

Implementing and Configuring Cisco Identity Services Engine (SISE) V4.1

Implementing and Configuring Cisco Identity Services Engine (SISE) V4.1

The Implementing and Configuring Cisco Identity Services Engine (SISE) v4.1 training teaches you to deploy and use Cisco® Identity Services Engine (ISE) v3.x, an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and virtual private network (VPN) connections. This hands-on training provides you with the knowledge and skills to implement and apply Cisco ISE capabilities to support use cases for Zero Trust security posture. These use cases include tasks such as policy enforcement, profiling services, web authentication and guest access services, Bring Your Own Device (BYOD), endpoint compliance services, and Terminal Access Controller Access Control Server (TACACS+) device administration. Through hands-on practice via lab exercises, you will learn how to use Cisco ISE to gain visibility into what is happening in your network, streamline security policy management, and contribute to operational efficiency.

This training prepares you for 300-715 SISE v1.1 exam. If passed, you earn the Cisco Certified Specialist – Security Identity Management Implementation certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification. This training also earns you 40 Continuing Education (CE) credits toward recertification.

How you'll benefit

This class will help you:

- Develop and implement SASE architecture
- Understand application of ISE capabilities towards development of a Zero Trust approach
- Enable BYOD and guest access
- Centrally configure and manage posture, authentication, and authorization services in a single web-based GUI console
- Gain leading-edge career skills for high-demand job roles and responsibilities focused on enterprise security
- Prepare for the 300-715 SISE v1.1 exam
- Earn 40 CE credits toward recertification

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Network Security Engineers
- Administrators

Course Duration

5 days

Course Price

\$4,295.00 or 43 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Prerequisites

To fully benefit from this course, you should have the following knowledge:

- Familiarity with the Cisco IOS® Software Command-Line Interface (CLI) for wired and wireless devices
- Familiarity with Cisco Secure Client
- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1X

OUTLINE

Module 1: Introducing Cisco ISE Architecture

- Cisco ISE as a Network Access Policy Engine
- Cisco ISE Use Cases
- Cisco ISE Functions

Module 2: Introducing Cisco ISE Deployment

- Cisco ISE Deployment Models
- Cisco ISE Licensing and Network Requirements
- Cisco ISE Context Visibility Features
- New Features in Cisco ISE 3.X

Module 3: Introducing Cisco ISE Policy Enforcement Components

- 802.1X for Wired and Wireless Access
- MAC Authentication Bypass for Wired and Wireless Access
- Identity Management
- Active Directory Identity Source
- Additional Identity Sources
- Certificate Services

Module 4: Introducing Cisco ISE Policy Configuration

- Cisco ISE Policy
- Cisco ISE Authentication Rules
- Cisco ISE Authorization Rules

Module 5: Troubleshooting Cisco ISE Policy and Third-Party NAD Support

- Cisco ISE Third-Party Network Access Device Support
- Troubleshooting Cisco ISE Policy Configuration

Module 6: Exploring Cisco TrustSec

- Cisco TrustSec Overview
- Cisco TrustSec Enhancements
- Cisco TrustSec Configuration

Module 7: Introducing Web Authentication and Guest Services

- Web Access with Cisco ISE
- Guest Access Components
- Guest Access Settings

Module 8: Configuring Hotspots and Guest Portals

Module 9: Configuring Cisco ISE BYOD

- Cisco ISE BYOD Solution Overview
- Cisco ISE BYOD Flow
- My Devices Portal Configuration
- Certificate Configuration in BYOD Scenarios

Module 10: Working with Network Access Devices

- Reviewing AAA
- Cisco ISE TACACS+ Device Administration
- Configuring TACACS+ Device Administration
- TACACS+ Device Administration Guidelines and Best Practices
- Migration from Cisco ACS to Cisco ISE

Module 11: Introducing the Cisco ISE Profiler

- ISE Profiler Overview
- Cisco ISE Probes
- Profiling Policy

Module 12: Introducing Profiling Best Practices and Reporting

- Profiling Best Practices

Module 13: Introducing Cisco ISE Endpoint Compliance Services

- Endpoint Compliance Services Overview

Module 14: Configuring Client Posture Services and Compliance

- Configuring Client Posture Services and Compliance
- Client Posture Services and Provisioning Configuration

LAB OUTLINE (these labs are Custom to CTCLC)

Lab 0: Lab Access via View Horizon Client

Lab 1: Cisco ISE GUI Familiarization and Initial Configuration

Lab 2: MAB Authentication

Lab 3: Integrate 9K-Client Switch and ISE

Lab 4: Create Policies for Domain Computers

Lab 5: Create Policies for Employee

Lab 6: Create Policies for Contractors

Lab 7: Create Policies for the Wireless Users

Lab 8: Configure Hotspot Portal

Lab 9: Client Testing – Hotspot Portal

Lab 10: Configure Self-Registration Portal

Lab 11: Configure Self-Registration Portal with Sponsor Approval

Lab 12: Configure Sponsored Guest Portal

Lab 13: Configure Profiling

Lab 14: Configure Profiling for Cisco IP Phone

Lab 15 (Optional): Create Cisco ISE Profiling Reports

Lab 16: Configure BYOD

Lab 17: BYOD Device Management

Lab 19: Configure Posture Compliance Services on Cisco ISE

Lab 20: Configure Client Provisioning Portal

Lab 21: Configure Posture Elements and Posture Policy

Lab 22: Posture Authorization Profiles and Policy Sets

Lab 23: Test Compliance Policy for BYOD User

Lab 24: Agentless Posture

Lab 25: Configure Cisco ISE for Basic Device Administration

Lab 26: Configure TACACS+ Command Authorization

Lab 27: Configure Cisco TrustSec