Sophos Certified Architect – Course overview

SafeGuard Encryption

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

The course is intended to be delivered in a classroom setting, and consists of presentations and practical lab exercises to reinforce the taught content. Printed copies of the supporting documents for the course will be provided to each trainee.
If the course is being taught via webinar then the documents will be sent electronically to the trainees, who are encouraged to print them out to keep as a reference.

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

The course lasts 3 days, of which roughly 7 hours will be spent on the practical exercises.

Objectives

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

- Size, scope and architect a SafeGuard Enterprise solution to fit a customer's environment.
- Install and configure SafeGuard Enterprise according to best practice.
- Troubleshoot individual SafeGuard Enterprise components.
- Describe the advanced architecture and features of SafeGuard Enterprise.

Prerequisites

Prior to attending this course, trainees should:

- Complete the SafeGuard Encryption Certified Engineer course.
- Be comfortable talking about each of the SafeGuard Enterprise modules, and the value that they provide.
- Be able to demonstrate basic functionality within the product.
- Have installed and managed an environment containing a SafeGuard server and clients.
- Have sufficient knowledge to troubleshoot and resolve Windows networked environments.

If you are uncertain whether you meet the necessary prerequisites to attend this course, please email us at training@exclusive-networks.be and we will be happy to help.

Certification

To achieve the Sophos Certified Architect certification in SafeGuard Encryption trainees must take and pass an online assessment. The assessment tests their knowledge of both the taught and practical content. The pass mark for the assessment is 80%, and it may be taken a maximum of three times.

Agenda

- Module 1: Engineer course recap
  - Product overview
  - SafeGuard Management Center
  - Device Encryption
  - Native Device Encryption
  - Data Exchange
  - Encryption for File Shares
  - Encryption for Cloud Storage
  - Mobile Encryption
- Module 2: Preparation
  - System requirements
  - SSL
  - Internet Information Services (IIS)
  - Users and groups
  - SQL configuration
  - Database connection test
- Module 3: Installation
  - Overview
  - SGN Server
  - SafeGuard database
  - Management Center
  - Server configuration package
  - Additional Management Centers
  - Web Help Desk
  - Troubleshooting
- Module 4: Server configuration
  - Licensing
  - Active Directory synchronization
  - Scheduling
  - Manually created objects
  - Security officers
  - Client configuration package
  - Installation overview revisited
  - BitLocker management
  - Reporting
  - Auditing
- Module 5: Client Deployment
  - System requirements
  - Preparation
  - Installation overview
  - Deployment strategy
  - Standalone clients
  - Client configuration package

- User machine assignment
- POA users and groups
- System tray application
- Troubleshooting

- Module 6: Policies
  - Recap
  - Policies
    - Authentication
    - General Settings
    - Logging
    - Password
    - PIN
    - Passphrase
    - Specific Machine Settings
    - Disk Encryption
    - Data Exchange
    - File Shares
    - Cloud Storage
  - Policy groups
  - Inheritance
  - Troubleshooting
- Module 7: Client architecture
  - Boot process
  - SafeGuard kernel
  - Encryption keys
  - Volume-based encryption
  - File-based encryption
  - Volume vs. file-based encryption
  - Decommissioning
- Module 8: Recovery
  - Logon
  - Logon recovery
  - Client recovery
  - Virtual client
  - Server and database recovery
  - Disaster recovery planning
- Module 9: Upgrading
  - Process overview
  - Server upgrade
  - Client upgrade
  - Troubleshooting
- Module 10: Advanced management
  - Multi tenancy
  - DMZ server
  - SGN Server configuration
  - Sophos encryption to SSL conversion
  - Load balancing
  - Database replication
  - Database maintenance
  - Scripting API

- Token and smartcard support
- Middleware support
- Using tokens

Further information

If you require any further information on this course, please contact the Sophos Training team at globaltraining@sophos.com.