

Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0

Course Duration: 40 Hours

Course Code: SISE v4.0

1. Course Overview

The **Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0** course provides in-depth knowledge and hands-on skills required to deploy, configure, and manage Cisco Identity Services Engine (ISE). This course covers key concepts such as policy enforcement, profiling services, guest access, BYOD, and TACACS+. You will gain practical experience through real-world labs to effectively secure and streamline access to network resources.

2. What You'll Learn?

By the end of this course, you will be able to:

- Understand the architecture and components of Cisco ISE.
- Deploy and configure Cisco ISE for secure network access.
- Implement authentication, authorization, and accounting (AAA) policies.
- Configure profiling, posture, and BYOD policies.
- Integrate Cisco ISE with external services and solutions.
- Manage guest access, secure wired/wireless access, and VPN connectivity.
- Implement TACACS+ for device administration.
- Perform troubleshooting and monitoring of Cisco ISE.

3. Target Audience

This course is ideal for:

- Network Security Engineers
- System Engineers
- ISE Administrators
- Network Access Control (NAC) Engineers
- Technical Support Personnel
- Professionals preparing for Cisco certifications

4. Pre-Requisites

Before attending this course, learners should have:

- Knowledge of Cisco networking concepts.
- Familiarity with Cisco IOS command-line interface (CLI).
- Understanding of network security fundamentals.
- Basic knowledge of 802.1X, wireless, and VPN technologies.

5. Course Content

Module 1: Introduction to Cisco ISE Architecture and Deployment

- Overview of Cisco ISE solution
- Deployment options and personas
- Licensing and scalability

Module 2: Cisco ISE Policy Enforcement

- Authentication and authorization policies

- Identity sources and groups
- Policy sets and conditions

Module 3: Profiling, Posture, and BYOD

- Endpoint profiling and classification
- Posture assessments and remediation
- BYOD onboarding and configuration

Module 4: Guest Access Management

- Guest portals and workflows
- Self-registration and sponsor approval
- Hotspot and secure guest access

Module 5: Securing Wired and Wireless Access

- 802.1X authentication
- MAC Authentication Bypass (MAB)
- Integrating ISE with WLAN controllers and switches

Module 6: Cisco ISE Integration and External Services

- Integration with Active Directory and LDAP
- Integration with PKI and certificates
- Logging and monitoring integration

Module 7: Device Administration with TACACS+

- Configuring TACACS+ policies
- Role-based access control
- Auditing administrative activities

Module 8: Operations, Monitoring, and Troubleshooting

- ISE dashboards and reports
- Troubleshooting tools and logs

- Common issues and resolutions

