Cisco Security

SISE3: Implementing and Configuring Cisco Identity Services Engine
$4,295.00

- 5 Days

Upcoming Dates

Course Description

The Implementing and Configuring Cisco Identity Services Engine (SISE) v3.0 course shows you how to deploy and use Cisco® Identity Services Engine (ISE) v2.4, 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 use Cisco ISE, including policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration. Through expert instruction and hands-on practice, you will learn how to use Cisco ISE to gain visibility into what is happening in your network, streamline security policy management, and contribute to operational efficiency.

Course Outline

The course contains these components:

- Section 1: Introducing Cisco ISE Architecture and Deployment
- Section 2: Cisco ISE Policy Enforcement
- Section 3: Web Auth and Guest Services
- Section 4: Cisco ISE Profiler
- Section 5: Cisco ISE BYOD
- Section 6: Cisco ISE Endpoint Compliance Services
- Section 7: Working with Network Access Devices

LAB OUTLINE:

- Discovery 1: Access the SISE Lab and Install ISE 2.4
- Discovery 2: Configure Initial Cisco ISE Setup, GUI Familiarization, and System Certificate Usage
- Discovery 3: Integrate Cisco ISE with Active Directory
- Discovery 4: Configure Cisco ISE Policy
- Discovery 5: Configure Access Policy for Easy Connect
- Discovery 6: Configure Guest Access
- Discovery 7: Configure Guest Access Operations
- Discovery 8: Create Guest Reports
- Discovery 9: Configure Profiling
- Discovery 10: Customize the Cisco ISE Profiling Configuration
- Discovery 11: Create Cisco ISE Profiling Reports
- Discovery 12: Configure BYOD
- Discovery 13: Blacklisting a Device
- Discovery 14: Configure Cisco ISE Compliance Services
- Discovery 15: Configure Client Provisioning
- Discovery 16: Configure Posture Policies

- Discovery 17: Test and Monitor Compliance Based Access
- Discovery 18: Test Compliance Policy
- Discovery 19: Configure Cisco ISE for Basic Device Administration
- Discovery 20: Configure TACACS+ Command Authorization

Audience

- Network Security Engineers
- ISE Administrators
- Wireless Network Security Engineers
- Cisco Integrators and Partners

Prerequisites

It is recommended, but not required, 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

What You Will Learn

Upon completion of this course, you will be able to:

- Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture. Describe the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages.
- Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services.
- Describe how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization.
- Describe third-party network access devices (NADs), Cisco TrustSec®, and Easy Connect.
- Describe and configure web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios.
- Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints. Describe best practices for deploying this profiler service in your specific environment.
- Describe BYOD challenges, solutions, processes, and portals. Configure a BYOD solution, and describe the relationship between BYOD processes and their related configuration components. Describe and configure various certificates related to a BYOD solution.
- Describe the value of the My Devices portal and how to configure this portal.
- Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE.
- Describe and configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understand the role of TACACS+ within the authentication, authentication, and accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols.
- Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool.