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 3 attempts. The time limit for this assessment is 3 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.

Agenda

Module 1: Sophos Central Overview (60 mins)

- Identify the products that are included in Sophos Central
- Learn about the anatomy of an attack
- See how Synchronized Security enhances protection
- How to access Sophos Central including the dashboard, toolbar and help sections
- Enable Multi-Factor Authentication (MFA)
- **Labs (10 mins)**
    - Register and activate a Sophos Central evaluation

Module 2: Infrastructure Deployment (60 mins)

- How to configure users (including AD Sync) and groups as well as an introduction to the Self Service Portal (SSP)
- Recognize the common deployment challenges
- Understand when Update Caches and Messages Relays can be beneficial
- Deploy Update Caches and Message Relays
- Deploy and manage Sophos Wireless
- Configure Sophos Central Email protection
- **Labs (45 mins)**
    - Install Server Protection
    - Install and Configure AD Sync Utility
    - Deploy an Update Cache and Message Relay

Module 3: Client Deployment (65 mins)

- Understand how the installation process works in different environments
- Automate deployment for Windows, Linux and Mac computers
- Locate and interrogate installation log files
- Troubleshoot common installation issues
- Remove third party products
- Run the Sophos Diagnostic Utility on problematic machines
- Use Tamper Protection to further enhance protection against unauthorised changes
- **Labs (55 mins)**
    - Prepare deployment using Active Directory Group Policy
    - Deploy to a Linux Server using a Script
    - Preparation for Lab 6, enable Server Lockdown
    - Complete installation of DC and CLIENT

Module 4: Threat Protection (40 mins)

- Manage computers, servers, and groups, including removal of devices
- Configure policies to meet your requirements and to follow security best practices
- Know when it is appropriate to configure exclusions and the risks associated with them
- **Labs (25 Mins)**
    - Configure and test threat protection policies
    - Configure and test exclusions
    - Preparation for Lab 8

Module 5: Defense in Depth (40 mins)

- Understand the protection features provided by Endpoint Protection to control web sites, applications and peripherals.
- Use Phish Threat to educate users about security threats
- Configure key settings for Sophos Email, including email security policies
- Manage Sophos Wireless access points and apply key security settings
- **Labs (25 mins)**
    - Configure and test Web Control policies
    - Configure and test Application Control policies

Module 6: Server Protection (30 mins)

- Configure server policies including exclusions
- Use server Lockdown to list the software installed and only allow that software to run in the future
- Server Lockdown emergency recovery and removal
- Configure the File Integrity Monitoring policy to monitor critical Windows system files
- **Labs (45 mins):**
    - Configure server groups and policies
    - Manage server Lockdown
    - Test Linux server protection

Module 7: Data Protection (25 mins)

- Protect sensitive data using Data Loss Prevention and learn how to use custom Content Control Lists (CCLs)
- Identify the different types of encryption available and the system requirements to allow encryption
- Manage Central Encryption for BitLocker and FileVault clients
- **Labs (20 mins):**
    - Configure and test data control using CCLs

Module 8: Protecting Virtual Servers (60 mins)

- Deployment best practices for virtual servers covering the installation of SVM and GVM
- Management and troubleshooting of key server elements
- How to connect an AWS account to Central
- Automating the deployment of Server Protection
- How to connect an Azure account Central
- Automating the deployment of Service Protection
- Deploy Cloud Optix to provide security monitoring, compliance, analytics, and remediation across your public cloud platform

Module 9: Managing Detections (45 mins)

- Identify the types of detection and how to investigate them
- Identify and use the tools available to clean up malware
- How to investigate potential false positives including submitting samples to Sophos
- How to manage quarantined items
- Clean up malware on a Linux server
- **Labs (20 Mins):**
    - Release a file from SafeStore
    - Use the source of infection tool
    - Disinfect a Linux server

Module 10: Endpoint Detection and Response (45 mins)

- 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
- Access and use forensic snapshots to investigate activity on an endpoint
- **Labs (25 mins)**
    - Create a forensic snapshot and interrogate the database
    - Run a threat search and generate a threat case

Module 11: Management (65 mins)

- Use the Controlled Updates policies appropriately
- Use the Enterprise Dashboard to manage multiple sub-estates
- Explain the types of alert in Sophos Central
- Export data from Sophos Central into a SIEM application
- Use the Sophos Central logs and reports to check the health of your estate
- Perform a health check of the environment
- **Labs (25 mins)**
  - Enable Manually Controlled Updates
  - Configure SIEM with Splunk

Further information

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