



REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Implementing Advanced Cisco® Unified Wireless Security (IAUWS) v2.0

Duration: 5 Days

Method: Instructor-Led Training (ILT) | Live Online Training

Course Description

This course is designed to provide participants with the information necessary to secure their wireless network from security threats via appropriate security policies and best practices, as well as ensure the proper implementation of security standards and proper configuration of security components. The course reinforces the instruction by providing participants with hands-on labs to ensure they thoroughly understand how to secure a wireless network.

Target Audience

This course is intended for:

- Wireless Network Engineer
- Mid-Level Wireless Support Engineer
- Wireless Test Engineer
- Wireless Network Designer

Prerequisites

To attend this course, candidates must have:

- *Cisco Certified Networking Associate (CCNA)*

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Configure administration and security on a WLAN controller.
- Configure administration and security on a WLAN controller using TACACS+.
- Secure client devices using EAP authentication.
- Configure the Cisco Secure Services Client.
- Design and implement guest services on a WLAN controller.
- Configure the WLAN controller for Cisco NAC.



Course Objectives *Continued*

- Configure local authentication on the WLAN controller.
- Configure Management Frame Protection (MFP) on the WLAN controller.
- Implement Access Control Lists (ACL) on a WLAN controller.
- Use WLAN controller-based Intrusion Detection Signatures (IDS).
- Configure the WLAN controller to integrate with IPS and IDS appliances.

Course Topics

Module 1: Organizational and Regulatory Security Policies

- Regulatory Compliance
- Segmenting Traffic
- Configuring Administrative Security
- Managing WLAN Controller and Cisco WCS Alarms
- Security Audit Tools

Module 2: Secure Client Devices

- Configuring EAP Authentication
- Impact of Security on Application and Roaming
- Configuring Cisco Secure Services Client
- Troubleshooting Wireless Connectivity

Module 3: Design and Implement Guest Access Services

- Guest Access Architecture
- Configuring the WLAN to Support Guest Access
- Configuring Guest Access Accounts
- Troubleshooting Guest Access

Module 4: Design and Integrate Wireless Network with NAC

- Cisco NAC Appliance Solution
- Configuring the Controller for Cisco NAC Out-of-Band Operations

Module 5: Implement Secure Wireless Connectivity Services

- Configuring Authentication for the WLAN Infrastructure
- Configuring Management Frame Protection
- Configuring Certificate Services
- Implementing Access Control Lists
- Configuring Identity-Based Networking on the Controller Issues
- Troubleshooting Secure Wireless Connectivity

Module 6: Internal and Integrated External Security Mitigations

- Mitigating Wireless Vulnerabilities
- Using Controller-Based IDS
- Cisco's End-to-End Security Solutions
- Integrating Cisco WCS with Wireless IPS

LABS INCLUDED