Guest Wi-Fi Network Design and Security Training Course

8 – 12 March 2027
Madrid

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Guest Wi-Fi Network Design and Security Training Course

Ref: 1680_226344 **Date:** 8 – 12 March 2027 **Location:** Madrid **Fees:** 5700 Euro

Overview

Guest Wi-Fi Network Design and Security Training Course is a one-week professional course for wireless, infrastructure and security teams, who leave with a Guest Wi-Fi Design, Security and Acceptance Pack. The course connects user journeys, RF coverage and capacity, network segmentation, captive portals, access controls, privacy, monitoring and service acceptance. Participants turn business requirements into a separated, measurable guest service rather than an extension of the internal network. Agile Leaders Training Center develops practical guest Wi-Fi engineering capability.

Who Should Attend

- Teams responsible for wireless coverage, capacity and access-point planning
- Infrastructure specialists responsible for VLANs, addressing and Internet access
- Security teams responsible for segmentation, policy enforcement and monitoring
- Service teams responsible for guest onboarding and user support
- Facilities and technology managers responsible for public-facing connectivity

The course assumes participants can interpret basic IP networking and wireless measurements at work, and leaves out consumer router setup, enterprise certification preparation and vendor-specific configuration.

Departments and Industries

The course supports departments that provide controlled wireless Internet access to visitors, customers and temporary users.

- Information technology infrastructure and network operations
- Cybersecurity, risk and service assurance
- Hospitality, events and visitor services
- Healthcare, education and public facilities
- Retail, transport and commercial property operations

Learning Objectives

By the end of this course, participants will be able to:

- Analyze guest user journeys, demand and service constraints
- Apply RF coverage and capacity planning methods
- Build segmented guest SSID, VLAN and firewall designs
- Evaluate captive portal and onboarding controls
- Diagnose wireless, addressing and access problems
- Use monitoring evidence to validate service acceptance

Course Agenda

Day 1: Requirements and User Journey

- Guest Access Stakeholder and Service Requirement Matrix
- Visitor Device and Session Demand Profile
- Guest Connection and Captive Portal Journey Map
- Acceptable-Use and Privacy Notice Checklist
- Guest Wi-Fi Risk and Constraint Register

Day 2: RF Coverage and Capacity Planning

- Floor-Plan RF Survey and Measurement Route
- Coverage, Capacity and Airtime Demand Model
- Access-Point Placement and Cell Overlap Map
- Channel Assignment and Interference Review Method
- Signal, Noise and Throughput Acceptance Criteria

Day 3: Segmentation and Access Enforcement

- Guest SSID, VLAN and Subnet Architecture Diagram
- Client Isolation and East-West Traffic Control Policy
- DHCP, DNS and Address-Pool Capacity Plan
- Guest-to-Internal Firewall Rule Matrix
- Internet Rate Limit and Session Control Profile

Day 4: Captive Portal, Monitoring and Response

- RFC 8952 Captive Portal Component Map
- RFC 8908 API and RFC 8910 Provisioning Flow
- Voucher, Identity and Policy Acceptance Decision Tree
- Wireless Monitoring and Service Health Dashboard
- Guest Network Incident Triage and Escalation Plan

Day 5: Testing and Acceptance Practice

- Exercise: Validate RF Coverage and Capacity Evidence
- Exercise: Test VLAN Segmentation and Client Isolation
- Exercise: Trace Captive Portal and Addressing Failures
- Exercise: Evaluate Logs, Alerts and Privacy Controls
- Capstone: Guest Wi-Fi Design, Security and Acceptance Pack

Practical Exercises

Suggested activities use hotel, healthcare facility and event-venue guest access scenarios.

- Suggested activity: translate visitor demand into coverage, capacity and session requirements
- Suggested activity: design guest SSID, VLAN, addressing and firewall separation
- Suggested activity: trace a failed captive portal onboarding journey
- Suggested activity: reconcile monitoring results with acceptance criteria and corrective actions

FAQs

Who suits guest Wi-Fi network design training and what does it assume?

Guest Wi-Fi network design training suits wireless, infrastructure, security and visitor-service teams. It assumes basic IP networking and wireless measurement familiarity while excluding consumer setup and vendor certification preparation.

How does guest Wi-Fi security differ from employee Wi-Fi security?

Guest Wi-Fi security prioritizes separation from internal systems, controlled Internet access, client isolation, temporary onboarding, session policies and public-user privacy. Employee Wi-Fi commonly relies on managed identities, enterprise authentication and access to authorized business resources.

Why does a guest Wi-Fi network use VLAN segmentation?

Guest Wi-Fi VLAN segmentation creates a separate traffic boundary for visitor devices. Firewall policy can then restrict internal destinations, control Internet services and make monitoring and incident investigation more manageable.

What causes guest Wi-Fi captive portal failures?

Guest Wi-Fi captive portal failures can result from provisioning, DNS, DHCP, TLS, API reachability, enforcement policy, session state or device behavior. Diagnosis should trace the connection journey instead of treating every failure as weak radio coverage.

AGILE LEADERS
Training Center

Conclusion

Participants take back a Guest Wi-Fi Design, Security and Acceptance Pack containing requirements, RF plans, segmentation diagrams, firewall rules, onboarding decisions, monitoring measures and test evidence. The pack makes guest-access decisions traceable across design, deployment and operation. It also helps teams separate internal resources, diagnose user journeys and manage service exceptions consistently.