Secure Tone

Secure 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 nonsecure indication tone, which comprises six short beeps, on a protected phone.

Note Only callers on protected phones can hear secure and nonsecure indication tones. Callers on phones that are not protected cannot hear these tones.

The secure and nonsecure 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

For video calls, the system plays secure and nonsecure 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 nonsecure indication tone for overall nonsecure media.

A lock icon that is displayed on a Cisco Unified IP Phone indicates that the media are encrypted, but does not indicate that the phone has been configured as a protected device. However, the lock icon must be present for a protected call to occur.

Protected Device Gateways

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

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

Protected devices provide these functions:

- You can configure phones that are running SCCP or SIP as protected devices.
- Protected devices can call nonprotected devices that are either encrypted or nonencrypted. In such cases, the call specifies nonprotected and the system plays nonsecure indication tone to the phones on the call.
- When a protected phone calls another protected phone, but the media is not encrypted, the system plays a nonsecure indication tone to the phones on the call.

Secure Tone Prerequisites

- You must configure the MGCP gateway for SRTP encryption. Configure the gateway with this command: **mgcp package-capability srtp-package**.
- The MGCP gateway must specify an Advanced IP Services or Advanced Enterprise Services image (for example, c3745-adventerprisek9-mz.124-6.T.bin).

Secure Tone Configuration Task Flow

Before you begin

- Review Secure Tone Prerequisites, on page 2

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List	Generate a report to identify devices that support the Secure Tone feature.
Step 2	Configure Phone As a Protected Device, on page 3	Configure the phone as a protected device.
Step 3	Configure Directory Number for Secure Tones, on page 3	Configure multiple calls and call waiting settings for the protected device.
Step 4	Configure Secure Tone Service Parameters, on page 4	Configure service parameters.
Step 5	(Optional) Configure MGCP E1 PRI Gateway, on page 4	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.

Configure Phone As a Protected Device

Before you begin

Generate a Phone Feature List

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click the phone for which you want to set secure tone parameters.
The **Phone Configuration** window is displayed.

Step 3 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.

Step 4 Set the **Join Across Lines** option to Off.

Step 5 Check the **Protected Device** check box.

Step 6 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**.

Step 7 Click **Save**.

What to do next

Perform one of the following procedures:

- Configure Directory Number for Secure Tones, on page 3
- Configure MGCP E1 PRI Gateway, on page 4

Configure Directory Number for Secure Tones

Before you begin

Configure Phone As a Protected Device, on page 3

Procedure

Step 1 Locate the **Association** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window is displayed.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 In the **Multiple Call/Call Waiting Settings on Device [device name]** area of the **Directory Number Configuration** window, set the **Maximum Number of Calls** and **Busy Trigger** options to 1.

Step 5 Configure the remaining fields in the **Directory Number Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Configure Secure Tone Service Parameters

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose a server.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager** .

Step 4 In the **Clusterwide Parameters (Feature - Secure Tone)** area, set the **Play Tone to Indicate Secure/Non-Secure Call Status** option to True.

Step 5 Click **Save**.

Configure MGCP E1 PRI Gateway

If you want the system to pass the protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that connect to the MGCP gateway, follow these steps:

Before you begin

Configure Phone As a Protected Device, on page 3

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Gateway**.

Step 2 Specify the appropriate search criteria and click **Find**.

Step 3 Choose a MGCP gateway.
The **Gateway Configuration** window appears.

Step 4 Set **Global ISDN Switch Type** to Euro.

Step 5 Configure the fields in the **Gateway Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 Click the **Endpoint** icon that appears to the right of subunit 0 in the window. The **Enable Protected Facility IE** check box appears. Check this check box.

Secure Tone Interactions and Restrictions

Secure Tone Interactions

Feature	Interaction
Call Transfer, Conference, and Call Waiting	When the user invokes these features on a protected phone, the system plays a secure or nonsecure indication tone to indicate the updated status of the call.
Hold/Resume and Call Forward All	These features are supported on protected calls.

Secure Tone Restrictions

Restriction	Description
Cisco Extension Mobility and Join Across Line services	Cisco Extension Mobility and Join Across Line services are disabled on protected phones.
Shared-line configuration	Shared-line configuration is not available on protected phones.
Non-encrypted media	If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway are not encrypted, the call drops.