Preface

Implementing security mechanisms in the Cisco Unified Communications Manager system prevents identity theft of the phones and the Unified Communications Manager server, data tampering, and call-signaling/media-stream tampering.

The CiscoIP telephony network establishes and maintains authenticated communication streams, digitally signs files before transferring the file to the phone, and encrypts media streams and call signaling between Cisco Unified IP Phones.

About this Manual

The Security Guide includes the following Parts with short Descriptions:

Table 1: Parts and Descriptions

Part	Description
An Introduction to CUCM Security	Provides information on following topics about security overview. • System Requirements • Common Icons • Best Practices It also provides an overview to configure Security in your systems.

Part	Description
Basic System Security	Provides information on following topics to configure basic security in your systems. • Certificates • Security Modes • Cipher Management • Secure Tones and Icons • TFTP Encryption • Phone Security • Trunk and Gateway SIP Security • TLS Setup

User Security	Provides information on following topics to configure user security in your systems.
	• Identity Management
	  • User Access Control
	  • Credential Policies
	• Directory Access
	  • Contact Search Authentication Configuration
	  • Configure Secure Directory Server for Contact Search

Part	Description
Advanced System Security	Provides information on following topics to configure advanced system security in your systems. • FIPS Mode • Enhanced Security Mode • Common Criteria Mode • Cisco V.150 Minimum Essential Requirements • ECDSA and RSA • IPsec Policies • Authentication and Encryption Set up for CTI • JTAPI, and TAPI • Secure Call Monitoring and Recording • VPN Client
Appendix	Provides information on following topics to secure your systems. • Additional Security Configurations • Terms and Acronyms • Interactions and Restrictions • Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) • Troubleshooting Information • Remote Account • Log Details • Common Vulnerabilities and PSIRT • OS Hardening

Audience

The intended audiences for this guide are:

- System Administrators
- Phone Administrators

They configure call security features for Unified Communications Manager.

Document Conventions

This section provides information on the document conventions followed in the guide.

Notes use the following convention:

Note Means *reader take note* of the important or additional information.

Tips use the following convention:

Tip Means *the following are useful tips*.

Cautions use the following convention:

Caution Means that *the reader should be careful*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Attentions use the following convention:

Attention Means that *the reader should pay attention*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Warning

Warning Means that *the reader **must** follow instructions*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Legal Compliance

The Unified Communications Manager (Security) product contains cryptographic features and its import, export information. Transfer and use of information is subject to the laws governing United States and the local country. Delivery of Cisco cryptographic products doesn't imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with the U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you're unable to comply with the U.S. and local laws, return this product immediately.

Find further information regarding U.S. export regulations at http://www.access.gpo.gov/bis/ear/ear_data.html.