

Implementing Cisco Secure Access Solutions (SISAS)

Duration 5 Days

COURSE CONTENT

Implementing Cisco Secure Access Solutions (SISAS) v1.0 is a newly created five-day instructor-led training course that is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience so that they can deploy Cisco's Identity Services Engine and 802.1X secure network access. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed network access security by utilizing Cisco ISE appliance product solution. The student will gain hands-on experience with configuring various advance Cisco security solutions for mitigating outside threats and securing devices connecting to the network. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco's ISE appliance feature and provide operational support identity and network access control.

COURSE OBJECTIVE

Upon completing this course, the learner will be able to meet these overall objectives:

- Understand Cisco Identity Services Engine architecture and access control capabilities.
- Understand 802.1X architecture, implementation and operation.
- Understand commonly implemented Extensible Authentication Protocols (EAP).
- Implement Public-Key Infrastructure with ISE.
- Understand the implement Internal and External authentication databases.
- Implement MAC Authentication Bypass.
- Implement identity based authorization policies.
- Understand Cisco TrustSec features.
- Implement Web Authentication and Guest Access.
- Implement ISE Posture service.
- Implement ISE Profiling.
- Understand Bring Your Own Device (BYOD) with ISE.
- Troubleshoot ISE

COURSE OUTLINE

Module 1 : Threat Mitigation through Identity Services

- Identity Services
- 802.1X and EAP
- Configure 802.1X Components

Module 2 : ISE Fundamentals

- Describe Cisco ISE Features and configure the fundamentals
- Cisco ISE with PKI
- Cisco ISE Authentication
- Cisco ISE with External Authentication

Module 3 : Advance Access Control

- Certificate Based User Authentication
- Authorization
- Cisco TrustSec

Module 4 : Web Authentication and Guest Access

- Web Authentication
- Guest Access Services

Module 5 : Endpoint

- Posture
- Profiler
- BYOD

Module 6 : Troubleshooting Network Access Control

- Troubleshooting ISE

LABS

- Lab 1: Installing a Certificate in ISE
- Lab 2: Local/Remote Identity Stores with Active Directory/LDAP and Sequence Lists
- Lab 3: Examining and Configuring Supplicants
- Lab 4: 802.1X: Wired Networks
- Lab 5: 802.1X: MAR and EAP Chaining

- Lab 6: 802.1X: MAC Authentication Bypass
- Lab 7: Implement Central WebAuth
- Lab 8: Implement Guest Access and My Device Portal
- Lab 9: Implement Posture Service
- Lab 10: Implement the Profile Service
- Lab 11: Implementing TrustSec and MACsec

WHO SHOULD ATTEND

- Channel Partner / Reseller
- Customer
- Employee

PREREQUISITES

- CCNA Security or valid CCSP.
- or any CCIE certification can act as a prerequisite