Cisco® SISE Implementing and Configuring Cisco® Identity Services Engine v3.0

Overview

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. 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.

Prerequisite Comments

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

Target Audience

Network security engineers
ISE administrators
Wireless network security engineers
Cisco integrators and partners

Course Objectives

After taking this course, you should 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.

Course Outline

1 - Introducing Cisco ISE Architecture and Deployment

Using Cisco ISE as a Network Access Policy Engine
Cisco ISE Use Cases
Describing Cisco ISE Functions
Cisco ISE Deployment Models
Context Visibility

2 - Cisco ISE Policy Enforcement

Using 802.1X for Wired and Wireless Access
Using MAC Authentication Bypass for Wired and Wireless Access
Introducing Identity Management
Configuring Certificate Services
Introducing Cisco ISE Policy
Implementing Third-Party Network Access Device Support
Introducing Cisco TrustSec
Cisco TrustSec Configuration
Easy Connect

3 - Web Authentication and Guest Services

Introducing Web Access with Cisco ISE
Introducing Guest Access Components
Configuring Guest Access Settings
Configuring Sponsor and Guest Portals

4 - Cisco ISE Profiler

Introducing Cisco ISE Profiler
Profiling Deployment and Best Practices

5 - Cisco ISE BYOD

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

6 - Cisco ISE Endpoint Compliance Services

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

7 - Working with Network Access Devices

Review TACACS+
Cisco ISE TACACS+ Device Administration
Configure TACACS+ Device Administration
TACACS+ Device Administration Guidelines and Best Practices
Migrating from Cisco ACS to Cisco ISE

8 - Lab outline

Access the SISE Lab and Install ISE 2.4
Configure Initial Cisco ISE Setup, GUI Familiarization, and System Certificate Usage
Integrate Cisco ISE with Active Directory
Configure Basic Policy on Cisco ISE
Configure Policy Sets
Configure Access Policy for Easy Connect
Configure Guest Access
Configure Guest Access Operations
Create Guest Reports
Configure Profiling
Customize the Cisco ISE Profiling Configuration
Create Cisco ISE Profiling Reports
Configure BYOD
Blacklisting a Device
Configure Cisco ISE Compliance Services
Configure Client Provisioning
Configure Posture Policies
Test and Monitor Compliance-Based Access
Test Compliance Policy
Configure Cisco ISE for Basic Device Administration
Configure TACACS+ Command Authorization