FIREFLY

CONTACT US

IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICES ENGINE BOOTCAMP

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

COURSE DESCRIPTION

This course is an intensive hands-on experience. With enhanced hands-on labs, you will cover the Cisco ISE version 2.4 (labs). You will learn how to perform a fundamental installation of ISE and how to configure identity-based networks using 802.1X for both wired and wireless clients, using Windows 8 and Apple iPad endpoints. You will also learn to use many of the new features, including AnyConnect 4.1 Posture Module for LAN and VPN posture compliance, EAP-FAST, PEAP, BYOD, and EAP Chaining. You'll also see how the new Virtual Wireless Controller (vWLC) works to integrate with ISE along with advanced features within ISE.

This course is focused specifically on the Cisco Identity Services Engine (ISE), an 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), posture, profiling, device on-boarding, and guest management, into a single context-aware identity-based platform.

The training provides learners with the knowledge and skills to enforce security posture compliance for wired and wireless endpoints and enhance infrastructure security using the Cisco ISE.

WHO SHOULD ATTEND

Individuals involved in the deployment and maintenance of the Cisco ISE platform

PREREQUISITES

Attendees should meet the following prerequisites:

- CCNA Security certification ICND1 or CCNA and IINS.
- Understand the concepts of 802.1X - recommended.
- Familiarity with Microsoft Windows and Active Directory.

LEARNING OBJECTIVES

Describe Cisco ISE architecture, installation, and distributed deployment options

Configure Network Access Devices (NADs), policy components and basic authentication and authorization policies in Cisco ISE

Implement Cisco ISE web authentication and guest services
Deploy Cisco ISE profiling, posture and client provisioning services
Describe administration, monitoring, troubleshooting, and TrustSec SGA security
Configure device administration using TACACS+ in Cisco ISE

COURSE OUTLINE

Lesson 1: Introducing Cisco ISE Architecture and Deployment
- Using Cisco ISE as a Network Access Policy Engine
- Introducing Cisco ISE Deployment Models

Lesson 2: Cisco ISE Policy Enforcement
- Introducing 802.1X and MAB Access: Wired and Wireless
- Introducing Identity Management
- Configuring Certificate Services
- Introducing Cisco ISE Policy
- Configuring Cisco ISE Policy Sets
- Implementing Third-Party Network Access Device Support
- Introducing Cisco TrustSec
- Introducing EasyConnect

Lesson 3: Web Authentication and Guest Services
- Introducing Web Access with Cisco ISE
- Introducing ISE Guest Access Components
- Configuring Guest Access Services
- Configuring Portals: Sponsors and Guests

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

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

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

Lesson 7: Cisco ISE with AMP and VPN-Based Services
- Introducing VPN Access Using Cisco ISE
- Configuring Cisco AMP for ISE

Lesson 8: Cisco ISE Integrated Solutions with API's
- Introducing Location-Based Authorization
- Introducing Cisco ISE2.x pxgrid

Lesson 9: Working with Network Access Devices
- Configuring TACACS+ for Cisco ISE Device Administration

Lesson 10: Cisco ISE Design (Self-Study)
- Designing and Deployment Best Practices
- Performing Cisco ISE Installation and Configuration Best Practices
- Deploying Failover and High Availability

Lesson 11: Configuring Third Party NAD Support
(Optional/Self-Study/Reference)
- Configuring Third-Party NAD Support

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 (Easy Connect)
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 Device Portal
13: Posture Compliance and Reports
14: Compliance Based VPN Access
15: Threat Centric NAC with AMP for Endpoint
16: Firepower pxGrid Remediation
17: TACACS+ Device Administration
18: TrustSec Security Group Access
19: Additional Guest Scenarios
20: ISE Distributed Deployment