# SECURING CISCO WIRELESS ENTERPRISE NETWORKS (WISECURE)

## Temario

This course provides guidelines for implementing Wi-Fi security architectures through proper configuration of Cisco wireless components. Hands-on labs are used to reinforce concepts. Topics covered include deployment and key features of Cisco AireOS 8.0, Cisco Prime Infrastructure Release 2.2, and Cisco Identity Services Engine Release 1.3

## Pre-requisitos

**Attendees should meet the following pre-requisites:**

- **ICND1** - Interconnecting Cisco Networking Devices Part 1 (CCENT)
- **WIFUND** - Implementing Cisco Wireless Network Fundamentals

## Objetivos del curso

After attending this course you should be able to:

- Identify common security issues influencing modern Wi-Fi designs
- Define security approaches in a Wi-Fi design
- Describe how to design and deploy end point and client security
- Describe how to design and deploy Cisco Identity Services Engine (ISE) in Wi-Fi network
- Explain how to secure the Wi-Fi infrastructure
- Design and deploy Wi-Fi access control
- Describe management and monitoring capabilities in the Wi-Fi environment

## Dirigido a

Engineers involved in the deployment and maintenance of a wireless network

## Contenido

### Define Security Approaches in a Wi-Fi Design

- Defining Security Areas in the Wi-Fi Design
- Describing Security Approaches in Wi-Fi Designs

### Design and Deploy End Point and Client Security

- Defining Endpoint and Client Standards and Features

### Design and Deploy Cisco ISE and Management Platforms

- Cisco Network Security Architecture
- Profiles and Policies
- Guest Access
- Secure BYOD

**Secure Wi-Fi Infrastructure**

- Defining Endpoint and Client Standards and Features

**Design and Deploy Wi-Fi Access Control**

- Defining Wi-FI Access Control Standards and Features

**Design and Deploy Monitoring Capabilities**

- Defining Threat and Interference Mitigation Approaches in Wi-Fi

**Labs**

- Discovery Lab 1: Overview of Cisco ISE
- Discovery Lab 2: Implementing SNMP v3
- Discovery Lab 3: Configure and Verify Cisco MFP
- Discovery Lab 4: Rogue AP Monitoring and Rules
- Challenge Lab 1: Configure WPA2 Access
- Challenge Lab 2: Configure 802.1X Access
- Challenge Lab 3: Configure RADIUS Integration
- Challenge Lab 4: Configure a Basic Access Policy
- Challenge Lab 5: Configure a Contractor2 Authentication Policy
- Challenge Lab 6: Configure Hotspot Guest Access
- Challenge Lab 7: CWA and Self-Registered Guest Operations
- Challenge Lab 8: Configure Secure Administrative Access
- Challeneg Lab 9: Configure a Basic Authentication Policy for an AP
- Challenge Lab 10: Implement Profiling
- Challenge Lab 11: Profiling and Device Onboarding
- Challenge Lab 12: Cisco ISE Profiling Reports
- Challenge Lab 13: Guest Reports
- Challenge Lab 14: Live Logs and Client 360° View
- Challenge Lab 15: Security Report Operations
- Challenge Lab 16: Use System Security Verification Tools