Secure and Nonsecure Indication Tone Setup

This chapter provides information about secure and nonsecure indication tone setup. The system plays secure and nonsecure indication tones on a protected phone to indicate whether a call is encrypted.

Secure and Non-Secure Indication Tone Overview

The Secure Tone feature can configure a phone to play a secure indication tone when a call is encrypted. The tone indicates that the call is protected and that confidential information may be exchanged. The 2-second tone comprises three long beeps. If the call is protected, the tone begins to play on a protected phone as soon as the called party answers.

When the call is not protected, the system plays a non-secure indication tone, which comprises six short beeps, on a protected phone. For video calls, you might first hear secure indication tone for the audio portion of the call and then non-secure indication tone for overall non-secure media.

The secure and non-secure indication tones are supported on the following types of calls:

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

Note Only callers on protected phones can hear secure and non-secure indication tones. Callers on phones that are not protected never hear these tones. For video calls, the system plays secure and non-secure indication tones on protected devices.

Protected Devices

Configuration designates a protected device in Unified Communications Manager. You can configure only supported Cisco Unified IP Phones and MGCP E1 PRI gateways as protected devices in Unified Communications Manager.

Unified Communications Manager can also direct an MGCP IOS gateway to play secure and nonsecure indication tones when the system determines the protected status of a call.

You can make the following types of calls that can use the secure and nonsecure indication tones:

- Intracluster IP-to-IP calls
- Intercluster calls that the system determines are protected
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

Supported Devices

You can use Cisco Unified Reporting to determine which Cisco IP Phone models support secure and nonsecure indication tones. From Cisco Unified Reporting, click **Unified CM Phone Feature List**. For the Feature pull-down menu, choose **Secure Tone**. The system displays a list of products that support the feature.

For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

Secure and Non-Secure Indication Tone Tips

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

- Following are the facts about protected devices:
  - You can configure phones that are running SCCP or SIP as protected devices.
  - Protected devices that call non-protected devices that are encrypted play the secure tone, while protected devices that call non-protected and non-encrypted devices play a non-secure tone.
  - When a protected phone calls another protected phone, and the media is not encrypted, the call does not drop. The system plays non-secure indication tone to the phones on the call.
- For video calls, the system plays secure and non-secure indication tones on protected devices.

Note For video calls, the user may first hear secure indication tone for the audio portion of the call and then non-secure indication tone for overall non-secure media.

- A lock icon that displays on a Cisco 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:
  - Multiline supplementary services (such as call transfer, conference, and call waiting) are supported on protected phones. When the user invokes a supplementary service on a protected phone, the system plays secure or non-secure indication tone to reflect the updated status of the call.
  - 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.

- Following are the facts about MGCP E1 PRI gateways:
  - You must configure the MGCP gateway for SRTP encryption. Configure the gateway using the following command: **mgcppackage-capabilitysrtp-package**.
  - The MGCP gateway must specify 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.
  - Unified Communications Managerkey 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 drops.

Note For more information about encryption for MGCP gateways, refer to *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software that you are using.

Secure and Non-Secure Indication Tone Configuration Tasks

Make sure that you configure the following items for the secure tone to play:

- In the **Phone Configuration** window, which you can navigate to by choosing **Device** > **Phone** in 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 Configuration** window (**System** > **Security Profile** > **Phone Security Profile**).

- Go to the **Directory Number Configuration** window that displays when you add a directory number from the **Phone Configuration** window. In the **Multiple Call/Call Waiting Settings on Device**

DeviceName area of the **Directory Number Configuration** window, set the following options to a value of 1:

- Maximum Number of Calls
- Busy Trigger

- In Unified Communications Manager Administration, choose **System** > **Service Parameters**. In the first **Service Parameter Configuration** window, choose your server and choose the Cisco CallManager service. In the second **Service Parameter Configuration** window, locate the **Clusterwide Parameters (Feature - Secure Tone)** area, and set the **Play Secure Indication Tone** option to **True**. (The default value specifies False.)
- If you are configuring a protected MGCP E1 PRI gateway, choose **Device** > **Gateway** > **Add New** in Unified Communications Manager Administration and choose a supported gateway. Choose **MCGP** as the protocol. When the **Gateway Configuration** window displays, specify the following configuration choices:
  - Set **Global ISDN Switch Type** to **Euro**.
  - After you complete the rest of the MGCP Gateway configuration, click **Save**; then, click 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 configuration allows the system to pass protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that connect to the MGCP gateway.