CHAPTER 9

Configuring Encryption to Analog Endpoints

This feature enables you to create a secure SCCP connection for analog phones to a Cisco VG2xx Gateway. The gateway uses Transport Layer Security (TLS) with Cisco Unified Communications Manager for SCCP signaling communication and uses SRTP for voice communication. The existing Cisco Unified Communications Manager TLS functionality, including certificate management, is used for secure SCCP communication.

This chapter contains the following sections:

Phone Security Profile

To establish an encrypted connection to analog phones, you must create a Phone Security Profile for analog phones with the Device Security Mode parameter set to **Authenticated** or **Encrypted**. To create a Phone Security Profile, navigate to **System > Security Profile > Phone Security Profile** in Cisco Unified Communications Manager Administration.

For more information about creating a Phone Security Profile, see Chapter 7, "Configuring a Phone Security Profile" in the *Cisco Unified Communications Manager Security Guide*.

When you configure an analog phone attached to a Cisco VG2xx gateway, choose the secure analog profile you created for the **Device Security Profile** parameter. To configure the Device Security Profile parameter, navigate to **Device > Phone** in Cisco Unified Communications Manager Administration and scroll down to the Protocol Specific Information section for the phone you want to configure.

Certificate Management

For secure analog phones to function, you must import the same CA-signed certificate into Cisco Unified Communications Manager that is being used by the Cisco VG2xx Gateway. For more information about importing certificates, see Chapter 6, "Security," in the *Cisco Unified Communications Operating System Administration Guide*.