

Cisco 300-725 SWSA 2026: Securing Cisco Networks

Cisco 300-725 SWSA 2026. Secure Cisco wireless networks with WPA3, ISE, identity management, and guest access.

IT Certifications Instructor: Brian Mitchell • 5 sections • 41 lessons • 12.75h total

[View this course online](#) [Browse all courses](#)

About this course

This course helps you cover the key concepts for the Cisco 300-725 Securing Cisco Wireless Enterprise Networks (SWSA) exam, updated for the 2026 blueprint. We cut through the noise and focus on what you need to know to secure modern Cisco wireless infrastructures, from WPA3 concepts to monitoring and troubleshooting.

You will learn how to implement and verify wireless security solutions, including Identity Management, Guest Access, and Cisco Identity Services Engine (ISE) integration. The course features video guides, downloadable configuration checklists, and real case study analysis.

Course curriculum

Foundations of Wireless Security

- **Understanding WPA2 vs WPA3 Security (12m)**
We'll break down the key differences between WPA2 and WPA3, explaining why the upgrade is critical for modern network security.
- **Defining Authentication and Encryption Methods (18m)**
Learn the fundamentals of 802.1X, EAP, and how encryption protects your wireless data frames from eavesdropping.
- **Cisco Wireless Architecture Overview (15m)**
A step-by-step guide to the components of a Cisco unified wireless network and where security policies are enforced.
- **Introduction to RADIUS and AAA Protocols (22m)**
We'll show you how Authentication, Authorization, and Accounting (AAA) works and why RADIUS is the backbone of secure access.
- **Identifying Common Wireless Threats (9m)**
A practical look at rogue access points, Evil Twin attacks, and other threats you need to defend against.
- **Setting Up a Lab Environment (11m)**
A quick guide to setting up a virtual lab using Cisco Packet Tracer or a WLC emulator to practice the concepts.
- **Key Terminology for the 300-725 Exam (7m)**
A fast-paced review of the essential acronyms and terms you'll encounter on the exam, from FlexConnect to CCKM.

Identity Management and Guest Access

- **Configuring Local EAP on the WLC (25m)**
A hands-on walkthrough of setting up Local EAP for local user authentication when a RADIUS server isn't available.
- **Integrating Cisco ISE for Policy Enforcement (30m)**
Learn how to connect your Wireless LAN Controller to Cisco ISE to create dynamic, role-based access policies.
- **Designing a Secure Guest Access Portal (21m)**
We'll build a custom captive portal, covering web authentication and the different guest lifecycle policies.
- **Implementing Identity-Based Policy Enforcement (19m)**
A real case study analysis on how to apply different policies (e.g., bandwidth limits, ACLs) based on user identity.
- **Troubleshooting Common Authentication Failures (28m)**
A problem-solving session focused on debugging EAP failures, certificate issues, and RADIUS timeouts.

- **Configuring CCKM and OKC for Fast Roaming (14m)**
Learn how to configure Cisco Centralized Key Management to ensure seamless roaming for voice and video clients.
- **Using Certificates in a Wireless Environment (16m)**
We'll explain how to properly deploy and trust certificates on your WLC, ISE, and client devices.
- **Deploying Pre-Shared Keys (PSK) Securely (10m)**
A practical guide to using WPA2/WPA3 PSK and advanced features like PSK management and MAC filtering.
- **Configuring MFP (Management Frame Protection) (13m)**
Learn how to protect your network from management frame spoofing attacks with step-by-step MFP configuration.

Wireless Security and Monitoring

- **Implementing Rogue Access Point Detection (20m)**
A deep dive into configuring rogue detection, containment, and classification on your Cisco WLC.
- **Using Wireless Intrusion Prevention System (WIPS) (24m)**
We'll show you how to configure WIPS policies to detect and mitigate wireless attacks in real-time.
- **Monitoring Client and Endpoint Security (17m)**
Learn how to use Cisco Identity Services Engine (ISE) posture assessment to check endpoint security before granting access.
- **Configuring Advanced Logging on the WLC (22m)**
A step-by-step guide to enabling and interpreting critical security logs for troubleshooting and auditing.
- **Setting Up SNMP and Syslog for Security Monitoring (19m)**
We'll configure SNMP traps and Syslog servers to centralize your security event monitoring.
- **Analyzing CleanAir Reports for RF Security (15m)**
A real case study on using Cisco CleanAir to identify and mitigate RF jamming and interference devices.
- **Best Practices for WLC Hardening (12m)**
A checklist-driven lesson covering password policies, management interface restrictions, and disabling unused services.

Advanced Security Applications

- **Securing FlexConnect Deployments (26m)**
We'll cover the unique security challenges of branch deployments and how to configure local authentication and switching.
- **Implementing OfficeExtend Access Points (18m)**
Learn how to secure remote APs and the VPN connections used to link back to the corporate network.
- **Leveraging Cisco DNA Center for Policy (29m)**
A practical guide to using Cisco DNA Center to define and deploy network-wide security policies for wireless.

- **Configuring Device Insight and Analytics (23m)**
We'll show you how to use Cisco's analytics tools to fingerprint devices and apply micro-segmentation policies.
- **Integrating with Third-Party Security Systems (20m)**
A problem-solving session on integrating your Cisco wireless network with firewalls and other security appliances.
- **Automating Security Tasks with Python (32m)**
Learn basic Python scripts to automate common security tasks like pushing ACLs or checking rogue status.
- **Securing Mesh Networks (16m)**
A step-by-step guide to the security considerations and configurations for outdoor mesh access points.
- **Advanced Troubleshooting: Packet Captures (35m)**
We'll teach you how to capture and analyze wireless traffic on the WLC to diagnose complex security issues.
- **Configuring Identity Services Engine (ISE) Profiling (27m)**
A deep dive into ISE profiling policies to automatically identify and apply policies to unknown devices.

Implementation and Next Steps

- **Final Review: Key Exam Topics for 300-725 (25m)**
A comprehensive review of the most critical exam objectives, with a downloadable study checklist.
- **Deploying a New Wireless Security Policy: A Walkthrough (31m)**
We'll put it all together in a real-world project: designing and deploying a complete security policy from scratch.
- **Common Exam Pitfalls and How to Avoid Them (14m)**
An honest look at tricky exam questions and common mistakes students make, with tips to score higher.
- **Practice Exam Strategy and Time Management (11m)**
Learn how to approach the exam format, manage your time, and use practice tests effectively.
- **Lab Challenge: Secure a Multi-Site Branch (28m)**
A hands-on challenge where you apply everything you've learned to secure a simulated branch office network.
- **Post-Certification: Building Your Security Career (9m)**
We'll discuss next steps, including advanced certifications and how to leverage your new skills on the job.
- **Staying Current: Wireless Security Trends for 2026 (13m)**
A look ahead at emerging threats and technologies like WPA4, Zero Trust, and AI-driven security.
- **Downloadable Resources and Templates (5m)**
Access a library of downloadable resources, including configuration guides, checklists, and script templates.
- **Final Q&A and Course Wrap-Up (8m)**
A final review of your journey, answers to common questions, and encouragement for your exam day.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **[Flight Attendant Preparation: What to Study Before You Apply](#)**

[Visit the blog](#) [All courses](#) [This course](#)