



300-715 SISE Overview

The SISE v3.0 course will enable you to deploy and use Cisco® Identity Services Engine (ISE) v2.4. Cisco SISE is an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across VPN connections, wired and wireless. You will also learn how to use Cisco ISE to gain visibility into what is happening in streamline security policy management, network, and contribute to operational efficiency.

About the training

- **Study Material:-** Virtual-led Training, Live lectures, Streaming Recorded Videos, Online Lab Workbook, and Remote Virtual Lab access.
- **Duration:-** 4 Days (32 Hours)

Requirements

- There are no such prerequisites but candidates should be familiarity with the Cisco IOS® Software Command-Line Interface (CLI), Cisco AnyConnect® Secure Mobility Client, Microsoft Windows operating systems, 802.1X

What you will learn

- Understanding how to provide secure business and context-based access based on policies.
- Centrally configure and manage authentication, profiler, guest, posture, and authorization services in a single web-based GUI console
- Provide experience for implementing and customizing guest network access
- Provide today's career skills for high-demand job roles and responsibilities focused on enterprise security

About Instructor

The trainer of this course has long years of industrial experience and where he has expertise in technology. The trainer is also verified by UniNets itself. He has delivered vast and complex project on the same all over the world.

Course Content

- Basic Understanding 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
- Understanding 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
 - Execute Third-Party Network Access Device Support
 - Introducing Cisco TrustSec
 - Cisco TrustSec Configuration
 - Easy Connect
- Understanding Web Authentication and Guest Services
 - Introducing Web Access with Cisco ISE
 - Introducing Guest Access Components
 - Configuring Guest Access Settings
 - Configuring Sponsor and Guest Portals
- Understanding Cisco ISE Profiler
 - Introducing Cisco ISE Profiler
 - Profiling Deployment and Best Practices
- Understanding Cisco ISE BYOD
 - Introducing the Cisco ISE BYOD Process
 - Describing BYOD Flow
 - Configuring the My Devices Portal
 - Configuring Certificates in BYOD Scenarios
- Understanding Cisco ISE Endpoint Compliance Services
 - Introducing Endpoint Compliance Services
 - Configuring Client Posture Services and Provisioning in Cisco ISE
- Understanding 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

Lab outline

- Access the SISE Lab and Install ISE 2.4
- Implement Initial Cisco ISE Setup, GUI Familiarization, and System Certificate Usage
- Integrate Cisco ISE with Active Directory
- Execute Basic Policy on Cisco ISE
- Execute Policy Sets
- Execute Access Policy for Easy Connect
- Execute Guest Access
- Execute Guest Access Operations
- Create Guest Reports
- Execute Profiling
- Customize the Cisco ISE Profiling Configuration
- Create Cisco ISE Profiling Reports
- Execute BYOD
- Blacklisting a Device

- Execute Cisco ISE Compliance Services
- Execute 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

Note: ***most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You

Visit us

<https://www.uninets.com/>