FIREFLY

CONTACT US

Implementing and Configuring Cisco Identity Services Engine Bootcamp

DURATION: 5 DAYS COURSE CODE: SISE FORMAT: LECTURE/LAB

COURSE DESCRIPTION

The Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0 course is an intensive experience with enhanced hands-on labs that cover all facets of Cisco Identity Services Engine (ISE) version 2.4. The training provides learners with the knowledge and skills to enforce security compliance for wired and wireless endpoints and enhance infrastructure security using the Cisco ISE.

In this course, you will learn about the Cisco ISE, a next-generation identity and access control policy platform that provides a single policy plane across the entire organization. The ISE combines multiple services including authentication, authorization, and accounting (AAA) using 802.1x, MAB, web authentication, posture, profiling, device on-boarding, guest services, and VPN access into a single context-aware identity-based platform..

This course helps you prepare to take the exam, Implementing and Configuring Cisco Identity Services Engine (300-715 SISE), which leads to CCNP® Security and the Cisco Certified Specialist - Security Identity Management Implementation certifications.

This class will help you use SISE to

- Provide secure business and context-based access based on policies
- Centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console
- Provide a streamlined experience for implementing and customizing guest network access
- Gain leading-edge career skills for high-demand job roles and responsibilities focused on enterprise security

This exam certifies your knowledge of Cisco Identify Services Engine, including architecture and deployment, policy enforcement, Web Auth and guest services, profiler, BYOD, endpoint compliance, and network access device administration.

After you pass 300-715 SISE:

- You earn the Cisco Certified Specialist - Security Identity Management Implementation certification.
- You will have satisfied the concentration exam requirement for the new CCNP Security certification. To complete CCNP Security, you also need to pass the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam or its equivalent.

PREREQUISITES

Attendees should meet the following prerequisites:

- 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

Recommended Cisco learning offerings that may help you meet these prerequisites:

- Cisco CCNP® Security Certification training
- Introduction to 802.1X Operations for Cisco Security Professionals (802.1X)

WHO SHOULD ATTEND

Network security engineers

ISE administrators

Wireless network security engineers

Cisco integrators and partners

LEARNING 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 (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

COURSE OUTLINE

1: Introducing Cisco ISE Architecture and Deployment
- Cisco ISE Features and Services
- Cisco ISE Deployment Models

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

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

4: Cisco ISE Profiler
- Introducing Cisco ISE Profiler
- Configuring Cisco ISE Profiling

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

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

7: Working with Network Access Devices
- Configuring TACACS+ for Cisco ISE Device Administration

DISCOVERY LABS

1: ISE Familiarization and Certificate Usage
2: Active Directory and Identity Source Sequences
3: Policy Sets, Conditions Studio, and Network Devices
4: Passive Identity
5: 802.1X-Wired Networks – PEAP
6: 802.1X-Wired Networks - EAP-FAST
7: 802.1X-Wireless Networks
8: 802.1X-MAC Authentication Bypass (MAB)
9: Centralized Web Authentication (CWA)
10: Guest Access and Reports
11: Endpoint Profiling and Reports
12: BYOD and My Devices Portal
13: Posture Compliance and Reports
14: Compliance Based VPN Access
15: TACACS+ Device Administration
16: Additional Guest Scenarios
17: Posture Compliance Using the Temporal Agent
18: pxGrid Integration with Firepower
19: TrustSec Security Group Access
20: ISE Distributed Deployment
21: pxGrid Integration with Stealthwatch