Preface

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.
- Configure FIPS (Federal Information Processing Standard) 140-2 mode.

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

The following table lists the major sections of this guide:

Table 1: Guide Overview

Chapter	Description
Security Basics	
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.
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.
Default Security Setup	Provides information about the Security by Default feature, which provides automatic security features for Cisco Unified IP Phones.
Cisco CTL Client Setup	Describes how to configure authentication by installing and configuring the CiscoCTL Client.
TLS Setup	
Certificate Setup	Describes how to manage certificates in the Certificate Configuration window.
Security for Phones and Voice Mail Ports	
Phone Security	Describes how Unified Communications Manager and the phone use security; provides a list of tasks that you perform to configure security for the phone.
Phone Security Profile Setup	Describes how to configure the security profile and apply it to the phones in Unified Communications Manager.
Secure and Nonsecure indication Tone Setup	Describes how to configure a phone to play a secure-indication tone.
Encryption to Analog Endpoint Setup	Describes how to configure a secure SCCP connection to analog endpoints.
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.

Chapter	Description
Encrypted Phone Configuration File Setup	Describes how to configure encrypted phone configuration files in Unified Communications Manager.
Digest Authentication for SIP phones Setup	Describes how to configure digest authentication on the phone that is running SIP in Unified Communications Manager Administration.
Phone Hardening	Describes how to tighten the security on the phone by using Unified Communications Manager Administration.
Secure Conference Resources Setup	Describes how to configure media encryption for secure conferences.
Voice-Messaging Ports Security Setup	Describes how to configure security for voice mail ports in Unified Communications Manager Administration.
Secure Call Monitoring and Recording Setup	Describes how to configure secure call monitoring and recording.
Virtual Private Networks for CiscoIPPhones	
Security for CTI, JTAPI, and TAPI	
Authentication and Encryption Setup for CTI, JTAPI and TAPI	Describes how to configure the Application User CAPF Profile and End User CAPF Profiles in Unified Communications Manager.
Certificate Revocation/Expiry Status Verification	Describes how to configure the Online Certificate Status Protocol (OCSP) to monitor the status of existing certificates and to revoke expired certificates automatically.
Security for SRST References, Gateways, Trunks, and Cisco Unified Mobility Advantage Servers	
Secure Survivable Remote Site Telephony (SRST) Reference	Describes how to configure the SRST reference for security in Unified Communications Manager Administration.
Encryption Setup for Gateways and Trunks	Describes how Unified Communications Manager communicates with a secure gateway or trunk; describes IPSec recommendations and considerations.
SIP Trunk Security Profile Setup	Describes how to configure and apply the SIP trunk security profile in Unified Communications Manager Administration.
Digest Authentication setup for SIP Trunks	Describes how to configure digest authentication for the SIP trunk in Unified Communications Manager Administration.
Cisco Unified Mobility Advantage Server security Profile Setup	Describes how to configure a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration.
FIPS 140-2 Mode Setup	Describes how to configure FIPS (Federal Information Processing Standard) 140-2 mode in Unified Communications Manager Administration.

Chapter	Description
Cisco V.150 Minimum Essential Requirements (MER)	Describes how to configure the V.150 feature, which allows you to make secure calls in a modem over IP network.

Related Documentation

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

Refer to the following documents for further information about related CiscoIP 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
- *Cisco IP Phone Administration Guide* for 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.

Obtain Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Ciscodocuments, see the monthly *What'sNew in CiscoProduct Documentation*, which also lists all new and revised Ciscotechnical 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.