Encryption to Analog Endpoint Setup

This chapter provides information about encryption to analog endpoint setup. 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 Unified Communications Manager for SCCP signaling communication and uses SRTP for voice communication. The existing Unified Communications Manager TLS functionality, including certificate management, is used for secure SCCP communication.

Analog 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 Unified Communications Manager Administration.

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 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

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 *Administration Guide for Cisco Unified Communications Manager* .