

Implementing Advanced Cisco Unified Wireless Security (IAUWS)

Days: 5

Who should attend

- Wireless network engineers
- Wireless test engineers
- Wireless network administrators
- Wireless network managers
- Mid-level wireless support engineer
- Project managers
- Program managers
- Other – sales and marketing personnel

Certifications

This course is part of the following Certifications:

- [Cisco Certified Network Professional Wireless \(CCNP WIRELESS\)](#)

Prerequisites

The knowledge and skills that a learner must have before attending this course are as follows:

- [Interconnecting Cisco Networking Devices Part 1 \(ICND1\)](#)
- [Interconnecting Cisco Networking Devices Part 2 \(ICND2\)](#)
- [Implementing Cisco Unified Wireless Networking Essentials \(IUWNE\)](#)

Course Objectives

Implementing Advanced Cisco Unified Wireless Security (IAUWS) v1.0 is a five-day day instructor-led course, designed to help students prepare for the CCNP® wireless certification, a professional-level certification specializing in the wireless field. The goal of the course is to provide network professional with information to prepare them to secure the 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 IAUWS reinforces the instruction by providing students with hand-on labs to ensure students thoroughly understand how to secure a network.

Upon completing this course, the learner will be able to meet these overall objectives:

- Translate organisational and regulatory security policies and enforce security compliances
- Integrate security on client devices
- Design and implement guest access services on the WLAN controller
- Design and integrate a wireless network with Cisco NAC Appliance
- Implement secure wireless connectivity services on the WLAN controller

- Use the internal security features on the WLAN controller and integrate the WLAN controller with advanced security platforms to isolate and mitigate security threats to the WLAN

Course Content

Module 1: Organisational and Regulatory Security Policies

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

Module 2: Secure Client Devices

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

Module 3: Design and Implement Guest Access Services

- Describing Guest Access Architecture
- Configuring the WLAN to Support Guest Access
- Configuring Guest Access Accounts
- Troubleshooting Guest Access
 - Configure a Controller to use the Cisco NGS for Authentication
 - Troubleshooting Guest Access Issues

Module 4: Design and Integrate Wireless Network with Cisco NAC Appliance

- Introducing the Cisco NAC Appliance Solution
- Configuring the Controller for Cisco NAC Appliance for 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
- Troubleshooting Secure Wireless Connectivity

Module 6: Internal and Integrated External Security Mitigations

- Mitigating Wireless Vulnerabilities
 - Managing Rogue Access Points
 - Managing IDS Signatures
- Understanding Cisco's End-to-End Security Solutions
- Integrating Cisco WCS with Wireless IPS

