Learning@Cisco

Cisco Training on Demand

Securing Cisco Wireless Enterprise Networks (WISECURE) v1.1

Overview
Securing Cisco Wireless Enterprise Networks (WISECURE) version 1.1 is a Cisco® Training on Demand course. It is in the curriculum for the CCNP® Wireless certification. The course provides you with guidelines for implementing Wi-Fi security architectures through correct configuration of Cisco Wireless components.

Hands-on labs reinforce concepts that include deploying Cisco AireOS 8.0, Cisco Prime™ Infrastructure Release 2.2, and Cisco Identity Services Engine (ISR) Release 1.3 features.

Interested in purchasing this course in volume at discounts for your company? Contact ctod-sales@cisco.com.

Duration
The WISECURE v1.1 Training on Demand is a self-paced course based on the 5-day instructor-led training version. It consists of 10 sections of instructor video and text totaling more than 8 hours of instruction along with interactive activities, 7 hands-on lab exercises, content review questions, and challenge questions.

Target Audience
This course is designed for wireless network engineers and technicians, test engineers, network designers, administrators and managers, midlevel wireless support engineers, project managers, and those preparing for the associated 300-375 WISECURE exam.
Objectives
After completing this course, you should be able to:

- Define security approaches in a Wi-Fi design
- Describe how to design and deploy endpoint and client security
- Describe how to design and deploy ISE in a 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

Course Prerequisites
The knowledge and skills recommended before attending this course are:

- Cisco Prime Infrastructure
- Cisco Identity Services Engine (ISR)
- Metageek Chanelyzer software
- Voice signaling protocols
- Basic quality of service (QoS)
- Application visibility and control
- LAN switching

Course Outline
- Course Introduction
- Section 1: Defining Security Areas in the Wi-Fi Design
- Section 2: Describing Security Approaches in Wi-Fi Designs
- Section 3: Defining Endpoint and Client Standards and Features
- Section 4: Cisco Network Security Architecture
- Section 5: Profiles and Policies
- Section 6: Guest Access
- Section 7: Secure BYOD
- Section 8: Defining Endpoint and Client Standards and Features
- Section 9: Defining Wi-Fi Access Control Standards and Features
- Section 10: Defining Threat and Interference Mitigation Approaches in Wi-Fi

Labs Outline
This course contains seven hands-on lab exercises.
Figure 1. Topology for All Labs in Securing Cisco Wireless Enterprise Networks

The labs included in this course are:

- Discovery Lab 3.28: Configure Required Interfaces
- Discovery Lab 3.29: Configure WLANs
- Discovery Lab 3.30: Configure a Local Network User on the WLAN Controller
- Discovery Lab 3.31: Configure Local EAP on the Controller
- Discovery Lab 3.32: Configure the Employee WLAN for Local EAP on Both Controllers
- Discovery Lab 3.33: Configure the Windows Supplicant
- Discovery Lab 3.34: Configure NADs for Cisco ISE

Cisco Capital Financing Helps You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx), accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital financing is available in more than 100 countries. Learn more.