Implementing and Configuring Cisco Identity Services Engine (SISE) v3.0 - On Demand

Modality: Self-Paced Learning

Duration: 40 Hours

SATV Value:

CLC: 5 Units

NATU:

SUBSCRIPTION: No

Course Information

About this course:

This course teaches you skills to deploy and use an identity and access control policy platform, Cisco Identity Services Engine (Cisco ISE) v2.4. With this platform you will be able to simplify the delivery of consistent, highly secure access control across wired, wireless, and VPN connections.

This course will also enable you to perform policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration.

With the ability to use Cisco ISE, you can streamline security policy management, gain visibility into your network, and contribute to operational efficiency.

Upon completing this course you will be fully prepared to take the Implementing and Configuring Cisco Identity Services Engine (300-715 SISE) exam, passing which will lead to CCNP Security and Cisco Certified Specialist - Security Identity Management Implementation certifications.

Course Objective:

You should be able to do the following after successfully completing the course:

- Describe third-party Network Access Devices (NADs), Cisco TrustSec®, and Easy Connect
- 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, authorization, and accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols
- 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
- Migrate TACACS+ functionality from Cisco Secure Access Control Server (Cisco Secure ACS) to Cisco ISE, using a migration tool
-
- 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

Audience:

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

Prerequisite:

To fully benefit from this course, you should have the following knowledge:

- Familiarity with Microsoft Windows operating systems
- Familiarity with 802.1X
- Familiarity with the Cisco IOS Software CLI
- Familiarity with Cisco AnyConnect® Secure Mobility Client

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

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

Course 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