SOPHOS
Cybersecurity evolved.

Sophos Central
Administrator Course Overview

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.

The course is available either online or as an instructor-led classroom course.

It consists of presentations and practical lab exercises to reinforce the taught content, and electronic copies of the supporting documents for the course will be provided to each trainee through the online portal.

The course is expected to take 3 days (24 hours) to complete, of which approximately 8 hours will be spent on the practical exercises.

Objectives

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

- Design an installation considering all variables.
- Undertake a multi-site installation appropriate for a customer environment.
- Explain the function of core components, how they work and how to configure them.
- Track the source of infections and clean up infected devices.
- Perform preliminary troubleshooting for common problems.

Prerequisites

There are no prerequisites for this course; however, it is recommended that trainees should have:

- Experience with Windows networking and the ability to troubleshoot issues.
- A good understanding of IT security.
- Experience configuring Active Directory Group Policies.
- Experience creating and managing virtual servers or desktops.

If you are uncertain whether you meet the necessary prerequisites to take this course, please email us at globaltraining@sophos.com and we will be happy to help.

Certification

To become a Sophos Certified Administrator, trainees must take and pass an online assessment. The assessment tests their knowledge of both the presented and practical content. The pass mark for the assessment is 80% and is limited to 4 attempts. The time limit for this assessment is 2.5 hours.

Lab Environment

Each student will be provided with a pre-configured environment which simulates a company using a Windows 2016 Domain Controller, a member server, a Windows 10 client, and a Linux server.

Note: The course includes 7 days of access to the virtual lab environment.

Recommended Course Schedule

Day 1	Modules 1 – 4 Labs 1 .1– 4.4
Day 2	Modules 5 – 7 Labs 5.1– 7.1
Day 3	Module 8 – 9 Labs 8.1 – 9.2

Agenda

Module 1: Introduction to Sophos Central (30 mins)

- Explanation of What Sophos Central is and supported browsers.
- Sophos Central Interfaces overview
  - Enterprise Dashboard
  - Self Service Portal
- Sophos Central Admin registration, activation, and sign-in.
- Overview of the toolbar and help sections in the Sophos Central Admin Dashboard.
- Global Settings overview explaining the key settings most used.

Labs (10 mins)

- Register and activate a Sophos Central trial account.

Module 2: User Management (30 mins)

- How to use MFA to secure Sophos Central.
- How to change the authentication type
- How to add users to Sophos Central
- API credential introduction
- Directory Service synchronization
  - Recommendations for AD sync
  - AD Sync Utility Tool information
  - Azure AD Sync information
- User Management
  - User Page and User Groups
  - RBAC

Labs (30 mins)

- **Install and configure the AD Sync Utility Tool**

Module 3: Planning Deployment (40 mins)

- Environment considerations
- Common deployment scenarios + solutions
- Deployment strategy
- The use of pilot groups and outcomes
- Synchronized security overview and use cases.
- Updating overview explaining how Sophos updates
- Controlled updates overview
- Introduction to Update Cache including considerations for use.
- Introduction to Message Relays including considerations for use.

Labs (20 mins)

- Install Sophos protection onto a Windows server.
- Manually control updates.

Module 4: Deployment Part 1 (20 mins)

- Deployment options for EP and SP (protect, email, and bulk).
- Migration from SEC
- Protection of virtual endpoints
- Protecting virtual servers using SVE
- Deployment options for virtual endpoints

Labs (20 mins)

- Deploy an Update Cache and a Message Relay.

Module 4: Deployment Part 2 (30 mins)

- Installation process
- Available installers
- Installation options
- Windows, Mac OS, and Linux deployment examples
- Deployment of update cache and message relay
- Automated deployment options for Windows, Mac OS, and Linux
- Removal of third-party products
- Troubleshooting installations

Labs (55 mins)

- Deploy Sophos protection to a Linux server.
- Prepare deployment using an AD group policy.
- Customize the competitor removal tool.

Module 5: Management (65 mins)

- Manage computers, servers, and groups, including removal of devices.
- Use Tamper Protection to further enhance protection against unauthorised changes.
- Manage Update Caches and Message Relays
- Troubleshooting Update Caches and Message Relays including removal.
- Introduction to policies including general recommendations.
- Policy settings and how to deploy policy changes and enabling new features.
- Global and policy exclusions including use cases and best practice for policies.
- Communication overview and troubleshooting.
- Exporting data from Sophos Central including SIEM integration simulation

Labs (60 mins)

- Prepare for later lab tasks.
- Configure server groups and policies.
- Configure and test threat protection policies.

- Configure and test exclusions.
- Configure and test tamper protection.

Module 6: Threat Protection (45 mins)

- Anatomy of attack walkthrough Identifying the products that are included in Sophos Central.
- Protection features of EP and IX outlined.
- Ransomware attack activity.
- Threat Protection policies.
- Explanation of the protection features provided by EP to control web sites, applications, and peripherals.
- SP features (Server Lockdown and File Integrity Monitoring)

Labs (55 Mins)

- Manage server lockdown.
- Test Linux protection.
- Configure and test Web Control policies.
- Configure and test Application Control policies.

Module 7: Data Management (40 mins)

- Protect sensitive data using Data Loss Prevention and learn how to use custom Content Control Lists (CCLs)
- Identify the available encryption types and the system requirements to allow encryption.
- Email encryption overview and email DLP settings
- Manage Central Encryption for BitLocker and FileVault clients.
- Overview of how to export data from Sophos Central – SIEM

Labs (25 mins)

- Configure and test data control using Content Control Lists.

Module 8: Managing Detections (80 mins)

- Identify the types of threats and detections.
- Respond to alerts and events using reports and logs.
- How to remediate threats and manage quarantined items
- How to investigate potential false positives including submitting samples to Sophos
- How to manage quarantined items
- Clean up malware on a Linux server.
- Explain what EDR is, and what is included in Intercept X with EDR
- Use threat cases to investigate a detection.
- Search for indicators of compromise (IoC) across your network
- Use the self-isolation functionality and understand the requirements for lateral movement protection.
- Post analysis actions
- Live Response introduction and how to get started.
- How to get more information
- SDU log's introduction and demonstration

Labs (40 mins)

- Release a file from SafeStore.
- Disinfect a Linux Server.

Module 9: Threat Hunting (45 mins)

- Threat hunting overview and where to start with threat hunting.
- Threat hunting using threat searches including how to generate file hashes and types of searching.
- Introduction to threat indicators.
- Live Discover introduction including data lake and pivoting.
- What actions to take following a threat hunt.
- How to review your environment including device, malware, protection, and policy health checks.

Labs (30 mins)

- Use Live Discover to hunt for a threat.

- Use Live Discover to locate unauthorized programs.

Further information

If you require any further information on this course, please contact us at globaltraining@sophos.com.