# Implementing and Configuring Cisco Identity Services Engine

**Duration: 5 Days** **Course Code: SISE** **Version: 4.0**

## Overview:

In the Implementing and Configuring Cisco Identity Services Engine (SISE) course you will learn 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 VPN connections.

This hands-on course 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, BYOD, endpoint compliance services, and TACACS+ device administration.Implementing and Configuring Cisco Identity Services Engine (SISE) course 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 VPN connections.

**You will learn how to use Cisco ISE to:**
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 authorisation services in a single web-based GUI console
Gain eading-edge career skills for high-demand job roles and responsibilities focused on enterprise security

**This course also earns you 40 Continuing Education (CE) credits toward recertification**

## Target Audience:

Individuals involved in the deployment and maintenance of a Cisco Identity Services Engine solution.

## Objectives:

- **After completing this course you should be able to:**
- Explain Cisco ISE deployment
- Describe Cisco ISE policy enforcement components
- Describe Cisco ISE policy configuration
- Troubleshoot Cisco ISE policy and third-party Network Access Device (NAD) support
- Configure guest access
- Configure hotspots and guest portals
- Describe the Cisco ISE profiler services
- Describe profiling best practices and reporting
- Configure a Cisco ISE BYOD solution
- Configure endpoint compliance
- Configure client posture services
- Configure Cisco ISE device administration
- Describe Cisco ISE TrustSec configurations

## Prerequisites:

**Attendees should meet the following prerequisites:**

- Familiarity with the Cisco IOS® Software Command-Line Interface (CLI) for wired and wireless devices
- Familiarity with Cisco AnyConnect® Secure Mobility Client
- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1x
- 8021X-CPLL - Introduction to 802.1X Operations for Cisco Security Professionals - CPLL

## Testing and Certification

**Recommended as preparation for the following exam:**

- **300-715 SISE -** Implementing and Configuring Cisco Identity Services Engine Exam

Students looking to obtain their CCNP Security Accreditation will need to have passed the SCOR - 350-701 Exam as well.

- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core Technologies

## Content:

Introducing Cisco ISE Architecture

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

Introducing Cisco ISE Deployment

- Introduction
- Cisco ISE Deployment Models
- Cisco ISE Licensing and Network Requirements
- Cisco ISE Context Visibility Features
- New Features in Cisco ISE 3.X
- Configure Initial Cisco ISE Setup and System Certificate Usage
- Summary
- Summary Challenge

Introducing Cisco ISE Policy Enforcement Components

- Introduction
- 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
- Integrate Cisco ISE with Active Directory
- Summary
- Summary Challenge

Introducing Cisco ISE Policy Configuration

- Introduction
- Cisco ISE Policy
- Cisco ISE Authentication Rules
- Cisco ISE Authorization Rules
- Configure Cisco ISE Policy for MAB
- Configure Cisco ISE Policy for 802.1X
- Summary
- Summary Challenge

Troubleshooting Cisco ISE Policy and Third-Party NAD Support

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

Introducing Web Authentication and Guest Services

- Introduction
- Web Access with Cisco ISE
- Guest Access Components
- Guest Access Settings
- Configure Guest Access
- Summary
- Summary Challenge

Configuring Hotspots and Guest Portals

- Introduction
- Sponsor and Guest Portals Configuration
- Configure Hotspot and Self-Registered Guest Access
- Configure Sponsor-Approved and Fully Sponsored Guest Access
- Create Guest Reports
- Summary
- Summary Challenge

Introducing the Cisco ISE Profiler

- Introduction
- ISE Profiler Overview
- Cisco ISE Probes
- Profiling Policy
- Configure Profiling
- Customize the Cisco ISE Profiling Configuration
- Summary
- Summary Challenge

Introducing Profiling Best Practices and Reporting

- Introduction
- Profiling Best Practices
- Create Cisco ISE Profiling Reports
- Summary
- Summary Challenge

Configuring Cisco ISE BYOD

- Introduction
- Cisco ISE BYOD Solution Overview
- Cisco ISE BYOD Flow
- My Devices Portal Configuration
- Certificate Configuration in BYOD Scenarios
- Configure BYOD
- Manage a Lost or Stolen BYOD Device
- Summary
- Summary Challenge

Introducing Cisco ISE Endpoint Compliance Services

- Introduction
- Endpoint Compliance Services Overview
- Configure Cisco ISE Compliance Services
- Summary
- Summary Challenge

Configuring Client Posture Services and Compliance

- Introduction
- Client Posture Services and Provisioning Configuration
- Configure Client Provisioning
- Configure Posture Policies
- Test and Monitor Compliance-Based Access
- Summary
- Summary Challenge

Working With Network Access Devices

- Introduction
- 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
- Configure Cisco ISE for Basic Device Administration
- Configure Cisco ISE Command Authorization
- Summary
- Summary Challenge

Exploring Cisco TrustSec

- Introduction
- Cisco TrustSec Overview
- Cisco TrustSec Enhancements
- Cisco TrustSec Configuration
- Configure Cisco TrustSec
- Summary
- Summary Challenge

Labs:

- Lab 1A: Installation and Basic Setup of Cisco ISE
- Lab 1B: Verify Initial Cisco ISE Setup and System Certificate Usage
- Lab 2: Integrate Cisco ISE with Active Directory
- Lab 3: Configure Cisco ISE Policy for MAB
- Lab 4: Configure Cisco ISE Policy for 802.1X
- Lab 5: Configure Guest Access
- Lab 6: Configure Hotspot and

Self-Registered Guest Access
- Lab 7: Configure Sponsor-Approved and Fully Sponsored Guest Access
- Lab 8: Create Guest Reports
- Lab 9: Configure Profiling
- Lab 10: Customize the Cisco ISE Profiling Configuration
- Lab 11: Create Cisco ISE Profiling Reports
- Lab 12: Configure BYOD
- Lab 13: Manage a Lost or Stolen BYOD Device
- Lab 14: Configure Cisco ISE Compliance Services
- Lab 15: Configure Client Provisioning
- Lab 16: Configure Posture Policies
- Lab 17: Test and Monitor Compliance-Based Access
- Lab 18: Configure Cisco ISE for Basic Device Administration
- Lab 19: Configure Cisco ISE Command Authorization
- Lab 20: Configure Cisco TrustSec

## Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge,  16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo