

## Implementing and Configuring Cisco Identity Services Engine v3.0

**Course#: SISE**  
**Duration: 5 Days**  
**Price: 0.00**

### Course Description

In this course, you will learn about the Cisco Identity Services Engine (ISE) a next-generation 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) using 802.1x, MAB, web authentication, posture, profiling, BYOD device on-boarding, guest services, MDM, and VPN access into a single context-aware identity-based platform. The training provides learners with the knowledge and skills to enforce security compliance for wired, wireless and VPN endpoints and enhance infrastructure security using the Cisco ISE.

This course is an intensive hands-on experience. With enhanced hands-on labs, you will cover all facets of Cisco ISE version 2.7. You will learn how to configure fundamental elements of ISE and how to secure identity-based networks using 802.1X for both wired and wireless clients, using Windows 10 and Cisco IP-Phone endpoints. You will integrate the Cisco Virtual Wireless LAN Controller (vWLC) with advanced ISE features. You will also learn to use the following advanced features of Cisco ISE: Active Directory Integration, Policy Sets, EasyConnect, EAP-FAST with EAP Chaining, Guest Access, Profiler, BYOD, AnyConnect 4.x Posture Module for LAN and VPN compliance, TACACS+ Device Management, pxGrid and TrustSec Security Group Access.

### Objectives

- ISE deployment options including node types, personas, and licensing
- Install certificates into ISE using a Windows 2012 Certificate Authority (CA)
- Configure the Local and Active Directory Based Identity Store and use of Identity Source Sequences
- Configure AAA clients and network device groups
- Implement Policy Sets to streamline Authentication and Authorization in the organization
- Deploy EasyConnect as an alternative to 802.1X port-based authentication
- Implement 802.1X for wired and wireless networks using the AnyConnect 4.x NAM module, the

latest dot1x commands on a catalyst switch, and version 8.4 of the vWLC

- Configure policies to allow MAC Authentication Bypass (MAB) of endpoints
- Use central web authentication (CWA) for redirection of legitimate domain users who need to register devices on the network using MAC addresses (BYOD device registration)
- Configure hotspot guest access, self-registration guest access, and sponsored guest access
- Configure profiler services in ISE and use newer probes available in IOS switch code 15.x as well as vWLC 8.4 code.
- Work with Profiling feeds, logical profiles, and building profiling conditions to match network endpoints
- Configure posture assessments using the new Cisco AnyConnect Secure Mobility 4.x posture module
- Configure Cisco ISE as a TACACS+ Server for Device Administration with Command Authorization
- Configure Cisco ISE to integrate with a 5500-X ASA and a Catalyst Switch for TrustSec and implement end-to-end Security Group Tagging (SGT) and Security Group Access Control (SGACL)
- Maintenance, best practices, and logging

## **Audience**

- Network security engineers
- ISE administrators
- Wireless network security engineers
- Cisco integrators and partners
- Consulting systems engineers
- Technical solutions architects
- Integrators who install and implement the Cisco ISE version 2.7
- End users (Cisco customers) desiring the knowledge to install, configure, and deploy Cisco ISE 2.7
- Cisco channel partners and field engineers who need to meet the educational requirements to attain Authorized Technology Partner (ATP) authorization to sell and support the ISE product

## **Prerequisites**

The learner is expected to have the following skills and knowledge before attending this course:

- 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

## **Content**

Classroom Live Outline

Module 1: Introducing Cisco ISE Architecture and Deployment

Cisco ISE Features and Services

Cisco ISE Deployment Models

Module 2: Cisco ISE Policy Enforcement

Introducing 802.1X and MAB Access: Wired and Wireless

Introducing Cisco ISE Identity Management

Configuring Cisco ISE Certificate Services

Introducing Cisco ISE Policy Sets

Configuring Cisco ISE Authentication and Authorization Policy

Implementing Third-Party Network Access Device Support

Overview of Cisco TrustSec using Cisco ISE

Introducing Cisco ISE EasyConnect

Module 3: Web Auth and Guest Services

Introducing Web Access with Cisco ISE

Introducing Cisco ISE Guest Access Components

Configuring Guest Access Settings

Configuring Portals: Sponsors and Guests

Module 4: Cisco ISE Profiler

Introducing Cisco ISE Profiler  
Configuring Cisco ISE Profiling

## Module 5: Cisco ISE BYOD

Introducing the Cisco ISE BYOD Process  
Describing BYOD Flow  
Configuring My Devices Portal Settings  
Configuring Certificates in BYOD Scenarios

## Module 6: Cisco ISE Endpoint Compliance

Introducing Cisco ISE Endpoint Compliance  
Configuring Client Posture Services and Provisioning in Cisco ISE

## Module 7: Working with Network Access Devices

Configuring TACACS+ for Cisco ISE Device Administration

## Classroom Live Labs

ISE Familiarization and Certificate Usage  
Active Directory and Identity Source Sequences  
Policy Sets, Conditions Studio, and Network Devices  
Passive Identity (Easy Connect)  
802.1X-Wired Networks PEAP  
802.1X-Wired Networks - EAP-FAST  
802.1X-Wireless Networks  
802.1X-MAC Authentication Bypass (MAB)  
Centralized Web Authentication (CWA)

Guest Access and Reports

Endpoint Profiling and Reports

BYOD and My Devices Portal

Posture Compliance and Reports

Compliance Based VPN Access (Optional, Exclusive)

TACACS+ Device Administration

Additional Guest Scenarios (Optional)

Posture Compliance Using the Temporal Agent (Optional, Exclusive)

pxGrid Integration with Firepower (Optional, Exclusive)

TrustSec Security Group Access (Optional, Exclusive)

ISE Distributed Deployment (Optional, Exclusive)

pxGrid Integration with Stealthwatch (Optional, Exclusive)