# SISE (IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICES ENGINE (SISE) V3.0) 3.0

## Objetivo

After taking this course, you should be able to: â¢ Describe Cisco ISE deployments, including core deployment components; â¢ Describe how they components interact to create a cohesive security architecture; â¢ Describe the advantages of such a deployment; â¢ Describe how each Cisco ISE capability contributes to these advantages; â¢ Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services; â¢ Describe how Cisco ISE policy sets are used to implement authentication and authorization; â¢ Describe how to leverage this capability to meet the needs of your organization; â¢ Describe third-party Network Access Devices (NADs), Cisco TrustSecÂ®, and Easy Connect; â¢ Describe and configure web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios; â¢ Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints; â¢ Describe best practices for deploying this profiler service in your specific environment; â¢ Describe BYOD challenges, solutions, processes, and portals; â¢ Configure a BYOD solution, and describe the relationship between BYOD processes and their related configuration components; â¢ Describe and configure various certificates related to a BYOD solution; â¢ Describe the value of the My Devices portal and how to configure this portal; â¢ Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE; â¢ Describe and configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets; â¢ Understand the role of TACACS+ within the Authentication, Authentication, and Accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols; â¢ Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool. Prepare for 300-715 SISE exam, that certifies your knowledge of Cisco Identify Services Engine, including architecture and deployment, policy enforcement, Web Auth and guest services, profiler, BYOD, endpoint compliance, and network access device administration.

## PÃºblico Alvo

â¢ Professionals involved in deployment and maintenance of the Cisco ISE platform, integrating with wired and wireless control access. â¢ Professionals who need to prepare for the Cisco 300-715 certification exam.

## PrÃ©-Requisitos

To fully benefit from this course, desirable have the following knowledge: â¢ Familiarity with Switch Cisco IOSÂ® Software Command-Line Interface (CLI); â¢ Familiarity with WLC Cisco AirOSÂ® Software GUI Interface; â¢ Familiarity with Cisco AnyConnectÂ® Secure Mobility Client; â¢ Familiarity with Microsoft Windows operating systems; â¢ Familiarity with 802.1X.

## Carga HorÃ¡ria

40 horas (5 dias).

## ConteÃºdo ProgramÃ¡tico

**Course Introduction**
Course Goal and Objectives
Course Flow

**Introducing Cisco ISE Architecture and Deployment**
Describe the advantages of each Cisco ISE capability contributes to network access control
Describe using Cisco ISE as a Network Access Policy Engine
Describe core components of secure access, Cisco ISE services, benefits, challenges, and functions.
Presenting examples of Cisco ISE Use Cases
Describe typical scenarios where Cisco ISE is particularly valuable
Describing Cisco ISE Functions
Describe each major Cisco ISE function, along with key aspects and advantages of those functions
Presenting the Cisco ISE Deployment Models
Describe Cisco ISE nodes, personas, and roles.
Presenting Radius & Tacacs+ Protocols
Describe the context visibility feature, and explain the advantages it offers to administration and troubleshooting tasks
Practical Use: Install and input basic settings for ISE 2.X

**Cisco ISE Policy Enforcement**
Describe concepts and configure components related to 802.1X and MAB authentication
Describe using identity management and certificate services
Understanding Cisco ISE policy sets
Describe hierarchical policy system is used to implement authentication and authorization policies
Describe how using 802.1X for Wired and Wireless Access
Describe how to Cisco ISE interacts with NADs to limit user access
Describe how the use VLAN assignment, ACL assignment, time-based access, and SGA
Describe how to use 802.1X deployment, using monitor mode, low-impact mode, and closed mode
Describe the components and processes related to 802.1X authentication, authorization, and CoA
Describe how access switch ports can accommodate various 802.1X host modes,
Describe how to accommodate a single host or multiple hosts
Describes MAC Authentication Bypass (MAB) benefits and functionality
Describe MAB message flow, along with MAB design considerations
Describe key 802.1X implementation guidelines using MAB for Wired and Wireless Access
Practical Usage: Using MAB (MAC Authentication Bypass) for Wired and Wireless Access
Practical Usage: 802.1X and MAB configuration

**Introducing Identity Management**
Describe identity sources databases of end user and machine credentials
Describe and configure identity sources that are internal to Cisco ISE
How using Local User Database, AD Microsoft, LDAP and Others
Describe external identity sources: AD, LDAP, RSA servers, multi-AD capabilities
Describe tools for diagnosing and troubleshooting AD issues, and more
Describe and configure Identity Source Sequences (ISS) to accommodate multiple identity sources
Configuring Certificate Services
Integrating ISE with CA Corporate Certificate Authority

Describe CA services, and how ISE uses them for secure communications
Describe key features provided by Cisco ISE Certificate Authority (CA) services.
Describe using server and client certificates
Describe how configuring certificate authentication profiles
Describe how Integrate Cisco ISE with Active Directory
Describe how populate the Cisco ISE dictionary with Active Directory attributes
Implementing Third-Party Network Access Device Support
Describes third-party Network Access Device (NAD) Support on Cisco ISE
Describe the key configurations steps for third-party NAD Support
Introducing Cisco TrustSec Model
Describe the functions and advantages of TrustSec, to create a very scalable security solution
Describe TrustSec components and capabilities
Cisco ISE TrustSec Configuration
Describe how to configure TrustSec on Cisco ISE, and on the NADs
Cisco ISE Easy Connect
Explain the purpose of Easy Connect Access, its key characteristics, and caveats related to its use.
Describe the two modes of Easy Connect: Visibility and Enforcement
Practical Usage: Integrate Cisco ISE with Active Directory
Practical Usage: Configure Cisco ISE Basic Policy-Sets
Practical Usage: Configure Access Policy for Easy Connect

**Web Auth and Guest Services**
Introducing Web Access with Cisco ISE
Describe Web Authentications Process
Describe the components involved in web access, as well as the various Cisco ISE Web Access Portals.
Describe the Guest Access use, like BYOD, and WebAuth
Describe the high-level configuration steps for web access
Web Guest Authentication & Authorization Options
Describe guest access services, and the access flow for various use cases.
Describe hotspot access, self-registered access, self-registered access with approval, and sponsored access
Describe how Cisco ISE supports multiple Guest Portals
Using for BYOD, Sponsored and Self-Registration
Introducing Guest Access Components
Configuring Guest Access Settings
Understand sponsor groups work and how to configure sponsor settings and customize sponsor portals
Describe how Sponsor user creating guest accounts via both the desktop and mobile sponsor portals
Describe how sponsor groups work, configure sponsor settings, and customize sponsor portals
Describes Cisco ISE sponsor components and configuration
Describe how Sponsor user to manage their guest accounts
Practical Use: Configure Sponsor and Guest Portals
Practical Use: Configure Guest Access Operations
Practical Use: Create Guest Reports

**Cisco ISE Profiler**
Describe and configure Cisco ISE profiling services, and to monitor these services
Describe the Profiler services, sources, processes, and probes
Describe various best practices for deploying this profiler service in your specific environment
Describe Change of Authorization, and also describe the Cisco ISE Profiler work center and dashboards

Describe Profiling Deployment and Best Practices
Describe each probe based on their difficulty to deploy, impact , and value in gathering the information
Practical Use: Configure Profiling
Practical Use: Customize the Cisco ISE Profiling Configuration
Practical Use: Create Cisco ISE Profiling Reports

**Cisco ISE BYOD**
Introducing the Cisco ISE BYOD Process
Describe the challenges that corporations have
Describe how Cisco ISE BYOD solution speaks directly to these challenges
Describe the BYOD solution, and specific BYOD services
Describe the employee self-registration of personal devices, and provisioning these devices with certificates
Describe the ability uses of Blacklists for stolen devices and reinstate when recovered
Describe BYOD design aspects related to single SSID and Dual SSID BYOD deployments
Describe various BYOD use cases
Describe BYOD Access Models
Describing BYOD Flow
Describe the relationship between various BYOD processes and their related Cisco ISE configuration
Describe processes and configurations involved in BYOD policies and native supplicant provisioning
Configuring the My Devices Portal
Describe and configure the My Devices portals to facilitate BYOD solutions
Describe two portals relevant to BYOD
Describe BYOD portal used for employee self-registration of their personal devices
Describe My Devices portal configuration
Configuring Certificates in BYOD Scenarios
Describe the use of certificates with BYOD access.
Describe how to use and configure the local ISE CA Server and Local Certificates
Describe how to use Certificate Templates and Certificate Operations
Practical Use: Configure BYOD

**Cisco ISE Endpoint Compliance Services**
Introducing Endpoint Compliance Services
Describe endpoint compliance and network access
Describe the components of endpoint compliance, including posture agents, posture services and conditions
Describe the flow of the posture process, operational modes, and licensing requirements
Describe Endpoint Compliance Configuration Steps
Describe how Cisco ISE collects various data from the client via a posture agent
Describe how this collected data is evaluated against posture policies to ensure endpoint compliance
Configure Policy for Endpoint Compliance
Configure Cisco Client Anyconnect Provisioning
Configure Cisco ISE policy to provision Cisco posture agents
Configuring Client Posture Services and Provisioning
Practical Use: Configure Cisco ISE Compliance Services
Practical Use: Configure Client Provisioning
Practical use: Configure Posture Policies
Practical Use: Test and Monitor Compliance Based Access
Practical Use: Test Compliance Policy

**Working with Network Access Devices**
Review AAA Model
Describe TACACS+ and its role within the AAA framework
Describe AAA, compare AAA protocols, and TACACS+ functions in network device administration
Describes configuring Cisco ISE for TACACS+ network device administration services
Describes the necessary configuration steps taken on Cisco ISE to enable device administration
Describes how to configure TACACS+ settings, command sets, profiles, and policy sets
Describes the TACACS logging capabilities in Cisco ISE
TACACS+ Device Administration Guidelines and Best Practices
Describe TACACS+ device administration best practices and guidelines when deploying TACACS+
Describe methods of deployment, configuration best practices, and policy set guidelines
Migrating from Cisco ACS to Cisco ISE
Describes migrating TACACS+ configurations from a Cisco Secure ACS to Cisco ISE
Describe the major differences between platforms
Describe the use of the ACS migration tool, and features that are migrated from Cisco ACS to Cisco ISE
Practical Use: Configure Cisco ISE for Basic Device Administration
Practical Use: Configure TACACS+ Command Authorization

**Labs Outline**
DISCOVERY 1: CONFIGURE INITIAL CISCO ISE
Task 1: Verify Cisco ISE setup using CLI
Task 2: Initial GUI login and Familiarization
Task 3: Promote Cisco ISE to Primary
Task 4: Certificate enrollment

DISCOVERY 2: INTEGRATE CISCO ISE WITH AD
Task 1: Configure Active Directory Integration
Task 2: Run Diagnostic Tools
Task 3: Add Active Directory Groups to Cisco ISE
Task 4: Test Authentication

DISCOVERY 3: CONFIGURE ISE BASIC POLICY
Task 1: Policy Configuration for AD Employees and AD Contractors
Task 2: Configure Client Access – Wired
Task 3: Test Client Wired Access
Task 4: Configure Client Access – Wireless Network
Task 5: Test Wireless Access
Task 6: Network visibility with Context Visibility

DISCOVERY 4: CONFIGURE PARAMETERS GUEST ACCESS
Task 1: Configure Guest General Settings
Task 2: Configure Guest Locations

DISCOVERY 5: CONFIGURE GUEST ACCESS OPERATIONS
Task 1: Configure Cisco ISE Guest Hotspot
Task 2: Test Cisco ISE Guest Hotspot
Task 3: Configure Guest Self-Registration
Task 4: Test Guest Self-Registration

Task 5: Guest Sponsor Registration

DISCOVERY 6: CREATE GUEST REPORTS
Task 1: Running Reports from Cisco ISE Dashboard
Task 2: Access from Cisco Operations Reports

DISCOVERY 7: CONFIGURE PROFILING
Task 1: Configuring Profiling in Cisco ISE
Task 2: Configure the Feed Service
Task 3: Configuring Profiling in Cisco ISE
Task 4: Check NAD Configuration for Profiling

DISCOVERY 8: CISCO ISE PROFILING CONFIGURATION
Task 1: Examine Endpoint Data
Task 2: Create a Logical Profile
Task 3: Creating a Policy Using a Logical Profile
Task 4: Testing Authorization Policies with Profiling Data

DISCOVERY 9: CREATE CISCO ISE PROFILING REPORTS
Task 1: Run Cisco ISE Profiler Feed Reports
Task 2: Endpoint Profile Changes Report
Task 3: Context Visibility Dashlet Reports

DISCOVERY 10: CONFIGURE ISE COMPLIANCE SERVICES
Task 1: Posture Preparation
Task 2: Authorization Profiles
Task 3: Adjusting Wired Authorization Policy for Compliance

DISCOVERY 11: CONFIGURE WIRED CLIENT PROVISIONING
Task 1: Client Updates
Task 2: Client Resources
Task 3: Client Provisioning Policies
Task 4: Testing Client Provisioning Policies

DISCOVERY 12: CONFIGURE POSTURE POLICIES
Task 1: Configure Posture Conditions
Task 2: Configuring Posture Remediation
Task 3: Configuring Posture Requirements
Task 4: Configuring Posture Policies

DISCOVERY 13: TEST WIRED COMPLIANCE ACCESS
Task 1: Testing Compliance Rules
Task 2: Testing Cisco ISE Default Rules

DISCOVERY 14: CONFIGURE WIRELESS COMPLIANCE
Task 1: Configure Autorization Profiles
Task 2: Modify Policy Set Rules

DISCOVERY 15: TEST WIRELESS COMPLIANCE ACCESS
Task 1: Testing Wireless Compliance Rules
Task 2: Verify Wireless Access

DISCOVERY 16: BASIC DEVICE ADMINISTRATION
Task 1: Configure TACACS+ Initial Parameters
Task 2: Configure TACACS+ Initial Parameters
Task 3: Configure Switch Integration TACACS+

DISCOVERY 17: TACACS+ COMMAND AUTHORIZATION
Task 1: Configure Command Sets
Task 2: Configure Switch Integration Commands TACACS+

DISCOVERY 18: CISCO TRUSTSEC
Task 1: Switch Configuration
Task 2: Cisco ISE Trustsec configuration
Task 3: Cisco ISE Policy Set Configuration
Task 4: Check Switch Pod & Cisco ISE TrustSec Synch
Task 5: Test Cisco ISE TrustSec