

---

---

# Implementing and Configuring Cisco Identity Services Engine (SISE)

***WHERE GREAT TRAINING  
HAPPENS EVERYDAY!***



## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Course Duration

5 Days

### Course Price

\$4,395.00

44 CLCs

### Methods of Delivery

In-Person ILT

Virtual ILT

Onsite ILT

### About this Class

In this Implementing and Configuring Cisco Identity Services Engine course provides a comprehensive introduction to Cisco Identity Services Engine, focusing on how identity, context, and policy are used to control network access across wired, wireless, and VPN environments. It is designed for network and security professionals who need to deploy, configure, and troubleshoot Cisco ISE as a centralized policy engine for authentication, authorization, and accounting. The course establishes a strong architectural foundation before progressing into hands-on policy enforcement and operational use cases.

Students begin by exploring Cisco ISE architecture, deployment models, licensing, and new features introduced in Cisco ISE 3.x. Core policy enforcement components are covered in detail, including 802.1X, MAC Authentication Bypass, certificate-based authentication, Active Directory integration, and support for additional identity sources. Policy configuration modules guide students through building authentication and authorization rules that dynamically control user and device access based on identity, posture, and context.

The course expands into advanced access scenarios such as guest services, web authentication, BYOD onboarding, endpoint profiling, and posture compliance. Cisco TrustSec is introduced as a scalable segmentation framework using Security Group Tags, while TACACS+ device administration modules address centralized management of network infrastructure access. Extensive CTCLC-custom labs reinforce each topic through real-world scenarios, including policy creation, profiling, guest access, BYOD compliance, TrustSec configuration, and troubleshooting, preparing students for enterprise deployments and the 300-715 certification exam.

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### How you will benefit

This class will help you:

- Gain hands-on experience configuring, deploying, and operating Cisco ISE for identity-based access control in enterprise environments
- Develop skills to design and implement secure authentication, authorization, guest access, and BYOD onboarding policies for both wired and wireless networks
- Learn to integrate Cisco ISE with Active Directory, LDAP, and network devices, as well as configure endpoint profiling and compliance-based access controls
- Acquire troubleshooting techniques for authentication and policy issues using practical labs and reporting tools, improving real-world problem-solving abilities
- Prepare for the 300-715 SISE v1.1 exam
- Earn 32 CE credits toward recertification

### Why Attend with Current Technologies CLC

- Our Instructors are 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 job roles best suited to the material in this course are:

- Network Security Engineers
- Network Administrators
- Consulting Security Engineers
- Technical Solutions Architects
- Network Managers
- Sales Engineers
- Account Managers

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Objectives

After taking this course, you should be able to:

- Describe how Cisco ISE fits into contemporary network security architectures and the main functions, design motivations, and common use cases
- Examine the functional roles of Cisco ISE node personas, supported deployment models, licensing considerations, and their implications for design planning and scalability decisions
- Implement the installation workflows, platform requirements, and initial setup steps for deploying Cisco ISE on supported virtual and hardware platforms
- Evaluate the principles, message flow, and authorization outcomes of 802.1X-based network access, and Cisco ISE's contribution to the security of wired and wireless connections with identity-based controls
- Describe how MAB works, including its fallback behavior, flow sequence, and policy application within Cisco ISE, and how MAB provides access to non-802.1X-compatible devices
- Establish the role of NADs in Cisco ISE authentication workflows, and provide an outline of the steps required to add, configure, and validate NADs within Cisco ISE to ensure secure policy enforcement
- Discuss the role of internal and external identity sources in Cisco ISE, how user and device identities are managed, and how certificates are used for identity-based authentication
- Evaluate how to configure Cisco ISE to integrate with Active Directory and LDAP, and outline the key settings and connectivity requirements needed to support external user authentication
- Interpret how Cisco ISE selects identity sources during authentication and the logic and conditions that determine identity store sequences, fallback behavior, and identity normalization techniques
- Discuss the structure and purpose of policy sets in Cisco ISE, including how global and local constructs interact, how policy sets are matched and evaluated, and how authentication and authorization logic is organized within each policy set

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Objectives

After taking this course, you should be able to:

- Identify how Cisco ISE evaluates authentication policies using rule conditions, identity store sequences, and dictionaries, as well as how behavior is applied when no rules match
- Interpret how Cisco ISE applies authorization policies following authentication, including how rules are constructed using Conditions Studio and matched against user and device attributes to apply appropriate access profiles
- Analyze Cisco ISE policies based on logs, RADIUS flow data, and session context to resolve authentication and authorization issues across different access scenarios
- Analyze how Cisco ISE provides web-based guest access using CWA, and distinguish between hotspot, self-registration, and sponsored access flows
- Establish global guest settings in Cisco ISE to define account lifecycle behavior, credential policies, communication methods, and access types for guests across supported onboarding processes
- Configure Cisco ISE guest portals to support different access flows, manage account lifecycles, and implement deployment models that are consistent with organizational policies and scalability requirements
- Set up sponsor-drive guest access in Cisco ISE via access roles, linking guest types to sponsor groups, and customizing portal behavior to support account creation and approval
- Establish a clear understanding of Cisco ISE's roles in secure and scalable BYOD access: its enterprise use cases, deployment models, policy-based control strategies, key components, Cisco ISE-specific capabilities, and onboarding designs such as single and dual SSIDs for seamless personal device integration into the network
- Configure Cisco ISE to deliver supplicants, issue certificates, and enforce policies as part of a complete BYOD onboarding pipeline

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Objectives

After taking this course, you should be able to:

- Identify how Cisco ISE evaluates authentication policies using rule conditions, identity store sequences, and dictionaries, as well as how behavior is applied when no rules match
- Interpret how Cisco ISE applies authorization policies following authentication, including how rules are constructed using Conditions Studio and matched against user and device attributes to apply appropriate access profiles
- Analyze Cisco ISE policies based on logs, RADIUS flow data, and session context to resolve authentication and authorization issues across different access scenarios
- Analyze how Cisco ISE provides web-based guest access using CWA, and distinguish between hotspot, self-registration, and sponsored access flows
- Establish global guest settings in Cisco ISE to define account lifecycle behavior, credential policies, communication methods, and access types for guests across supported onboarding processes
- Configure Cisco ISE guest portals to support different access flows, manage account lifecycles, and implement deployment models that are consistent with organizational policies and scalability requirements
- Set up sponsor-drive guest access in Cisco ISE via access roles, linking guest types to sponsor groups, and customizing portal behavior to support account creation and approval
- Establish a clear understanding of Cisco ISE's roles in secure and scalable BYOD access: its enterprise use cases, deployment models, policy-based control strategies, key components, Cisco ISE-specific capabilities, and onboarding designs such as single and dual SSIDs for seamless personal device integration into the network
- Configure Cisco ISE to deliver supplicants, issue certificates, and enforce policies as part of a complete BYOD onboarding pipeline

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Objectives

After taking this course, you should be able to:

- Operate post-onboarding workflows using the My Device Portal, including revocation of certificates and device de-registration for lost or stolen endpoints
- Explain how Cisco ISE uses profiling to identify endpoints by taking advantage of classification logic, profiler components, data flows, and feed services to provide the foundation for advanced profiling and policy enforcement
- Analyze how Cisco ISE collects endpoint data using built-in probes, device sensors, and pxGrid enrichment, and how each method contributes to the accuracy and coverage of profiling
- Analyze how the profiling policies in Cisco ISE classify endpoints based on collection attributes, and how logical profiles are created and applied to support the decision-making process for determining access based on identity
- Design scalable profiling solutions by aligning design principles, probe selection, and NAD integration with diverse network environments
- Maintain visibility of profiling through dashboards and reporting tools, and improve deployment efficiency through optimization techniques
- Apply foundational understanding of Cisco ISE posture services, including agent types, flow logic, operational modes, and use cases
- Implement Cisco ISE to deliver posture agents and related resources to endpoints by configuring update services, portals, and delivery policies
- Administer Cisco ISE policies to ensure secure and compliant network access
- Test compliance-based access enforcement by simulating a variety of endpoint scenarios using Cisco AnyConnect
- Assess session behavior, interpret posture outcomes, and analyze reporting tools to confirm the effectiveness of posture policy application and remediation

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Objectives

After taking this course, you should be able to:

- Examine Cisco ISE's use of TACACS+ for securing administrative access, including key AAA concepts and a comparison with RADIUS to illustrate centralized authentication and authorization
- Set up Cisco ISE for TACACS+ based device administration by configuring policy elements such as command sets, profiles, and policy sets
- Onboard network devices, define access permissions, and set up authentication and authorization rules to control administrator access
- Implement advanced TACACS+ authorization logic, implement administrator command access, and implement scalable deployments using proven design guidelines
- Compare Cisco's TrustSec core architecture, operation, and design considerations, including its enhancements and planning prerequisites for enterprise deployment
- Configure Cisco TrustSec segmentation in Cisco ISE, including SGT classification, SXP propagation, and tag-based policy enforcement
- Interpret how to operationalize Cisco ISE through system maintenance, backup/restore procedures, certificate management, and structured upgrades in production environments

### Prerequisites

The knowledge and skills you are recommended to have before attending this training are:

- 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

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Course 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

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Course Outline

#### 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

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### Course Outline

#### 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

## Implementing and Configuring Cisco Identity Services Engine (SISE)

### 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