CS-SISE

CCNP SECURITY IDENTITY MANAGEMENT SISE 300-715

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Professional	Cisco Security	ILT / VILT	NA

INTRODUCTION

This 5-day course is aligned with the objectives for the CCNP Security SISE exam and will help you master topics such as:

- Architecture and deployment
- Policy enforcement
- Web Authentication and guest services
- Profiler
- BYOD
- Endpoint compliance
- Network access device administration

AUDIENCE PROFILE

This course is primarily intended for:

- Cisco partners and integrators, ISE administrators, Network and Wireless network security engineers
- Individuals preparing for the CCNP Security Certification, specifically the SISE elective.

PREREQUISITES

There are no formal prerequisites for CCNP Security. In other words, you do not have to pass the CCNA Security or any other certifications to take CCNP-level exams. On the other hand, CCNP candidates often have three to five years of experience in IT and cybersecurity.

The ideal knowledge and skills that a learner should have before attending this course are as follows:

- Be Familiar with Microsoft Windows Operating System
- Familiar with 802.1X and with Cisco's secure mobility client – AnyConnect
- Familiar with Cisco's IOS CLI

COURSE OBJECTIVES

On completion of this course, participants should be familiar with:

Architecture and Deployment:

- Configure Personas
- Describe Deployment Options

Policy Enforcement:

- Configure native AD and LDAP
- Describe identity store options
- Configure wired/wireless 802.1x network access
- Explain the importance of an endpoint patching strategy
- Configure 802.1x phasing deployment

- Configure network access devices
- Implement MAB
- Configure Cisco TrustSec
- Configure policies including authentication and authorization profiles

Web Auth and Guest Services:

- Configure web authentication
- Configure guest access services
- Configure sponsor and guest portals

Profiler:

- Implement profiler services
- Implement probes
- Implement CoA
- Configure endpoint identity management

BYOD:

- Describe Cisco BYOD functionality
- BYOD device onboarding using internal CA with Cisco switches and Cisco wireless LAN controllers
- Configure certificates for BYOD
- Configure blacklist/whitelist

Endpoint Compliance:

- Describe endpoint compliance, posture services, and client provisioning
- Configure posture conditions and policy and client provisioning
- Configure the compliance module
- Configure Cisco ISE posture agents and operational modes
- Describe supplicant, supplicant options, authenticator, and server

Network Access Device Management:

- Compare AAA protocols
- Configure TACACS+ device administration and command authorization

COURSE CONTENT

Lesson 1: Fundamentals of AAA
- Comparing and Selecting AAA Options
- TACACS+
- RADIUS
- Comparing RADIUS and TACACS+

Lesson 2: Identity Management
- What Is an Identity?
- Identity Stores
- Identity Source Sequences
- Special Identity Sources

Lesson 3: Extensible Authentication Protocol (EAP) over LAN: 802.1X
- Extensible Authentication Protocol
- EAP over LAN (802.1X)
- Supplicant Options

Lesson 4: Non-802.1X Authentication
- Devices Without a Supplicant
- MAC Authentication Bypass
- Web Authentication
- Remote-Access Connections
- EasyConnect

Lesson 5: Introduction to Advanced Concepts
- Change of Authorization
- Automating MAC Authentication Bypass (MAB)
- Posture Assessment
- Mobile Device Management (MDM)

Lesson 6: Cisco Identity Services Engine Architecture
- What Is Cisco ISE?
- Personas
- Physical or Virtual Appliances
- ISE Deployment Scenarios

Lesson 7: Cisco ISE Graphical User Interface (GUI)
- Logging in to ISE
- Organization of the ISE GUI
- Types of Policies in ISE

Lesson 8: Initial Configuration of Cisco ISE
- Cisco Identity Services Engine Form Factors
- Bootstrapping Cisco ISE

- Network Devices
- ISE Identity Stores

Lesson 9: Authentication Policies

- The Relationship Between Authentication and Authorization
- Authentication Policy
- Understanding Policy Sets
- Understanding Authentication Policies
- Common Authentication Policy Examples
- More on MAB
- Restore the Authentication

Lesson 10: Authorization Policies

- Authentication Versus Authorization
- Authorization Policies
- Saving Conditions for Reuse

Lesson 11: Implement Wired and Wireless Authentication

- Authentication Configuration on Wired Switches
- Authentication Configuration on WLCs
- Verifying Dot1x and MAB

Lesson 12: Web Authentication

- Web Authentication Scenarios
- Configuring Centralized Web Authentication
- Building CWA Authorization Policies
- Verifying Centralized Web Authentication

Lesson 13: Guest Services

- Guest Services Overview
- Portals, Portals, and More Portals!
- Configuring Guest Portals and Authorization Rules
- Sponsors
- SAML Authentication

Lesson 14: Profiling

- ISE Profiler
- Infrastructure Configuration
- Profiling Policies
- ISE Profiler and CoA
- Profiles in Authorization Policies
- Verify Profiling

Lesson 15: Certificate-Based Authentication

- Certificate Authentication Primer
- A Common Misconception About Active Directory
- EAP-TLS
- Configuring ISE for Certificate-Based Authentications

Lesson 16: Bring Your Own Device

- BYOD Challenges
- Onboarding Process
- Configuring NADs for Onboarding
- ISE Configuration for Onboarding
- BYOD Onboarding Process Detailed
- Verifying BYOD Flows
- MDM Onboarding
- Managing Endpoints
- The Opposite of BYOD: Identify Corporate Systems

Lesson 17: TrustSec and MACsec

- Ingress Access Control Challenges
- What Is TrustSec?
- What Is a Security Group Tag?
- What Is the TrustSec Architecture?
- TrustSec-Enabled Network Access Devices
- Network Device Admission Control (NDAC)
- Defining the SGTs
- Classification
- Transport: SGT Exchange Protocol (SXP)
- Transport: Native Tagging
- Enforcement
- Software-Defined Access (SD-Access)
- MACsec

Lesson 18: Posture Assessment

- Posture Assessment with ISE
- Configuring Posture
- The Endpoint Experience
- Mobile Posture

Lesson 19: Deploying Safely

- Why Use a Phased Approach?
- Comparing authentication open to Standard 802.1X
- Prepare ISE for a Staged Deployment
- Monitor Mode
- Low-Impact Mode
- Closed Mode
- Transitioning from Monitor Mode to Your End State
- Wireless Networks

Lesson 20: ISE Scale and High Availability

- Configuring ISE Nodes in a Distributed Environment
- Understanding the High Availability Options Available
- Using Load Balancers
- Maintaining ISE Deployments

Lesson 21: Troubleshooting Tools

- Logging
- Diagnostic Tools
- Troubleshooting Methodology
- Troubleshooting Outside of ISE

Lesson 22: ISE Context Sharing and Remediation

- Integration Types in the ISE Ecosystem
- pxGrid

Lesson 23: Threat Centric NAC

- Vulnerabilities and Threats, Oh My!
- Integrating Vulnerability Assessment Sources
- Integrating with Threat Sources

Lesson 24: Device Administration AAA with ISE

- Device Administration AAA Refresher
- Device Administration in ISE
- Device Administration Global Settings
- Device Administration Work Center

Lesson 25: Configuring Device Administration AAA with Cisco IOS

- Overview of IOS Device Administration AAA
- Configure ISE and an IOS Device for Device Administration AAA
- Testing and Troubleshooting

Lesson 26: Configuring Device Admin AAA with the Cisco WLC

- Overview of WLC Device Administration AAA
- Configure ISE and the WLC for Device Administration AAA
- Testing and Troubleshooting

ASSOCIATED CERTIFICATIONS & EXAM

The Implementing and Configuring Cisco Identity Services Engine (SISE 300-715) exam are one of the elective options for the CCNP Security certification. Passing the associated exam certifies your knowledge of Cisco Identify Services Engine, including architecture and deployment, policy enforcement, Web Auth and guest services, profiler, BYOD, endpoint compliance, and network access device administration.