

|                         |          |  |  |
|-------------------------|----------|--|--|
| Cisco Standard Training | Security |  |  |
| Classroom Training      | 5 Days   |  |  |

## INTRODUCTION

Cisco Unified Communications support several features and mechanisms to secure voice signaling and communications and to mitigate attacks against Cisco Unified Communications networks. The *Implementing Cisco Unified Communications Security* (UCSEC) v1.0 course introduces security mechanisms and describes different implementation scenarios that increase the security level of Cisco Unified Communications networks. The course is designed to provide students with the necessary knowledge and skills to implement security features in a Cisco Unified Communications environment.

## OBJECTIVES

**After finishing this course, students will be able to:**

- Identify vulnerabilities in Cisco Unified Communications networks and describe security strategies, cryptographic services, PKI, and VPN technologies
- Implement network infrastructure security features
- Implement Cisco Unified Communications Manager and Cisco Unified Communications endpoint security features
- Implement network infrastructure security features

## TARGET AUDIENCE

This course is designed for experienced Cisco Unified Communications engineers who will be deploying or managing secure Cisco Unified Communications networks

## PREREQUISITES

**It is required that the participant has a good understanding of the following items:**

- Working knowledge of converged voice and data networks
- Working knowledge of Cisco IOS gateways, Cisco Unified SRST gateways, and Cisco Unified Border Element
- Working knowledge of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- CCNP® Voice certification is recommended

Additional knowledge and skills that will help the learner benefit fully from the course are as follows:

- Knowledge of network security fundamentals
- Knowledge of Cisco IOS Firewall and Cisco ASA adaptive security appliance firewalls
- Knowledge of IPsec and SSL VPNs
- CCNA® Security certification is recommended

## COURSE OUTLINE

- Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals
  - Assessing Vulnerabilities of Cisco Unified Communications Networks
    - Lab: Identifying Security Weaknesses in a Cisco Unified Communications Network
  - Describing Security Implementation Strategies
  - Describing Cryptographic Services and Functions
  - Describing Key Management and PKI
  - Describing IPsec and Cisco AnyConnect SSL VPN
- Network Infrastructure Security
  - Implementing Network Separation and Packet Filtering
    - Lab: Implementing Firewalls
  - Implementing Switch Security Features
    - Lab: Implementing 802.1X
  - Implementing Cisco AnyConnect SSL VPNs in Cisco Unified Communications Networks
    - Lab: Implementing Cisco AnyConnect SSL VPNs
- Cisco Unified Communications Manager and Endpoint Security Features
  - Hardening Cisco Unified Communications Endpoints
  - Implementing Toll-Fraud Prevention
  - Implementing Native Cisco Unified Communications Manager Security Features
  - Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens
    - Lab: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens
- Secure Cisco Unified Communications Integration and Features
  - Implementing SRTP to Gateways and Signaling Protection by IPsec
    - Lab: Implementing SRTP to Gateways and Signaling Protection by IPsec
  - Implementing Secure Signaling and SRTP in SRST and Cisco Unified Communications Manager Express
    - Lab: Implementing Secure SRST and Secure Cisco Unified Communications Manager Express
  - Implementing Trusted Relay Points
    - Lab: Implementing Trusted Relay Points
  - Implementing Proxies for Secure Signaling and SRTP
    - Lab: Implementing Proxies for Signaling and RTP