



Global Knowledge®

# WISECURE - SECURING CISCO WIRELESS ENTERPRISE NETWORKS V1.1

Course Code: 4391

Learn the guidelines for implementing Wi-Fi security architectures through proper configuration of Cisco wireless components. This course is required training to achieve CCNP Wireless certification.

In this course, you will learn how to secure Cisco wireless networks. The course provides guidelines for implementing Wi-Fi security architectures through proper configuration of Cisco wireless components, and also includes hands-on labs to reinforce concepts. You will learn about deploying Cisco AireOS 8.0, Cisco Prime Infrastructure Release 2.2, as well as Cisco Identity Services Engine Release 1.3 features.

Cisco CCNP Wireless certification addresses the need for designing, implementing, and operating Cisco Wireless networks and mobility infrastructures. CCNP Wireless certification emphasizes wireless networking principles and theory.

Note: For the classroom version of this course, laptops are provided to participate in the hands-on labs. If you are attending the virtual version or desire to use your own laptop, please bring a laptop computer with an Ethernet port as well as an internal wireless NIC, 802.11a/b/g/n. Access to the remote labs requires a browser that supports Java and permissions to open RDP or encrypted (RDP443) RDP sessions. If your browser does not support Java, you will need administrator rights to the laptop to install the software.

## What You'll Learn

- Security approaches in a Wi-Fi design
- Design and deploy end point and client security
- Design and deploy Cisco ISE in Wi-Fi network
- Secure the Wi-Fi infrastructure
- Design and deploy Wi-Fi access control
- Management and monitoring capabilities in the Wi-Fi environment

## Who Needs to Attend

- Wireless network engineers

## Prerequisites

- CCNA Routing and Switching certification

- CCNA Wireless certification



Global Knowledge®

# WISECURE - SECURING CISCO WIRELESS ENTERPRISE NETWORKS V1.1

Course Code: 4391

CLASSROOM LIVE

\$3,595 USD

5 days

## Classroom Live Outline

1. Define Security Approaches in a Wi-Fi Design
  - Security Areas in the Wi-Fi Design
  - Security Approaches in Wi-Fi Designs
2. Design and Deploy End Point and Client Security
  - Endpoint and Client Standards and Features
3. Design and Deploy Cisco ISE and Management Platforms
  - Cisco Network Security Architecture
  - Profiles and Policies
  - Guest Access
  - Secure BYOD
  - Discovery 1: Overview of Cisco ISE
4. Secure Wi-Fi Infrastructure
  - Endpoint and Client Standards and Features
  - Discovery 2: Implementing SNMP v3
  - Discovery 3: Configure and Verify Cisco MFP
  - Discovery 4: Rogue AP Monitoring and Rules
5. Design and Deploy Wi-Fi Access Control
  - Wi-Fi Access Control Standards and Features
6. Design and Deploy Monitoring Capabilities
  - Threat and Interference Mitigation Approaches in Wi-Fi

## Classroom Live Labs

Lab 1: Configure WPA2 Access  
Lab 2: Configure 802.1X Access  
Lab 3: Configure RADIUS Integration  
Lab 4: Configure a Basic Access Policy  
Lab 5: Configure a Contractor2 Authentication Policy  
Lab 6: Configure Hotspot Guest Access  
Lab 7: CWA and Self-Registered Guest Operations  
Lab 8: Configure Secure Administrative Access  
Lab 9: Configure a Basic Authentication Policy for an AP  
Lab 10: Implement Profiling  
Lab 11: Profiling and Device Onboarding  
Lab 12: Cisco ISE Profiling Reports  
Lab 13: Guest Reports  
Lab 14: Live Logs and Client 360° View  
Lab 15: Security Report Operations  
Lab 16: Use System Security Verification Tools

Oct 7 - 11, 2019 | 8:30 AM - 5:00 PM | ATLANTA, GA

Nov 11 - 15, 2019 | 8:30 AM - 4:30 PM | RICHARDSON, TX

Dec 9 - 13, 2019 | 8:30 AM - 5:00 PM | SAN ANTONIO, TX



Global Knowledge®

# WISECURE - SECURING CISCO WIRELESS ENTERPRISE NETWORKS V1.1

Course Code: 4391

VIRTUAL CLASSROOM LIVE

\$3,595 USD

5 days

## Virtual Classroom Live Outline

1. Define Security Approaches in a Wi-Fi Design
  - Security Areas in the Wi-Fi Design
  - Security Approaches in Wi-Fi Designs
2. Design and Deploy End Point and Client Security
  - Endpoint and Client Standards and Features
3. Design and Deploy Cisco ISE and Management Platforms
  - Cisco Network Security Architecture
  - Profiles and Policies
  - Guest Access
  - Secure BYOD
  - Discovery 1: Overview of Cisco ISE
4. Secure Wi-Fi Infrastructure
  - Endpoint and Client Standards and Features
  - Discovery 2: Implementing SNMP v3
  - Discovery 3: Configure and Verify Cisco MFP
  - Discovery 4: Rogue AP Monitoring and Rules
5. Design and Deploy Wi-Fi Access Control
  - Wi-Fi Access Control Standards and Features
6. Design and Deploy Monitoring Capabilities
  - Threat and Interference Mitigation Approaches in Wi-Fi

## Virtual Classroom Live Labs

Lab 1: Configure WPA2 Access  
Lab 2: Configure 802.1X Access  
Lab 3: Configure RADIUS Integration  
Lab 4: Configure a Basic Access Policy  
Lab 5: Configure a Contractor2 Authentication Policy  
Lab 6: Configure Hotspot Guest Access  
Lab 7: CWA and Self-Registered Guest Operations  
Lab 8: Configure Secure Administrative Access  
Lab 9: Configure a Basic Authentication Policy for an AP  
Lab 10: Implement Profiling  
Lab 11: Profiling and Device Onboarding  
Lab 12: Cisco ISE Profiling Reports  
Lab 13: Guest Reports  
Lab 14: Live Logs and Client 360° View  
Lab 15: Security Report Operations  
Lab 16: Use System Security Verification Tools

Oct 7 - 11, 2019 | 8:30 AM - 5:00 PM EST

Oct 14 - 18, 2019 | 9:30 AM - 6:00 PM EST

Nov 11 - 15, 2019 | 8:30 AM - 4:30 PM EST

Dec 9 - 13, 2019 | 9:30 AM - 6:00 PM EST



Global Knowledge®

# WISECURE - SECURING CISCO WIRELESS ENTERPRISE NETWORKS V1.1

Course Code: 4391

ON-DEMAND

\$750 USD

## On-Demand Outline

1. Define Security Approaches in a Wi-Fi Design
  - Security Areas in the Wi-Fi Design
  - Security Approaches in Wi-Fi Designs
2. Design and Deploy End Point and Client Security
  - Endpoint and Client Standards and Features
3. Design and Deploy Cisco ISE and Management Platforms
  - Cisco Network Security Architecture
  - Profiles and Policies
  - Guest Access
  - Secure BYOD
  - Discovery 1: Overview of Cisco ISE
4. Secure Wi-Fi Infrastructure
  - Endpoint and Client Standards and Features
  - Discovery 2: Implementing SNMP v3
  - Discovery 3: Configure and Verify Cisco MFP
  - Discovery 4: Rogue AP Monitoring and Rules
5. Design and Deploy Wi-Fi Access Control
  - Wi-Fi Access Control Standards and Features
6. Design and Deploy Monitoring Capabilities
  - Threat and Interference Mitigation Approaches in Wi-Fi

## On-Demand Labs

Lab 1: Configure WPA2 Access

Lab 2: Configure 802.1X Access  
Lab 3: Configure RADIUS Integration  
Lab 4: Configure a Basic Access Policy  
Lab 5: Configure a Contractor2 Authentication Policy  
Lab 6: Configure Hotspot Guest Access  
Lab 7: CWA and Self-Registered Guest Operations  
Lab 8: Configure Secure Administrative Access  
Lab 9: Configure a Basic Authentication Policy for an AP  
Lab 10: Implement Profiling  
Lab 11: Profiling and Device Onboarding  
Lab 12: Cisco ISE Profiling Reports  
Lab 13: Guest Reports  
Lab 14: Live Logs and Client 360° View  
Lab 15: Security Report Operations  
Lab 16: Use System Security Verification Tools





Global Knowledge.

# WISECURE - SECURING CISCO WIRELESS ENTERPRISE NETWORKS V1.1

Course Code: 4391

PRIVATE GROUP TRAINING

5 days

Visit us at [www.globalknowledge.com](http://www.globalknowledge.com) or call us at 1-866-716-6688.

Date created: 9/16/2019 12:34:47 PM

Copyright © 2019 Global Knowledge Training LLC. All Rights Reserved.