

# SISE (IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICES ENGINE) 2.1

## Objetivo

Implementing and Configuring Cisco Identity Services Engine (SISE) 2.1 é um curso com carga horária de 5 dias (40 horas) para a capacitação de profissionais para instalação e implantação de soluções de nova geração para controles de acesso (NAC) Cisco ISE 2.1. O Curso abrange os componentes chaves e procedimentos necessários para instalação, configuração, gerência e suporte da solução em rede cabeadas, sem fio e serviços de VPN de acesso remoto. O curso tem uma abordagem direta e prática, e como principal característica apresentações dos conceitos e utilização de laboratórios intensivos. Ao completar o curso, o aluno vai estar preparado para:

- Instalar o Cisco ISE 2.1;
- Entender os conceitos e utilização de políticas para controle da conformidade de acesso a rede utilizando: o Integração com Active Directory; o Cisco ISE Policy Sets; o Cisco ISE EasyConnect; o EAP-FAST com EAP Chaining; o Políticas para BYOD; o Postura com AnyConnect 4.x para LAN and VPN; o Integrar Threat Centric NAC utilizando AMP; o Integração PxGrid; o TACACS+ para gerenciamento de equipamentos; o TrustSec Security Group Access.
- Configurar e disponibilizar uma solução para controle central do acesso de usuários convidados e patrocinadores de convidados ;
- Configurar uma solução para controle da postura de acesso;
- Entendimento das melhores práticas recomendadas pela Cisco.

## Público Alvo

O público primário recomendado para esse curso são:

- Profissionais de canais parceiros ou do cliente final para implantação e configuração de uma solução envolvendo Cisco ISE versão 2.1.

## Pré-Requisitos

Para um melhor aproveitamento desse curso é recomendado que o aluno possua os seguintes habilidades e conhecimentos prévios:

- Conhecimentos e familiaridade com Cisco IOS CLI
- Conhecimentos e familiaridade com Cisco ASA
- Conhecimentos e familiaridade com Cisco VPN clients
- Conhecimentos e familiaridade Windows OS
- Conhecimentos e familiaridade com 802.1X

## Carga Horária

40 horas (5 dias).

## Conteúdo Programático

Module 1: Introducing Cisco ISE Architecture and Deployment

Lesson 1: Using Cisco ISE as a Network Access Policy Engine

- Cisco Identity Services Overview
- Cisco Identity Solution Benefits

- The Attack Continuum
- Controlling Access to the Network
- Security Challenges for IT Organizations
- Centralized Policy Management
- Cisco Identity Solution Guest Use Case
- Cisco Identity Solution BYOD Use Case
- Cisco Identity Solution Profiling Use Case
- Cisco Identity Solution Compliance Use Case
- Cisco Identity Solution Security Group Access Use Case
- Introducing the Components of a Cisco ISE Deployment
- Secure Access Control
- Describing Cisco ISE Functions
- Summary

## Lesson 2: Introducing Cisco ISE Deployment Models

- Cisco ISE Nodes and Personas
- Implementing Nodes, Personas, and Roles
- Admin Node
- Policy Service Node
- Monitoring Node
- pxGrid Services
- Collector Agent
- Policy Synchronization
- Deployment Options
- Cisco ISE Communication Model
- Introducing Context Visibility
- Context Visibility Benefits
- Context Visibility Wizard
- Streamline Visibility Wizard
- Summary

## Module 2: Cisco ISE Policy Enforcement

### Lesson 1: Introducing 802.1X and MAB Access: Wired and Wireless

- IEEE 802.1X Primer
- MAC Authentication Bypass
- Overview: Configure 802.1X and MAB
- Summary

### Lesson 2: Introducing Identity Management

- Identity Sources Overview
- Internal Identity Sources
- External Identity Sources
- Multi-AD Overview and Configuration
- Lightweight Directory Access Protocol
- RADIUS
- SAMLv2
- Identity Source Sequence

- Summary

#### Lesson 3: Configuring Certificate Services

- Certificate Overview and Implementation
- Certification Authority Services
- Summary

#### Lesson 4: Introducing Cisco ISE Policy

- Authentication and Authorization Process
- Dictionaries, Identity Sources, and ISSs
- Authentication and Its Components
- Authorization and Its Components
- Exception Policies and Policy Sets
- Sessions in Cisco ISE
- Summary

#### Lesson 5: Configuring Cisco ISE Policy Sets

- Cisco ISE Policy Sets Overview
- Global versus Local Exception Processing

#### Lesson 6: Implementing Third-Party Network Access Device Support

- Third-Party NAD Support: Features and Workflows
- Summary

#### Lesson 7: Introducing Cisco TrustSec

- Introducing Cisco TrustSec

#### Lesson 8: Introducing EasyConnect

- Easy Connect Overview
- EasyConnect Modes and Flows
- EasyConnect Configuration
- Summary

#### Module 3: Web Auth and Guest Services

##### Lesson 1: Introducing Web Access with Cisco ISE

- Web Authentication Overview
- ISE Web Authentication Configuration Overview
- Web Authentication Verification Overview
- Summary

##### Lesson 2: Introducing ISE Guest Access Components

- Guest Access Services Overview
- Summary

##### Lesson 3: Configuring Guest Access Settings

- Review Guest Access Settings
- Guest Types Overview

- Summary

## Lesson 4: Configuring Portals: Sponsors and Guests

- Cisco ISE Sponsor Components and Configuration

## Module 4: Cisco ISE Profiler

### Lesson 1: Introducing Cisco ISE Profiler

- Introduction to the Profiler Service
- Cisco ISE Probes
- Profiling Policies
- Summary

### Lesson 2: Configuring Cisco ISE Profiling

- Configure Profiling on Cisco ISE Overview
- Prepare for Profiling
- Enable the Profiling Service
- Profiling Probe Configuration
- Configuring the Profiler Feed Service
- Profiling Settings
- Define Profiling Parameters
- Configure Profile Policies and Logical Profiles
- NMAP Scan Actions
- Go Live and Monitor
- Summary

## Module 5: Cisco ISE BYOD

### Lesson 1: Introducing the Cisco ISE BYOD Process

- BYOD Problem and Solutions
- BYOD Design

### Lesson 2: Describing BYOD Flow

- Describe BYOD portal selection process.
- Summary

### Lesson 3: Configuring My Devices Portal Settings

- My Devices Portal Configuration
- My Devices Portal End-User Experience

### Lesson 4: Configuring Certificates in BYOD Scenarios

- Local ISE CA Server and Local Certificates
- Cisco ISE Certificates Set Up Walk-through

## Module 6: Cisco ISE Endpoint Compliance Services

### Lesson 1: Introducing Endpoint Compliance

- Endpoint Compliance

- Posture Service
- Posture Conditions
- Compliance Module
- Posture Flow
- Cisco ISE Posture Agents
- Posture Operational Modes
- Posture Service Deployment and Licensing
- Summary

## Lesson 2: Configuring Client Posture Services and Provisioning in

### Cisco ISE

- Client Provisioning
- Posture Configuration Procedure
- Prepare
- Client Provisioning Resources
- Posture General Settings
- Posture Policy
- Client Provisioning Portal
- Client Provisioning Policy
- Additional Configuration Tasks
- Summary

## Module 7: Cisco ISE with AMP and VPN-Based Services

### Lesson 1: Introducing VPN Access Using Cisco ISE

- AAA – External Authentication
- Using Cisco ASA for VPN Authentication
- VPN Access Configuration Overview
- Summary

### Lesson 2: Configuring Cisco AMP for ISE

- Threat Centric NAC Overview
- Threat Centric NAC Configuration
- Summary

## Module 8: Cisco ISE Integrated Solutions with APIs

Objective: Introduce location-based authorization on Cisco ISE using Cisco MSE

### Lesson 1: Introducing Location-Based Authorization

- Introducing Location-Based Authorization

### Lesson 2: Introducing Cisco ISE 2.x pxGrid

- pxGrid Framework
- pxGrid on Cisco ISE
- Use Case: pxGrid for Rapid Threat Detection

## Module 9: Working with Network Access Devices

### Lesson 1: Configuring TACACS+ for Cisco ISE Device Administration

- 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
- Summary

## Module 10: Cisco ISE Design (Self-Study)

### Lesson 1: Designing and Deployment Best Practices

- Cisco ISE Planning and Pre-deployment
- Cisco ISE Sizing and Scaling Practices

### Lesson 2: Performing Cisco ISE Installation and Configuration Best Practices

- Cisco ISE Deployment Best Practices
- ISE Certificates Best Practices
- ISE Profiling Best Practices
- Web Portals Best Practices
- Logging and Troubleshooting Best Practices

### Lesson 3: Deploying Failover and High-Availability

- PSN HA or Load Sharing
- Deploying Monitoring Personas
- Preparing the Network Infrastructure

## Module 11: Configuring Third Party NAD Support (Optional/Self-Study/Reference)

### Lesson 1: Configuring Third-Party NAD Support

- Configuring Third-Party NAD Support
- Summary

## Labs

Lab 1: Configure Initial Cisco ISE setup, GUI Familiarization, system certificate usage

Lab 2: Integrate Cisco ISE with Active Directory

Lab 3: Configure Basic Policy on Cisco ISE

Lab 4: Configure Conversion to Policy Sets

Lab 5: Configure Access Policy for Easy Connect

Lab 6: Configure Guest Access

Lab 7: Configure Guest Access Operations

Lab 8: Create Guest Reports

Lab 9: Configure Profiling

Lab 10: Customize the Cisco ISE Profiling Configuration

Lab 11: Create Cisco ISE Profiling Reports

Lab 12: Configure BYOD

Lab 13: Blacklisting a Device

- Lab 14: Configure Compliance Services on Cisco ISE
- Lab 15: Configure Client Provisioning
- Lab 16: Configure Posture Policies
- Lab 17: Test and Monitor Compliance Based Access
- Lab 18: Test Compliance Policy
- Lab 19: Configure Cisco ISE for VPN Access
- Lab 20: Configure Threat-Centric NAC using Cisco AMP
- Lab 21: Configure Cisco ISE pxGrid and Cisco WSA Integration
- Lab 22: Configure Cisco ISE for Basic Device Administration
- Lab 23: Configure TACACS+ Command Authorization