Phone Security Overview

This chapter contains information on the following topics:

Understanding How Security Works for Phones

When you perform a new installation of Cisco Unified CallManager, the Cisco Unified CallManager cluster boots up in nonsecure mode; when the phones boot up after the Cisco Unified CallManager installation, all devices register as nonsecure with Cisco Unified CallManager.

After you upgrade from Cisco Unified CallManager 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 CallManager 5.0 installation creates a self-signed certificate on Cisco Unified CallManager and TFTP servers. You may also choose to use a third-party, CA-signed certificate for Cisco Unified CallManager instead of the self-signed certificate. After you configure the cluster for authentication, Cisco Unified CallManager uses the certificate to authenticate with supported Cisco Unified IP Phones. After a certificate exists on the Cisco Unified CallManager and TFTP servers, Cisco Unified CallManager does not reissue the certificates during each Cisco Unified CallManager 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 1-5.

Cisco Unified CallManager 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 CallManager retains the authentication and encryption status of the device when a user uses Cisco Extension Mobility. Cisco Unified CallManager 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

This security document does not list the security features that are supported on your Cisco Unified IP Phone. For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports Cisco Unified CallManager 5.0(4) or the firmware documentation that supports your firmware load.

Although you may be able to configure the security features in Cisco Unified CallManager 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 CallManager.

When Cisco Unified CallManager classifies a call as authenticated or encrypted, an icon displays on the phone to indicate the call state. To determine when Cisco Unified CallManager classifies the call as authenticated or encrypted, refer to the "Interactions and Restrictions" section on page 1-5.

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 cluster 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 6-1
Step 3	Configure phone security profiles.	Configuring a Phone Security Profile, page 5-1
Step 4	Apply a phone security profile to the phone.	Applying a Phone Security Profile, page 5-9

Table 4-1 Phone Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	If a SIP phone supports digest authentication, configure the digest credentials in the End User window in Cisco Unified CallManager Administration.	• Configuring Digest Credentials in the End User Configuration Window, page 8-3 • End User Digest Credential Configuration Settings, page 8-3
Step 6	After you configure digest credentials, choose the Digest User from the Phone Configuration window in Cisco Unified CallManager Administration.	Configuring the Digest User in the Phone Configuration Window, page 8-4
Step 7	On Cisco Unified SIP IP Phone 7960 or 7940, enter the digest authentication username and password (digest credentials) that you configured in the End User Configuration window.	The *Cisco Unified CallManager Security Guide* 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 CallManager.
Step 8	Encrypt the phone configuration file, if the phone supports this functionality.	Configuring Encrypted Phone Configuration Files, page 7-1
Step 9	To harden the phone, disable phone settings in Cisco Unified CallManager Administration.	Phone Hardening, page 9-1

Where to Find More Information

Related Topics

- Interactions and Restrictions, page 1-5
- Authentication, Integrity, and Authorization Overview, page 1-14
- Encryption Overview, page 1-18
- Configuration Checklist Overview, page 1-20
- Using the Certificate Authority Proxy Function, page 6-1
- Phone Security Configuration Checklist, page 4-2
- Configuring a Phone Security Profile, page 5-1
- Configuring Encrypted Phone Configuration Files, page 7-1
- Phone Hardening, page 9-1

Related Cisco Documentation

- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
- *Cisco Unified CallManager Troubleshooting Guide*