Document Generated: 11/24/2026

Learning Style: Virtual Classroom

Technology: Cisco

Difficulty: Intermediate

Course Duration: 5 Days

Implementing and Configuring Cisco Identity Services Engine (SISE) v5.x



About This Course:

This 5-day Cisco ISE training program discusses the Cisco Identity Services Engine, an identity and access control policy platform that provides a single policy plane across the entire organization, combining multiple services, including authentication, authorization, and accounting (AAA), posture, profiling, device onboarding, and guest management, into a single context-aware identity-based platform. This CCNP course provides students with the knowledge and skills to enforce security posture compliance for wired and wireless endpoints as well as enhance infrastructure security using the Cisco ISE.

Course Objectives:

- Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture. Describe the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages
- Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services
- Describe how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization
- Describe third-party Network Access Devices (NADs), Cisco TrustSec®, and Easy Connect
- Describe and configure web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios
- Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints. Describe best practices for deploying this profiler service in your specific environment
- Describe BYOD challenges, solutions, processes, and portals. Configure a BYOD solution, and describe the relationship between BYOD processes and their related configuration components. Describe and configure various certificates related to a BYOD solution
- Describe the value of the My Devices portal and how to configure this portal
- Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE
- Describe and configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understand the role of TACACS+ within the Authentication, Authentication, and Accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols
- Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool

Audience:

The primary audience for this course is as follows:

- Network security engineers
- ISE administrators
- Wireless network security engineers
- Cisco integrators and partners

Prerequisites:

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

- Familiarity with the Cisco IOS® Software Command-Line Interface (CLI)
- Familiarity with Cisco AnyConnect® Secure Mobility Client
- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1X

Recommended Cisco learning offerings that may help you meet these prerequisites:

- Cisco CCNP® Security Certification training
- Introduction to 802.1X Operations for Cisco Security Professionals (802.1X)

Course Outline:

?Module 1: Introducing Cisco ISE Architecture and Deployment

- Lesson 1: Using Cisco ISE as a Network Access Policy Engine
- Lesson 2: Introducing Cisco ISE Deployment Models

Module 2: Cisco ISE Policy Enforcement

- Lesson 1: Introducing 802.1x and MAB Access: Wired and Wireless
- Lesson 2: Introducing Identity Management
- Lesson 3: Configuring Certificate Services
- Lesson 4: Introducing Cisco ISE Policy
- Lesson 5: Configuring Cisco ISE Policy Sets
- Lesson 6: Implementing Third-Party Network Access Device Support
- Lesson 7: Introducing Cisco TrustSec
- Lesson 8: Introducing EasyConnect

Module 3: Web Authentication and Guest Services

- Lesson 1: Introducing Web Access with Cisco ISE
- Lesson 2: Introducing ISE Guest Access Components
- Lesson 3: Configuring Guest Access Settings
- Lesson 4: Configuring Portals: Sponsors and Guests

Module 4: Cisco ISE Profiler

- Lesson 1: Introducing Cisco ISE Profiler
- Lesson 2: Configuring Cisco ISE Profiling

Module 5: Cisco ISE BYOD

- Lesson 1: Introducing the Cisco ISE BYOD Process
- Lesson 2: Describing BYOD Flow
- Lesson 3: Configuring My Devices Portal Settings
- Lesson 4: Configuring Certificates in BYOD Scenarios

Module 6: Cisco ISE Endpoint Compliance Services

- Lesson 1: Introducing Endpoint Compliance
- Lesson 2: Configuring Client Posture Services and Provisioning in Cisco ISE

Module 7: Cisco ISE with AMP and VPN-Based Services

- Lesson 1: Introducing VPN Access Using Cisco ISE
- Lesson 2: Configuring Cisco AMP for ISE

Module 8: Cisco ISE Integrated Solutions with APIs

- Lesson 1: Introducing Location-Based Authorization
- Lesson 2: Introducing Cisco ISE pxGrid

Module 9: Working with Network Access Devices

- Lesson 1: Configuring TACACS+ for Cisco ISE Device Administration

Module 10: Cisco ISE Design

- Lesson 1: Designing and Deployment Best Practices
- Lesson 2: Performing Cisco ISE Installation and Configuration Best Practices
- Lesson 3: Deploying Failover and High-Availability

Module 11: Configuring Third Party NAD Support

- Lesson 1: Configuring Third-Party NAD Support

Lab Outline:

Current Lab Software is ISE Version 3.x

Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Lab 1: Configure Initial Cisco ISE Setup, GUI Familiarization, System Certificate Usage
- Lab 2: Integrate Cisco ISE with Active Directory

- Lab 3: Configure Basic Policy on Cisco ISE
- Lab 4: Configure Conversion to Policy Sets
- Lab 5: Configure Guest Access
- Lab 6: Configure Guest Access Operations
- Lab 7: Create Guest Reports
- Lab 8: Configure Profiling
- Lab 9: Customize the Cisco ISE Profiling Configuration
- Lab 10: Create Cisco ISE Profiling Reports
- Lab 11: Configure BYOD
- Lab 12: Blacklisting a Device
- Lab 13: Configure Compliance Services on Cisco ISE
- Lab 14: Configure Client Provisioning
- Lab 15: Configure Cisco ISE for Basic Device Administration
- Lab 16: Configure TACACS+ Command Authorization

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges