



CHAPTER 6

Configuring Secure-Indication Tone

The secure-indication tone is a special tone that gets played on both ends of a call that is established through devices configured as “protected” and when encrypted media is established. The tone denotes that the call is protected and that confidential information may be exchanged. The tone lasts for two seconds and begins to play as soon as the called party answers.

A “protected” device in Cisco Unified Communications Manager is designated by configuration. You can configure only certain Cisco Unified IP Phones and MGCP E1 PRI gateways as protected devices in Cisco Unified Communications Manager.

Therefore, you can make the following two types of calls that can use the secure-indication tone feature:

- Intracluster IP-to-IP calls
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

Intercluster protected calls are not supported. For the list of Cisco Unified IP Phone models and gateways that can be configured as protected devices, see the [“Supported Devices” section on page 6-2](#).

This chapter contains information on the following topics:

- [Supported Devices, page 6-2](#)
- [Important Information About Secure-Indication Tone, page 6-2](#)
- [Configuration Requirements, page 6-3](#)

Supported Devices

You can configure the following devices as protected devices in Cisco Unified Communications Manager (and can therefore use the secure-indication tone if all other configuration requirements are met):

- 7906G
- 7911G
- 7931G
- 7941G/7941G-GE
- 7942G
- 7945G
- 7961G/7961G-GE
- 7962G
- 7965G
- 7970G
- 7971G-GE
- 7975G
- Cisco ISR 28xx and 38xx MGCP E1 PRI Gateways

Important Information About Secure-Indication Tone

This section provides information that pertains to the impact of using the secure-indication tone feature:

- Facts about protected devices:
 - You can configure phones that are running SCCP or SIP as protected devices.
 - Protected devices can call non-protected devices that are either encrypted or non-encrypted. In this case, the call will be non-protected and the secure-indication tone will not play.
 - If a protected phone calls another protected phone, but the media is not encrypted, the call will get dropped.
- The secure-indication tone is not supported for video calls.
- A lock icon that displays on a Cisco Unified IP Phone indicates that the media is encrypted, but does not necessarily mean that the phone has been configured as a protected device. However, the lock icon must be present for a protected call to occur.
- The following services and features are impacted:
 - Multi-line supplementary services such as call transfer, conference, and call waiting are disabled on protected phones.
 - Cisco Extension Mobility and Join Across Line services are disabled on protected phones.
 - Shared-line configuration is not available on protected phones.
 - Hold/Resume and Call Forward All are supported for protected calls.

- Facts about MGCP E1 PRI gateways:
 - You must configure the MGCP gateway for SRTP encryption. Configure “mgcp package-capability srtp-package.”
 - The MGCP gateway must have an Advanced IP Services or Advanced Enterprise Services image (for example, c3745-adventerprisek9-mz.124-6.T.bin).
 - Protected status gets exchanged with the MGCP E1 PRI gateway by using proprietary FacilityIE in the MGCP PRI Setup, Alert, and Connect messages.
 - Cisco Unified Communications Manager plays the secure-indication tone only to the Cisco Unified IP Phone. A PBX in the network plays the tone to the gateway end of the call.
 - If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway is not encrypted, the call gets dropped.

**Note**

For more information about encryption for MGCP gateways, refer to the *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*, located at the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtsecure.html#wp1043332

Configuration Requirements

You must configure the following items for the secure tone to play:

- On the Phone Configuration window, which you can navigate to by choosing **Device > Phone** in Cisco Unified Communications Manager Administration, configure the following items:
 - From the Softkey Template drop-down list in the Device Information portion of the window, choose "Standard Protected Phone."

**Note**

You must use a new softkey template without supplementary service softkeys for a protected phone.

- For the Join Across Lines option (also in the Device Information portion of the window), choose "Off."
- Check the Protected Device check box (also in the Device Information portion of the window).
- From the Device Security Profile drop-down list (in the Protocol Specific Information portion of the window), choose a secure phone profile that is already configured in the Phone Security Profile window (**System > Security Profile > Phone Security Profile**).
- Go to the Directory Number Configuration window that appears when you add a directory number from the Phone Configuration window. In the area of the Directory Configuration window that is called “Multiple Call/Call Waiting Settings on Device *DeviceName*,” set the following two options to a value of 1:
 - Maximum Number of Calls
 - Busy Trigger

- Choose **System > Service Parameters** in Cisco Unified Communications Manager Administration, select your server, and select the Cisco CallManager service. On the Service Parameter Configuration window, in the Feature - Secure Tone area, set the “Play Secure Indication Tone” option to True (it is False by default).
- If you are configuring a protected MGCP E1 PRI gateway, choose **Device > Gateway > Add New** in Cisco Unified Communications Manager Administration and select one of the supported gateways listed in the [“Supported Devices” section on page 6-2](#). Select MGCP as the protocol. When the Gateway Configuration window appears, be sure to include the following configuration choices:
 - Set “Global ISDN Switch Type” to Euro.
 - After you complete the rest of the MGCP Gateway configuration, click **Save**, then select the endpoint icon that appears to the right of subunit 0 in the window. The Enable Protected Facility IE check box displays. Check this check box.

This allows the passing of “protected” status between Cisco Unified IP Phone endpoints and the protected PBX phones that are connected to the MGCP gateway.