TECHLAN

IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICE ENGINES (SISE)

ACADEMY

COURSE OBJECTIVE:

In this course, you will learn about the Cisco Identity Services Engine (ISE)—a next-generation 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) using 802.1x, MAB, web authentication, posture, profiling, device on-boarding, guest services, and VPN access into a single context-aware identity-based platform. The training provides learners with the knowledge and skills to enforce security compliance for wired and wireless endpoints and enhance infrastructure security using the Cisco ISE.

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

- Configure fundamental elements of ISE
- How to secure identity-based networks using 802.1X for both wired and wireless clients
- You will integrate the Cisco Virtual Wireless LAN Controller (vWLC) with advanced ISE features.
- You will also learn to use the following advanced features of Cisco ISE: Active Directory Integration, Policy Sets, EasyConnect, EAP-FAST with EAP Chaining, BYOD, AnyConnect 4.x Posture Module for LAN and VPN compliance, and TrustSec Security Group Access.

PREREQUISIT:

It is recommended, but not required, that students have the following knowledge and skills:

CCNA Security or equivalent level of experience with Cisco devices
Foundation-level wireless knowledge and skills
Familiarity with Microsoft Windows and Microsoft Active Directory
Familiarity with 802.1X
Familiarity with Cisco ASA
Familiarity with Cisco AnyConnect Secure Mobility Client

In relation to EXAM:

210-260 IINS

WHO SHOULD ATTEND

Consulting systems engineers

Technical solutions architects

Integrators who install and implement the Cisco ISE version 2.1

End users (Cisco customers) desiring the knowledge to install, configure, and deploy Cisco ISE 2.1

Field engineers who need to meet the educational

TECHLAN

ACADEMY

COURSE CONTENT:

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

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

MODULE 3: Web Authority and Guest Services
Web Access with Cisco ISE
ISE Guest Access Components
Configuring Guest Access Settings
Configuring Portals: Sponsors and Guests

MODULE 4: Cisco ISE Profiler
Cisco ISE Profiler
Configuring Cisco ISE Profiling

MODULE 5: Cisco ISE BYOD
Cisco ISE BYOD Process
BYOD Flow
Configuring My Devices Portal Settings
Configuring Certificates in BYOD Scenarios

MODULE 6: Cisco ISE Endpoint Compliance Services
Endpoint Compliance
Configuring Client Posture Services and Provisioning in Cisco ISE

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

MODULE 8: Cisco ISE Design
Designing and Deployment Best Practices
Performing Cisco ISE Installation and Configuration Best Practices
Deploying Failover and High-Availability

LABS:

Lab 1: ISE Familiarization and Certificate Usage
Lab 2: Active Directory and Identity Source Sequences
Lab 3: Conversion to Policy Sets
Lab 4: Access Policy for EasyConnect
Lab 5: 802.1X-Wired Networks – PEAP
Lab 6: 802.1X-Wired Networks - EAP-FAST
Lab 7: 802.1X-Wireless Networks
Lab 8: 802.1X-MAC Authentication Bypass (MAB)
Lab 9: Centralized Web Authentication (CWA)
Lab 10: Guest Access and Reports
Lab 11: Endpoint Profiling and Reports
Lab 12: BYOD and My Device Portal
Lab 13: Posture Compliance and Reports
Lab 14: Compliance Based VPN Access