

IMPLEMENTING CISCO UNIFIED COMMUNICATIONS SECURITY

DURATION: **5 DAYS**

COURSE OVERVIEW

The Implementing Cisco Unified Communications Security (UCSEC) course is designed to provide students with the necessary knowledge and skills to implement security features in a Cisco Unified Communications environment. 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) course introduces security mechanisms and describes different implementation scenarios that increase the security level of Cisco Unified Communications networks

TARGET AUDIENCE

This course is designed for:

1. Network administrators and network engineers
2. System Engineers

COURSE OBJECTIVES

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

1. Identify vulnerabilities in Cisco Unified Communications networks and describe security strategies, cryptographic services, PKI, and VPN technologies
2. Implement network infrastructure security features
3. Implement Cisco Unified Communications Manager and Cisco Unified Communications endpoint security features
4. Implement network infrastructure security features

COURSE CONTENT

Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals

Assessing Vulnerabilities of Cisco Unified Communications Networks
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

Implementing Switch Security Features

Implementing Cisco AnyConnect SSL VPNs in Cisco Unified Communications Networks

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

Secure Cisco Unified Communications Integration and Features

Implementing SRTP to Gateways and Signaling Protection by Ipsec

Implementing Secure Signaling and SRTP in SRST and Cisco Unified Communications Manager Express

Implementing Trusted Relay Points

Implementing Proxies for Secure Signaling and SRTP

COURSE PREREQUISITES

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

1. Working knowledge of converged voice and data networks
2. Working knowledge of Cisco IOS gateways, Cisco Unified SRST gateways, and Cisco Unified Border Element
3. Working knowledge of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
4. CCNP Voice certification is recommended
5. To gain the prerequisite skills and knowledge, Cisco strongly recommends the knowledge of the following courses:
6. Implementing Cisco Voice Communications and QoS (CVOICE)

7. Implementing Cisco Unified Communications Manager Part 1 (CIPT1)
8. Implementing Cisco Unified Communications Manager Part2 (CIPT2)
9. Troubleshooting Cisco Unified Communications (TVOICE)