SISE

Implementing and Configuring Cisco Identity Services Engine (SISE) 5.0

40 horas | Security & Cybersecurity | Cisco

Cisco Continuing Education Credits

32 CE Credits

INTRODUÇÃO

The Implementing and Configuring Cisco Identity Services Engine (SISE) training teaches you to deploy, configure, and operate Cisco® Identity Services Engine (ISE) as the central platform for identity-based access control. Learning begins with the core architecture and installation and progresses through network access control, identity stores, policy design, and day-to-day operations.

In this course, you will learn to deploy and use Cisco Identity Services Engine (ISE) v3.x, an identity and access control policy platform that simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. This hands-on course provides you with the knowledge and skills to implement and apply Cisco ISE capabilities to support use cases for Zero Trust security posture. These use cases include tasks such as policy enforcement, profiling services, web authentication and guest access services, BYOD, endpoint compliance services, and TACACS+ device administration.

• Covering Cisco ISE versions 3.4 & v3.5

This training will help you:

• Gain hands-on experience configuring, deploying, and operating Cisco ISE for identity-based access control in enterprise environments

• Develop skills to design and implement secure authentication, authorization, guest access, and BYOD onboarding policies for both wired and wireless networks

• Learn to integrate Cisco ISE with Active Directory, LDAP, and network devices, as well as configure endpoint profiling and compliance-based access controls

• Acquire troubleshooting techniques for authentication and policy issues using practical labs and reporting tools, improving real-world problem-solving abilities

• Prepare for the 300-715 SISE v1.1 exam

• Earn 32 CE credits toward recertification

This training prepares you for 300-715 SISE v1.1 exam. If passed, you earn the Cisco Certified Specialist – Security Identity Management Implementation certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification. This training also earns you 32 Continuing Education (CE) credits toward recertification.

Implementing and Configuring Cisco Identity Services Engine (300-715 SISE) v1.1 is a 90-minute exam associated with the Cisco Certified Specialist – Security Identity Management Implementation certification and satisfies the concentration exam requirement for the CCNP Security certification.

This exam tests your knowledge of Cisco ISE, including:

• Architecture and deployment

• Policy enforcement

• Web Auth and guest services

• Profiler

• BYOD

• Endpoint compliance

• Network access device administration

OBJETIVO DO CURSO

Upon completing this course you will be able to:

• Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture.

• Describe the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages

• Describe concepts and configure components related authentication, identity management, and certificate services

• Describe how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization

• Describe third-party Network Access Devices (NADs), Cisco TrustSec, and Easy Connect

• Configure web authentication and guest services, including guest access components and various guest access scenarios

• Describe and configure Cisco ISE profiling services. Understand how to monitor these services to enhance endpoint security and ensure secure edge

• Describe BYOD challenges, solutions, processes, and portals. Configure a BYOD solution and describe the relationship between BYOD processes and their related configuration components. Describe and configure various certificates related to a BYOD solution

• Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE

• Describe the fundamentals of Identity and Access Management (IAM) by leveraging TACACS+. Configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understand the role of TACACS+ within the Authentication, Authorization, and Accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols

PÚBLICO-ALVO

• Network Security Engineers

• Network Administrators

• Consulting Security Engineers

• Technical Solutions Architects

• Network Managers

• Sales Engineers and Account Managers

PRÉ-REQUISITOS

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

• Familiarity with the Cisco IOS® Command-Line Interface (CLI) for wired and wireless network devices

• Familiarity with Cisco Secure Client

• Familiarity with Microsoft Windows operating systems

• Familiarity with 802.1X

These skills can be found in the following Cisco Learning Offering:

• Implementing and Operating Cisco Security Core Technologies (SCOR)

CONTEÚDO PROGRAMÁTICO

Introduction

• Cisco ISE Evolution, Foundation, and Role
• What Is Cisco ISE?
• Evolution and Origin of Cisco ISE
• Cisco ISE Core Functions
• Cisco ISE Core Functions
• Common Enterprise Drivers for Deploying Cisco ISE

Architecture and Design

• Node Personas
• Cisco ISE Nodes Communication
• Cisco ISE v3.x Smart Licensing
• Cisco ISE Design Considerations

Cisco ISE Installation and Initial Config

• Supported Deployment Platforms
• VM Provisioning Guidance
• Installing Cisco ISE
• Cisco ISE Initial CLI Setup Wizard
• Zero Touch Provisioning in Cisco ISE
• Cisco ISE System Certificates
• Discovery 1: Explore the Initial Cisco ISE Configuration, GUI and System Certificate

802.1X in Cisco ISE

• EAP Methods and 802.1X Authentication Flow
• Authorization Results in Cisco ISE
• 802.1X Deployment Modes
• Host Modes and Considerations
• Cisco ISE Support for TLS 1.3

MAB in Cisco ISE

• MAB Overview
• MAB Operations and Message Flow
• Cisco ISE Process for MAB

Network Device Integration with Cisco ISE

• NADs Role
• NAD and Cisco ISE Interaction
• Add NADs in Cisco ISE
• Cisco ISE with Third-Party NADs
• Discovery 2: Configure Network Device Groups and Network Devices

Identity Sources and Authentication Types

• Identity Source Types in Cisco ISE
• Internal User Identity Sources
• External Identity Sources
• Certificate-Based Identity
• Certificate Management and Provisioning

Active Directory and LDAP Integration

- Active Directory and LDAP
- Active Directory Integration
- LDAP Integration
- Validate Connectivity
- Discovery 3: Integrate Cisco ISE with Active Directory

Identity Selection and Resolution Logic

- Identity Source Sequences
- Attribute Mapping and Resolution Behavior
- Identity Use Cases
- Authentication Policy Rule

Cisco ISE Policy Framework

- Policy-Set Structure
- Policy-Set Evaluation
- Filter Access Requests

Authentication Policies

- Authentication Policy Rule Structure
- Identity Source Mapping
- Condition Dictionaries and Reusable Expressions
- Discovery 3: Configure MAB

Authorization Policies

- Authorization Policy Overview
- Authorization Policy Rule Structure
- Conditions Studio
- Authorization Profile Actions
- Default Rule and Rules Ordering
- Discovery 3: Configure Wired 802.1X
- Discovery 4: Configure Wireless 802.1X & Optional Wired EAP-TLS and TEAP

Troubleshoot Policies and Sessions

- Troubleshoot Authentication and Authorization Issues
- RADIUS Communication Overview
- Live Logs Overview
- Identify Policy Set Issues
- Analyze Cisco ISE Session Data
- Discovery 5: Troubleshoot Cisco ISE 802.1X Configuration Errors

Guest Access

- Guest Access Overview
- CWA and Redirection Overview
- CWA Operation
- Guest Flow Types
- Cisco ISE Guest Management
- Guest Identities Validation Methods

Guest Access Policies and Settings

• Guest Access Settings Overview
• Guest Access Purge, Username, and Password Settings
• Guest Email and SMS Gateway
• Custom Fields Configuration
• Guest Types

Guest Portals and Lifecycle Operations
• Guest Portal Types
• Guest Portal Customization
• Guest Account Lifecycle
• Guest Portal Deployment Strategies
• Multiple Portals in Cisco ISE
• Discovery 6: Configure Non-Sponsored Guest Access

Guest & Sponsor Users
• Sponsor Group Planning
• Sponsor Groups Settings
• Sponsor Portal Configuration
• Sponsor Portal Customization
• Managing Sponsor Workflows
• Discovery 7: Configure Sponsored Guest Access

BYOD Architecture and Use Cases
• BYOD Security Challenges
• Policy-Based Approach to BYOD Enablement
• BYOD Solution Components
• Cisco ISE BYOD Features
• Single- and Dual-SSID

BYOD Onboarding with Native Supplicant Provisioning
• BYOD Onboarding Flow
• Native Supplicant Provisioning (NSP)
• NSP Configuration
• Cisco ISE Internal CA for BYOD
• Client Provisioning Policy
• Authorization Profiles and Policy Rules for BYOD
• Review: Configure BYOD

BYOD Lifecycle Operations
• My Devices Portal Overview
• My Devices Portal Flow
• Steps to Manage Lost or Stolen BYOD Devices
• Cisco ISE Internal Certificate Authority for BYOD Certificate Lifecycle
• Review: Manage BYOD Devices

Profiling: Architecture and Capabilities
• Profiling Use Cases and Benefits
• Cisco ISE Profiler Operation
• Cisco ISE Profiler Components and Data Flow
• Cisco ISE Profiler Feed Service and Identity Groups

Profiling: Probes & Data Collection

- Profiling Probes Overview
- Commonly Used Profiling Probes
- Other Profiling Probes
- Profiling Without Probes
- Device Sensors

Profiling: Policies and Authorization

- Profiling Policy Structure and Matching Logic
- Create and Manage Logical Profiles
- Profiling in Authorization Policy
- Profiler Work Center and Endpoints Classification Monitoring
- Discovery 8: Configure Profiling

Profiling: Monitoring and Design

- Profile Design
- Probe Types for Various Environments
- NAD Profiling Configuration
- Profiling Scalability and Optimization
- Monitoring with Reports and Dashboards
- Discovery 9: Configure Authorization Policy Rules and Run Profiler Reports

AAA and TACACS+

- AAA Protocols and Usage
- One Authentication, Many Authorizations
- Device Administration Basics
- Device Administration with Cisco ISE
- TACACS+ Deployment Models and Strategy

TACACS+ Device Administration

- TACACS+ Device Administration with Cisco ISE
- TACACS+ Network Device Configuration
- TACACS+ Authentication and Authorization Policy Sets
- TACACS+ Device Administration Operations Validation
- TACACS+ over TLS
- Discovery 10: Configure TACACS+ Basic Device Administration

TACACS+ Command Authorization

- Command Sets and Stacking
- Granular Control with Wildcards and Regular Expressions
- Profiles, Privilege Levels, and Role Mapping
- TACACS+ Logs and Reports
- TACACS+ Management Best Practices
- Discovery 11: Configure TACACS+ Command Authorization

Posture Service Flow and Agents

- Posture and Compliance
- Cisco ISE Posture Agent and Temporal Agent
- Posture Service Assessment and Remediation
- Posture Operational Modes

• Posture Enhancements in Cisco ISE 3.X

Posture Updates and Client Provisioning
• Evaluating Client Posture Capabilities
• Client Provisioning
• Cisco ISE Posture Work Center and Posture Updates
• Client Provisioning Resources
• Client Provisioning Policy
• Discovery 12: Configure Posture Preparations and Client Provisioning

Posture Policies and Compliance-Based Access
• Posture Policy Framework
• Posture-Driven Access Decisions
• Centralized Policy Management

Posture Testing and Monitoring
• Posture Testing and Enforcement
• Posture Sessions and Policy Outcomes
• Reports and Remediation Behavior
• Discovery 13: Configure Posturing and Reporting

Cisco TrustSec Overview (Optional)
• Introduction to Cisco TrustSec
• TrustSec Data Flow and Communication
• HTTPS Servers and REST APIs
• TrustSec Deployment and Planning

Cisco TrustSec in Cisco ISE (Optional)
• Initial TrustSec Setup and Components
• TrustSec Classification Configuration
• SGT Propagation with Cisco ISE Configuration
• TrustSec Policy Enforcement Configuration
• TrustSec Troubleshooting
• Discovery 14: Configure Cisco TrustSec

Cisco ISE Administration (Optional)
• ISE Backup and Recovery
• ISE Certificate Management
• ISE Health and Alarms
• ISE Upgrade Process
• ISE Patch Management
• ISE Log Management
• Encrypted Syslog with TLS 1.3
• Review: Configure Secure Syslog with TLS v1.3 and Install Cisco ISE Patch