

Implementing Cisco Bring Your Own Device Solutions (SBYOD)

Duration 5 Days

OVERVIEW

The Implementing Cisco Bring Your Own Device Solutions (SBYOD) course is a three-day instructor-led course that is aimed at enabling Cisco customers and System Engineers (SEs) to understand advanced concepts, architecture, and use cases that are related to the Cisco Identity Services Engine (ISE). This course will also prepare learners to implement advanced Cisco ISE solutions. The focus is to extend the knowledge that is gained in the SWISE course material to ensure that students can implement additional, advanced features of Cisco ISE deployments.

OBJECTIVES

After you complete this course you should be able to:

- Describe the concepts and components of the Cisco ISE solution
- Describe AAA concepts as they relate to Cisco ISE
- Create a BYOD policy
- Describe and configure guest access
- Create BYOD policy flows using device profiling capabilities
- Describe device registration and the MDP, and implement NSP and BYOD policies
- Integrate MDM with Cisco ISE, including on-boarding and posturing configuration and control

TARGET AUDIENCE

Engineers involved in the deployment and management of corporate security policies, that incorporate the Cisco Identity Services Engine Solution.

PREREQUISITES

Attendees should meet the following prerequisites:

- Cisco CCNA Wireless certification (ICND1+IUWNE) or commensurate wireless experience
- Basic knowledge of 802.1X
- Familiarity with Microsoft Active Directory and LDAP
- Have attended the SISE or SWISE course, or have commensurate field experience

OUTLINE

Reviewing Cisco ISE and NAD

- Cisco ISE architecture and components
- NAD types and features
- Cisco AnyConnect and endpoint native supplicants

Reviewing Authentication and Authorization

- Authentication services
- Validating Credentials from Different Identity Sources
- Authentication Policy, Components and their Configuration
- Cisco ISE Authorization Policies and their Components
- CoA and common enforcement mechanisms, including dACLs, named ACLs, VLANs, and SGTs

Creating a BYOD Policy

- BYOD concepts
- BYOD Policy Flows
- Guest Access Services
- Device Profiling Services and BYOD Policy Flows
- Cisco ISE Device Management Services and BYOD Policy Flows
- MDM Services and BYOD Policy Flows

Providing Guest Access

- Operating Guest services
- Implementing MAB and Configuring NADs for guest access
- Configuring and customizing Guest Services Portals
- Customizing Portal Interfaces and Ports
- Common Guest Policy BYOD scenarios

Configuring Device Profiling

- Cisco ISE Profiling Components and Features
- Enable and Configure Profiling Probes
- Configure Device Sensor Functionality
- Deploying the Profiling Attribute Filter
- Device Profile Conditions and Customization
- Configure BYOD policies using logical profiles and custom profiles

Implementing Device Registration and NSP

- Configuring MDP to support employee device registration
- Integrating Cisco ISE with a CA service
- Configuring NSP using the dual SSID method
- Configuring Authorization logic for device on-boarding and NSP flows

Integrating Mobile Device Management

- Cisco ecosystem MDM partners
- Configuring Cisco ISE and Cisco ecosystem partner MDM server integration
- Deploying MDM on-boarding
- Deploying Mobile Device Posture
- Configure BYOD policies using on-boarding and mobile device posture

LABS

- Lab 2-1: Configure Basic Authentication and Authorization
- Lab 4-1: Configure Cisco ISE Guest Access
- Lab 5-1: Configure and Validate Cisco ISE Profiling
- Lab 6-1: Configure Device Registration and NSP BYOD On-Boarding using Dual SSIDs
- Lab 6-2: Test On-Boarding
- Lab 7-1: Integrate Mobile Device Management