Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

The preface covers these topics:

Purpose

Cisco Unified Communications Manager Security Guide helps system and phone administrators perform the following tasks:

- Configure authentication.
- Configure encryption.
- Configure digest authentication.
- Install server authentication certificate that is associated with HTTPS
- Configure the Cisco CTL Client.
- Configure security profiles.
- Configure Certificate Authority Proxy Function (CAPF) to install, upgrade, or delete locally significant certificates on supported Cisco Unified IP Phone models.
- Configure phone hardening.
- Configure Survivable Remote Site Telephony (SRST) references for security.
- Configure gateways and trunks for security.

Audience

This guide provides a reference and procedural guide for system and phone administrators who plan to configure call security features for Cisco Unified Communications Manager.

Organization

Table 1 lists the major sections of this guide:

Table 1 Guide Overview

Chapter	Description
Security Basics	
Chapter 1, "Security Overview"	Provides an overview of security terminology, system requirements, interactions and restrictions, installation requirements, and a configuration checklist; describes the different types of authentication and encryption.
Chapter 2, "Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)"	Provides an overview of HTTPS and describes how to install the server authentication certificate in the trusted folder.
Chapter 3, "Security by Default"	Provides details of Security by Default, which provides automatic security features for Cisco Unified IP Phones.
Chapter 4, "Configuring the Cisco CTL Client"	Describes how to configure authentication by installing and configuring the Cisco CTL Client.
Chapter 5, "Certificate Configuration"	Provides details of certificate configuration.
Security for Phones and Voice Mail Ports	
Chapter 6, "Phone Security Overview"	Describes how Cisco Unified Communications Manager and the phone use security; provides a list of tasks that you perform to configure security for the phone.
Chapter 7, "Configuring a Phone Security Profile"	Describes how to configure the security profile and apply it to the phones in Cisco Unified Communications Manager Administration.
Chapter 8, "Configuring Secure and Nonsecure Indication Tones"	Describes how to configure a phone to play a secure-indication tone.
Chapter 9, "Configuring Encryption to Analog Endpoints"	Describes how to create a secure SCCP connection for analog phones to a Cisco VG2xx Gateway.
Chapter 10, "Using the Certificate Authority Proxy Function"	Provides an overview of Certificate Authority Proxy Function and describes how to install, upgrade, delete, or troubleshoot locally significant certificates on supported phones.

Table 1 Guide Overview (continued)

Chapter	Description
Chapter 11, "Configuring Encrypted Phone Configuration Files"	Describes how to configure encrypted phone configuration files in Cisco Unified Communications Manager Administration.
Chapter 12, "Configuring Digest Authentication for the SIP Phone"	Describes how to configure digest authentication on the phone that is running SIP in Cisco Unified Communications Manager Administration.
Chapter 13, "Phone Hardening"	Describes how to tighten the security on the phone by using Cisco Unified Communications Manager Administration.
Chapter 14, "Configuring Secure Conference Resources"	Describes how to configure media encryption for secure conferences.
Chapter 15, "Configuring Voice-Messaging Ports for Security"	Describes how to configure security for voice mail ports in Cisco Unified Communications Manager Administration.
Chapter 16, "Configuring Secure Call Monitoring and Recording"	Describes how to perform secure call monitoring and recording.
Security for CTI, JTAPI, and TAPI	
Chapter 17, "Configuring Virtual Private Networks"	Describes how to configure virtual private networks.
Chapter 18, "Configuring a VPN Gateway"	Describes how to configure a VPN gateway.
Chapter 19, "Configuring a VPN Group"	Describes how to configure a VPN group.
Chapter 20, "Configuring a VPN Profile"	Describes how to configure a VPN profile.
Chapter 21, "VPN Feature Configuration"	Describes how to configure a VPN features.
Chapter 22, "Configuring Authentication and Encryption for CTI, JTAPI, and TAPI"	Describes how to configure the Application User CAPF Profile and End User CAPF Profiles in Cisco Unified Communications Manager Administration.
Security for SRST References, Gateways, Trunks, and Cisco Unified Mobility Advantage Servers	
Chapter 23, "Configuring a Secure Survivable Remote Site Telephony (SRST) Reference"	Describes how to configure the SRST reference for security in Cisco Unified Communications Manager Administration.
Chapter 24, "Configuring Encryption for Gateways and Trunks"	Describes how Cisco Unified Communications Manager communicates with a secure gateway or trunk; describes IPSec recommendations and considerations.
Chapter 25, "Configuring the SIP Trunk Security Profile"	Describes how to configure and apply the SIP trunk security profile in Cisco Unified Communications Manager Administration.

Table 1 Guide Overview (continued)

Chapter	Description
Chapter 26, "Configuring Digest Authentication for the SIP Trunk"	Describes how to configure digest authentication for the SIP trunk in Cisco Unified Communications Manager Administration.
Chapter 27, "Configuring a Cisco Unified Mobility Advantage Server Security Profile"	Describes how to configure a Cisco Unified Mobility Advantage server security profile in Cisco Unified Communications Manager Administration.

Related Documentation

Each chapter contains a list of related documentation for the chapter topic.

Refer to the following documents for further information about related Cisco IP telephony applications and products:

- *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*
- Cisco Unified Survivable Remote Site Telephony (SRST) administration documentation that supports the SRST-enabled gateway
- The firmware release notes that support your phone model

Conventions

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following are useful tips.*

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.