CHAPTER 4

Phone Security Overview

This chapter contains information on the following topics:

Understanding How Security Works for Phones

At installation, Cisco Unified Communications Manager boots up in nonsecure mode. When the phones boot up after the Cisco Unified Communications Manager installation, all devices register as nonsecure with Cisco Unified Communications Manager.

After you upgrade from Cisco Unified Communications Manager 4.0(1) or a later release, the phones boot up in the device security mode that you enabled prior to the upgrade; all devices register by using the chosen security mode.

The Cisco Unified Communications Manager installation creates a self-signed certificate on the Cisco Unified Communications Manager and TFTP server. You may also choose to use a third-party, CA-signed certificate for Cisco Unified Communications Manager instead of the self-signed certificate. After you configure authentication, Cisco Unified Communications Manager uses the certificate to authenticate with supported Cisco Unified IP Phones. After a certificate exists on the Cisco Unified Communications Manager and TFTP server, Cisco Unified Communications Manager does not reissue the certificates during each Cisco Unified Communications Manager upgrade. You must create a new CTL file with the new certificate entries.

Tip For information on unsupported or nonsecure scenarios, see the "Interactions and Restrictions" section on page 1-6.

Cisco Unified Communications Manager maintains the authentication and encryption status at the device level. If all devices that are involved in the call register as secure, the call status registers as secure. If one device registers as nonsecure, the call registers as nonsecure, even if the phone of the caller or recipient registers as secure.

Cisco Unified Communications Manager retains the authentication and encryption status of the device when a user uses Cisco Extension Mobility. Cisco Unified Communications Manager also retains the authentication and encryption status of the device when shared lines are configured.

Tip When you configure a shared line for an encrypted Cisco Unified IP Phone, configure all devices that share the lines for encryption; that is, ensure that you set the device security mode for all devices to encrypted by applying a security profile that supports encryption.

Supported Phone Models

For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports this Cisco Unified Communications Manager release or the firmware documentation that supports your firmware load.

Although you may be able to configure the security features in Cisco Unified Communications Manager Administration, the features may not work until you install a compatible firmware load on the Cisco TFTP server.

Viewing Security Settings on the Phone

You can configure and view certain security-related settings on phones that support security; for example, you can view whether a phone has a locally significant certificate or manufacture-installed certificate installed. For additional information on the security menu and icons, refer to the Cisco Unified IP Phone administration and user documentation that supports your phone model and this version of Cisco Unified Communications Manager.

When Cisco Unified Communications Manager classifies a call as authenticated or encrypted, an icon displays on the phone to indicate the call state. To determine when Cisco Unified Communications Manager classifies the call as authenticated or encrypted, refer to the "Security Icons" section on page 1-6 and the "Interactions and Restrictions" section on page 1-6.

Phone Security Configuration Checklist

Table 4-1 describes the tasks to configure security for supported phones.

Table 4-1 Phone Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	If you have not already done so, configure the Cisco CTL Client and ensure that the Cisco Unified Communications Manager security mode equals Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	If the phone does not contain a locally significant certificate (LSC) or manufacture-installed certificate (MIC), install a LSC by using the Certificate Authority Proxy Function (CAPF).	Using the Certificate Authority Proxy Function, page 7-1
Step 3	Configure phone security profiles.	Configuring a Phone Security Profile, page 5-1

Table 4-1 Phone Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Apply a phone security profile to the phone.	Applying a Phone Security Profile, page 5-9
Step 5	If a phone that is running SIP supports digest authentication, configure the digest credentials in the End User Configuration window.	• Configuring Digest Credentials in the End User Configuration Window, page 9-3 • End User Digest Credential Configuration Settings, page 9-3
Step 6	After you configure digest credentials, choose the Digest User from the Phone Configuration window.	Configuring the Digest User in the Phone Configuration Window, page 9-4
Step 7	On Cisco Unified IP Phone 7960G or 7940G (SIP only), enter the digest authentication username and password (digest credentials) that you configured in the End User Configuration window.	This document does not provide procedures on how to enter the digest authentication credentials on the phone. For information on how to perform this task, refer to the Cisco Unified IP Phone administration guide that supports your phone model and this version of Cisco Unified Communications Manager.
Step 8	Encrypt the phone configuration file, if the phone supports this functionality.	Configuring Encrypted Phone Configuration Files, page 8-1
Step 9	To harden the phone, disable phone settings.	Phone Hardening, page 10-1

Where to Find More Information

Related Topics

- Interactions and Restrictions, page 1-6
- Authentication, Integrity, and Authorization Overview, page 1-17
- Encryption Overview, page 1-21
- Configuration Checklist Overview, page 1-24
- Using the Certificate Authority Proxy Function, page 7-1
- Phone Security Configuration Checklist, page 4-2
- Configuring a Phone Security Profile, page 5-1
- Configuring Encrypted Phone Configuration Files, page 8-1
- Phone Hardening, page 10-1

Related Cisco Documentation

- *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*
- *Troubleshooting Guide for Cisco Unified Communications Manager*