Implementing and Configuring Cisco Identity Services Engine (CPLL-SISE)

Duration: 180 Days

The Implementing and Configuring Cisco Identity Services Engine (SISE) Learning Path teaches you to deploy, configure, and operate Cisco® Identity Services Engine (ISE) as the central platform for identity-based access control. Learning begins with the core architecture and installation and progresses through network access control, identity stores, policy design, and day-to-day operations. You will learn how to configure authentication and authorization policies, create scalable guest onboarding workflows, integrate network devices, and apply identity-based access decisions across wired and wireless environments. It also covers endpoint profiling, posture assessment, Terminal Access Controller Access Control Server (TACACS+) device administration, TrustSec concepts, certificate management, lifecycle operations, and advanced administration practices. The labs provide you with practical experience in Cisco ISE personas, certificate-based authentication, TEAP (EAP Chaining), Bring Your Own Device (BYOD) onboarding, device profiling, guest services, and policy enforcement in real-world environments. A wide range of use cases are covered, including 802.1X, MAB, and certificate provisioning. As a result of this Learning Path, you will be able to design, implement, and operate a Cisco ISE deployment that meets modern enterprise requirements for identity, security, visibility, and access control.

This Learning Path prepares you for 300-715 SISE v1.1 exam. If passed, you earn the Cisco Certified Specialist – Security Identity Management Implementation certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

Skills You'll Learn:

- Deploy, configure, and operate Cisco ISE as the central platform for identity-based access control
- Design and implement authentication and authorization policies for wired and wireless networks
- Integrate Cisco ISE with Active Directory, LDAP, and network devices
- Implement BYOD onboarding and lifecycle operations
- Use endpoint profiling and posture assessment to enforce compliance-based access controls

Learning Path Objectives:

1. Cisco ISE Architecture and Installation: Explore the foundational concepts of Cisco ISE, including its role in network security, deployment models, supported platforms, initial setup, licensing, and system certificates, to build a solid understanding for future learning.
2. Network Access Control: Examine how Cisco ISE enables secure network access through methods like 802.1X and MAB, detailing access flows, fallback mechanisms, NAD configuration, and identity-based policy enforcement during authentication.
3. Identity and Authentication: Investigate how Cisco ISE leverages identity sources, certificate management, and identity policies to identify and group users and devices, forming the basis for reliable, context-aware access control across the network.
4. Policy Configuration and Troubleshooting: Understand Cisco ISE's access control mechanisms by exploring structured policy sets, authentication and authorization decisions, conditions, rule logic, and policy evaluation, offering a scalable framework for modern enterprise requirements.
5. Guest Access: Learn how Cisco ISE enables secure and flexible guest access through web-based authentication, covering various guest models, portal components, and configurations to design enterprise-aligned access experiences.
6. BYOD: Discover how Cisco ISE manages secure enterprise access for personally owned devices by guiding you through the BYOD lifecycle, including onboarding, certificate provisioning, access configuration, and key features like the My Devices portal and client provisioning workflows.
7. Profiling: Explore how Cisco ISE collects and analyzes network intelligence using probes, sensors, and feed services to profile devices and refine profiling policies, enabling adaptive and automated access decisions across diverse environments.
8. TACACS+: Control administrative access to network devices with Cisco ISE and TACACS+ by understanding AAA fundamentals, configuring device administration, and implementing user roles and authorization policies for precise permissions.
9. Posturing: Assess endpoint health and enforce secure, policy-driven access with Cisco ISE by leveraging posture assessment, compliance modules, remediation workflows, and real-time device status to maintain network security.
10. TrustSec and Administration: Expand Cisco ISE with TrustSec for scalable network segmentation, integrate segmentation policies, and apply operational practices to ensure system resilience and adaptability.