Software Defined Access & ISE Integration for Policy Deployment & Enforcement (SDAISE) 1.0

Course Overview:

There are many challenges today in managing the network because of manual configuration and fragmented tool offerings. Manual operations are slow and error-prone and these issues will be exacerbated due to the constantly changing environment with more users, devices and applications. With the growth of users and different devices types coming into the network, it is more complex to configure user credentials and maintain a consistent policy across the network. If your policy is not consistent, there is the added complexity of maintaining separate policies between wired and wireless. As users move around the network, it also becomes difficult to locate users and troubleshoot issues. The bottom line is that the networks of today do not address today's network needs. This SDA course addresses these issues.

Software-Defined Access (SD-Access) is the industry's first intent-based networking solution for the Enterprise built on the principles of **Cisco's Digital Network Architecture (DNA)**. **SD-Access** provides automated end-to-end segmentation to separate user, device and application traffic without redesigning the network. **SD-Access** automates user access policy so organizations can make sure the right policies are established for any user or device with any application across the network. This is accomplished with a single network fabric across LAN and WLAN which creates a consistent user experience anywhere without compromising on security.

Who Should Attend:

- Anyone interested in knowing about SD-Access
- Personnel involved in SD-Access Design and Implementation
- Network Operations team with SD-Access solution

PREREQUISITES:

It is recommended that students have the following knowledge and skills prior to attending this course:

- Knowledge level equivalent to Cisco CCNA Routing & Switching
- Basic knowledge of Software Defined Networks
- Basic knowledge of network security including AAA, Access Control and ISE
- Basic knowledge and experience with Cisco IOS, IOS XE and CLI

COURSE OBJECTIVES:

Upon completion of this course, the learner will be able to meet these overall objectives:

- Explain the role that ISE plays as part of the solution
- Configure AAA services and TrustSec Policy in ISE
- Explain ISE Integration with DNA Center for Policy enforcement
- Know and understand Cisco's SD-Access concepts, features, benefits, terminology and the way this approach innovates common administrative tasks on today's networks.
- Differentiate and explain each of the building blocks of SD-Access Solution
- Explain the concept of "Fabric" and the different node types that conform it (Fabric Edge Nodes, Control Plane Nodes, Border Nodes)
- Describe the role of LISP in Control Plane and VXLAN in Data Plane for SD-Access Solution
- Understand TrustSec concepts, deployment details and the way it is used as part of SD-Access Solution for segmentation and Policy Enforcement
- Understand the role of DNA Center as solution orchestrator and Intelligent GUI
- Be familiar with workflow approach in DNA Center - Design, Policy, Provision and Assurance

Course Outline:

Module 1: Cisco ISE Integration for SD Access

- Introduction to Cisco ISE
- Using Cisco ISE as a Network Access Policy Engine
- Introducing Cisco ISE Deployment Models
- Introducing 802.1x and MAB Access: Wired and Wireless
- Introducing Identity Management
- Configuring Certificate Service
- Introducing Cisco ISE Policy
- Configuring Cisco ISE Policy Sets
- Introduction to Cisco TrustSec for segmentation
- The Concept of Security Group (SG) and Security Group Tag (SGT)
- Cisco TrustSec Phases
  - Classification
  - Propagation
  - Enforcement
- Methods for Classification
  - Static Classification
  - Dynamic Classification
- Methods for SGT tag propagation
  - Inline Tagging
  - SGT Exchange Protocol (SXP)

Module 2: Introduction to Cisco's Software Defined Access (SD-Access)

- SD-Access Overview
- SD-Access Benefits
- SD-Access Key Concepts
- SD-Access Main Components
  - Campus Fabric
    - Wired
    - Wireless

- Nodes
  - Edge
  - Border
  - Control Plane
- DNA Controller (APIC-EM Controller)
- Introducing Cisco ISE 2.x px
- 2-level Hierarchy
  - Macro Level: Virtual Network (VN)
  - Micro Level: Scalable Group (SG)

Module 3: DNA Center Workflow

- DNA Center Refresher
- Creating Enterprise and Sites Hierarchy
- Configuring General Network Settings
- Loading maps into the GUI
- IP Address Management
- Software Image Management
- Network Device Profiles
- Introduction to Analytics
- NDP Fundamentals
- Overview of DNA Assurance

Module 4: SD-Access Campus Fabric

- The concept of Fabric
- Node types (Breakdown)
- LISP as protocol for Control Plane
- VXLAN as protocol for Data Plane

Module 5: Campus Fabric External Connectivity for SD-Access

- Enterprise Sample Topology for SD-Access
- Role of Border Nodes
- Types of Border Nodes
  - Border
  - Default Border

- Single Border vs. Multiple Border Designs
- Collocated Border and Control Plane Nodes
- Distributed (separated) Border and Control Plane Nodes

Module 6: Implementing WLAN in SD-Access Solution

- WLAN Integration Strategies in SD-Access Fabric
  - Fabric CUWN
  - SD-Access Wireless (Fabric enabled WLC and AP)
- SD-Access Wireless Architecture
  - Control Plane: LISP and WLC
  - Data Plane: VXLAN
  - Policy Plane and Segmentation: VN and SGT
- Sample Design for SD-Access Wireless

Lab Outline:

- Configure Initial Cisco ISE
- Integrate ISE with Active Directory
- Configure Basic Policies on ISE
- Navigating Cisco DNA Center
- Discover the SD-Access Underlay
- DNA Center Design
- DNA Center Policies
- DNA Center Provisioning and Onboarding