CISC-22 - SISE - IMPLEMENTING AND CONFIGURING CISCO IDENTITY SERVICES ENGINE V5.0

Categoria: **Cisco**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	Cisco	Cisco Certified Instructor	Professionista IT	Cisco

OBIETTIVI

After completing this course, you should be able to:

- Describe how Cisco ISE fits into contemporary network security architectures and the main functions, design motivations, and common use cases
- Examine the functional roles of Cisco ISE node personas, supported deployment models, licensing considerations, and their implications for design planning and scalability decisions
- Implement the installation workflows, platform requirements, and initial setup steps for deploying Cisco ISE on supported virtual and hardware platforms
- Evaluate the principles, message flow, and authorization outcomes of 802.1X-based network access, and Cisco ISE’s contribution to the security of wired and wireless connections with identity-based controls
- Describe how MAB works, including its fallback behavior, flow sequence, and policy application within Cisco ISE, and how MAB provides access to non-802.1X-compatible devices
- Establish the role of NADs in Cisco ISE authentication workflows, and provide an outline of the steps required to add, configure, and validate NADs within Cisco ISE to ensure secure policy enforcement
- Discuss the role of internal and external identity sources in Cisco ISE, how user and device identities are managed, and how certificates are used for identity-based authentication
- Evaluate how to configure Cisco ISE to integrate with Active Directory and LDAP, and outline the key settings and connectivity requirements needed to support external user authentication
- Interpret how Cisco ISE selects identity sources during authentication and the logic and conditions that determine identity store sequences, fallback behavior, and identity normalization techniques
- Discuss the structure and purpose of policy sets in Cisco ISE, including how global and local constructs interact, how policy sets are matched and evaluated, and how authentication and authorization logic is organized within each policy set
- Identify how Cisco ISE evaluates authentication policies using rule conditions, identity store sequences, and dictionaries, as well as how behavior is applied when no rules match
- Interpret how Cisco ISE applies authorization policies following authentication, including how rules are constructed using Conditions Studio and matched against user and device attributes to apply appropriate access profiles
- Analyze Cisco ISE policies based on logs, RADIUS flow data, and session context to resolve authentication and authorization issues across different access scenarios
- Analyze how Cisco ISE provides web-based guest access using CWA, and distinguish between hotspot, self-registration, and sponsored access flows

- Establish global guest settings in Cisco ISE to define account lifecycle behavior, credential policies, communication methods, and access types for guests across supported onboarding processes
- Configure Cisco ISE guest portals to support different access flows, manage account lifecycles, and implement deployment models that are consistent with organizational policies and scalability requirements
- Set up sponsor-drive guest access in Cisco ISE via access roles, linking guest types to sponsor groups, and customizing portal behavior to support account creation and approval
- Establish a clear understanding of Cisco ISE’s roles in secure and scalable BYOD access: its enterprise use cases, deployment models, policy-based control strategies, key components, Cisco ISE-specific capabilities, and onboarding designs such as single and dual SSIDs for seamless personal device integration into the network
- Configure Cisco ISE to deliver supplicants, issue certificates, and enforce policies as part of a complete BYOD onboarding pipeline
- Operate post-onboarding workflows using the My Device Portal, including revocation of certificates and device de-registration for lost or stolen endpoints
- Explain how Cisco ISE uses profiling to identify endpoints by taking advantage of classification logic, profiler components, data flows, and feed services to provide the foundation for advanced profiling and policy enforcement
- Analyze how Cisco ISE collects endpoint data using built-in probes, device sensors, and pxGrid enrichment, and how each method contributes to the accuracy and coverage of profiling
- Analyze how the profiling policies in Cisco ISE classify endpoints based on collection attributes, and how logical profiles are created and applied to support the decision-making process for determining access based on identity
- Design scalable profiling solutions by aligning design principles, probe selection, and NAD integration with diverse network environments
- Maintain visibility of profiling through dashboards and reporting tools, and improve deployment efficiency through optimization techniques
- Apply foundational understanding of Cisco ISE posture services, including agent types, flow logic, operational modes, and use cases
- Implement Cisco ISE to deliver posture agents and related resources to endpoints by configuring update services, portals, and delivery policies
- Administer Cisco ISE policies to ensure secure and compliant network access
- Test compliance-based access enforcement by simulating a variety of endpoint scenarios using Cisco AnyConnect
- Assess session behavior, interpret posture outcomes, and analyze reporting tools to confirm the effectiveness of posture policy application and remediation
- Examine Cisco ISE’s use of TACACS+ for securing administrative access, including key AAA concepts and a comparison with RADIUS to illustrate centralized authentication and authorization
- Set up Cisco ISE for TACACS+ based device administration by configuring policy elements such as command sets, profiles, and policy sets
- Onboard network devices, define access permissions, and set up authentication and authorization rules to control administrator access
- Implement advanced TACACS+ authorization logic, implement administrator command access, and implement scalable deployments using proven design guidelines
- Compare Cisco’s TrustSec core architecture, operation, and design considerations, including its enhancements and planning prerequisites for enterprise deployment
- Configure Cisco TrustSec segmentation in Cisco ISE, including SGT classification, SXP propagation, and tag-based policy enforcement
- Interpret how to operationalize Cisco ISE through system maintenance, backup/restore procedures, certificate management, and structured upgrades in production environments

PREREQUISITI

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® Software Command-Line Interface (CLI) for wired and wireless devices
- -Familiarity with Cisco Secure Client
- -Familiarity with Microsoft Windows operating systems
- -Familiarity with 802.1X

Recommended prerequisites:

- -CCNA - Implementing and Administering Cisco Solutions
- -SCOR - Implementing and Operating Cisco Security Core Technologies

CONTENUTI

Course Outline

- -Cisco ISE Evolution, Foundation, and Role
- -Architecture and Design
- -Cisco ISE Installation and Initial Config
- -802.1X in Cisco ISE
- -MAB in Cisco ISE
- -Network Device Integration with Cisco ISE
- -Identity Sources and Authentication Types
- -Active Directory and LDAP Integration
- -Identity Selection and Resolution Logic
- -Cisco ISE Policy Framework
- -Authentication Policies
- -Authorization Policies
- -Troubleshoot Policies and Sessions
- -Guest Access Overview
- -Guest Access Policies and Settings
- -Guest Portals and Lifecycle Operations
- -Sponsor Portals
- -BYOD Architecture and Use Cases
- -BYOD Onboarding with Native Supplicant Provisioning
- -BYOD Lifecycle Operations
- -Profiling Architecture and Capabilities
- -Probes and Data Collection
- -Profile Policies and Authorization
- -Profile Monitoring and Design
- -Posture Service Flow and Agents
- -Posture Updates and Client Provisioning
- -Posture Policies and Compliance-Based Access
- -Posture Testing and Monitoring
- -AAA and TACACS+
- -TACACS+ Device Administration
- -TACACS+ Command Authorization

-Cisco TrustSec Overview
-Cisco TrustSec in Cisco ISE
-Cisco ISE Administration

Lab Outline

-Explore the Initial Cisco ISE Configuration, GUI and System Certificate
-Configure Network Device Groups and Network Devices
-Integrate Cisco ISE with Active Directory
-Configure MAB
-Configure Wired 802.1X
-Configure Wireless 802.1X and Optional Wired EAP-TLS and TEAP
-Troubleshoot Cisco ISE 8021.X Configuration Errors
-Configure Hotspot Guest Access
-Configure Sponsored Guest Access
-Configure BYOD
-Manage BYOD Devices
-Configure Profiling
-Configure Authorization Policy Rules and Run Profiler Reports
-Configure Posture Preparations and Client Provisioning
-Configure Posturing and Reporting
-Configure TACACS+ Basic Device Administration
-Configure TACACS+ Command Authorization
-Configure Cisco TrustSec
-Configure Secure Syslog with TLS v1.3 and Install Cisco ISE Patch

INFO

Esame: 300-715 - Implementing and Configuring Cisco Identity Services Engine
Materiale didattico: Materiale didattico ufficiale Cisco in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)