineer course**
- Have completed any subsequent delta courses up to v4.0

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

Module	Chapter	Duration
1. Sophos Central Overview		
Chapters	<ul style="list-style-type: none"> Getting Started with SURF 	10 minutes
Lab Tasks	Lab Preparation <ul style="list-style-type: none"> Register and activate a Sophos Central Evaluation 	10 minutes
2. Sophos Central User Management		
Chapters	<ul style="list-style-type: none"> Sophos Central role-based user access Advanced directory synchronization in Sophos Central Configuring federated authentication in Sophos Central 	25 minutes
Lab Tasks	User Management <ul style="list-style-type: none"> Install and configure Windows AD Sync Utility Configure role-based access Deployment preparation tasks <ul style="list-style-type: none"> Install Sophos protection on a Windows server Deploy an Update Cache and Message Relay 	80 minutes
3. Sophos Central Agent Deployment		
Chapters	<ul style="list-style-type: none"> 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 	40 minutes
Lab Tasks	Sophos Central Endpoint Agent Deployment <ul style="list-style-type: none"> Install Sophos Server Protection for Linux Use AD group policy to deploy Sophos protect multiple devices Enable server lockdown (preparation for a later lab task) 	60 minutes
4. Sophos Central Updating and Communication		
Chapters	<ul style="list-style-type: none"> 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
5. Sophos Central Virtual Protection		
Chapters	<ul style="list-style-type: none"> Protecting Azure hosted virtual servers with Sophos Central Protecting AWS hosted virtual servers with Sophos Central 	25 minutes
Simulation Tasks	<ul style="list-style-type: none"> Configure automated deployment on Azure hosted virtual servers Configure automated deployment on AWS hosted virtual servers 	30 minutes

Sophos Central 5.0v1 Architect Course Overview

6. Sophos Central Device Management		
Chapters	<ul style="list-style-type: none"> Managing Server Protection for Linux 	10 minutes
Lab Tasks	<p>Device Management</p> <ul style="list-style-type: none"> Create server groups Manage tamper protection 	15 minutes
7. Sophos Central Policies		
Chapters	<ul style="list-style-type: none"> 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 	60 minutes
Lab Tasks	<p>Policies</p> <ul style="list-style-type: none"> Preparation 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 Remediation and Reports		
Chapters	<ul style="list-style-type: none"> Getting Started with SIEM integration with Sophos Central Linux Server Protection Threat Detection and Remediation Advanced Sophos Central threat remediation Getting Started with Sophos Central forensic snapshots 	30 minutes
Lab Tasks	<p>Remediation and Reports</p> <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
8. Sophos Central Detection and Response		
Chapters	<ul style="list-style-type: none"> Sophos XDR Data Lake APIs Writing Queries for Sophos Central XDR Live Discover Writing Scenarios for Sophos Central XDR Live Discover Queries Using Sophos Central Detection and Response for IT Operations Using Sophos Central Detection and Response for Threat Hunting 	60 minutes
Lab Tasks	<p>Sophos Detection and Response</p> <ul style="list-style-type: none"> Use Live Discover to locate unauthorized programs Investigate a detection using Sophos Central XDR 	40 minutes

Sophos Central 5.0v1 Architect Course Overview

9. Sophos 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.

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