Implementing and Configuring Cisco Identity Services Engine Bootcamp

Course Code	SISE
Duration	5 days

Overview

The Implementing and Configuring Cisco Identity Services Engine 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 required 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.

Delegates will be expected to work in groups and share lab equipment; if you are attending virtually you may also be required to work in virtual breakout rooms. Extended hours may also be required to cover all of the content included in this class.

Audience

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

Learning Objectives

By actively participating in this course, you will learn about the following:

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

Pre-Requisites

- Foundational level understanding of Security Concepts
- Understand the concepts of 802.1X.
- Familiarity with Cisco AnyConnect Secure Mobility Client.
- Familiarity with Microsoft Windows and Active Directory.

Recommended courses:

- 8021X-CPLL - Introduction to 802.1X Operations for Cisco Security Professionals - CPLL
- CCNA - Implementing and Administering Cisco Solutions
- SCOR - Implementing and Operating Cisco Security Core Technologies

Course Contents

Introducing Cisco ISE Architecture and Deployment

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

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
- TrustSec Configuration
- Easy Connect

Web Authentication and Guest Services

- Introducing Web Access with Cisco ISE
- Introducing Guest Access Components
- Configuring Guest Access Services
- Configure Sponsor and Guest Portals

Cisco ISE Profiler

- Introducing Cisco ISE Profiler
- Profiling Deployment and Best Practices

Cisco ISE BYOD

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

Cisco ISE Endpoint Compliance Services

- Introducing Endpoint Compliance Services
- Configuring Client Posture Services and Provisioning

Working with Network Access Devices

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

Labs

- 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 Cisco ISE Policy
- 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

Exam Details

This course leads to the 300-715 - Implementing and Configuring Cisco Identity Services Engine (SISA) exam.

Successful completion will earn you the CIsco Certified Specialist - Security Identity Management certification and satisfy the concentration requirement for the CCNP Security certification.

Further Information

For more information or to book this course, please contact our Course Enquiries Team on **01752 227330** (Option 2) or email us at **enquiries@skilltec.co.uk**.