



Secure Tones and Icons

- [Secure Tones and Icons Overview](#), on page 1
- [Secure Icons and Tones Tips](#), on page 3
- [Secure Icons and Tones Configuration Tasks](#), on page 5
- [Secure Calls and Tones Limitations and Restrictions](#), on page 7

Secure Tones and Icons Overview

Secure Icons and Secure Tone provide audio and visual indicators that alert you as to the security status of a call. Both of these features alert call participants of the security level of a call, so that participants know whether it's safe to exchange confidential information.


- **Secure Icons**—Refers to an icon that displays on the phone to indicate the level of security for a call.
- **Secure Tones**—Refers to a 2-second tone that plays at the start of a call to indicate whether the call is secure or non-secure.


Secure Icons

Security icons provide a visual indicator that appears on the phone display, letting you know whether a call is secure or nonsecure. The icon appears on the phone right next to the call duration timer.

The following table displays the security icons along with a description of its meaning:

Table 1: Secure Icons

Security Icon	Security Level	Description
Lock 	Encrypted Call	Both call signaling (with TLS) and call media (with SRTP) are encrypted. Note It's always required that the audio stream be encrypted in order for the Encryption icon to display on the phone. Encryption for additional media streams (video, BFCP and iX channel) may be required depending on how you configure the Call Secure Status Policy parameter. The default value is that the media is considered encrypted so long as the audio and video streams are both encrypted.

Security Icon	Security Level	Description
Shield 	Authenticated call	Call signaling is encrypted with TLS, call media is either unencrypted or partially encrypted. For example, the audio is encrypted, but not video. However, the Call Secure Status Policy indicates both must be encrypted for the call to have an Encrypted status.
No icon	Non secure call	Unauthenticated device with non secure audio and video

Additional Information

- Some phone models display only the lock icon (encrypted) and do not display the shield icon (authenticated)
- The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signal toning support notification of call security status changes to participating endpoints.
- For conference and barge calls, the security icon displays the security status of the conference.

Secure Tones Overview

Secure Tones can be configured to play on a Protected Phone at the start of a call. The tone alerts you to whether the other device in the call is secure or non secure—if the other device is non secure, you hear the nonsecure tone, if the other device is secure, you hear the secure tone.

Unlike Secure Icons, which display on all phones, Secure Tones play only on phones that are configured as a Protected Device. If both phones in a call are secured, but only one phone is Protected, only the Protected Phone hears the tone.

The following table lists the type of tone and what each means:

Table 2: Secure Tones

Secure Tones	Description
Three long beeps	Secure call. Other phone is a secure phone.
Six short beeps	Non secure call. Other phone is non secure.

Midcall Changes

If the security status of the call changes during the call, a new secure or nonsecure tone plays midcall in order to alert the caller on a Protected Device of the new security status. Only a user who is on a Protected Device hears the tone:

Types of Calls

Secure tone works for the following types of calls:

- Intracluster calls (IP to IP)
- Intercluster calls that are deemed protected

- IP to TDM calls over an MGCP gateway E1 connection (the MGCP gateway must be a protected device)

Secure Phone Call Identification

You can establish and identify a secure call when your phone and the phone on the other end is configured for secure calling. Conference calls support secure calls after secure conference bridge is set.

A secured call is established when you initiate a call from a secured phone (secured mode). A secure icon appears on the phone screen and indicates that the phone is configured for secure calls, but does not mean that the other phone connected is also secured.

You will hear a security tone if the call connects to another secured phone, indicating that both ends of the conversation are encrypted and secured.





Note If the call connects to a non secure phone, you will not hear the security tone.

Secure Icons and Tones Tips

Secure calling is supported between two phones. For protected phones, features such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured. Only callers on protected phones can hear secure and non secure indication tones. Callers on non protected phones don't hear these tones. For video calls, the system plays secure and non secure indication tones on protected devices.

All phones that support security icons display call security level.

- The phone displays a shield icon  for calls with a signaling security level of authentication. A shield icon identifies a secured connection between Cisco IP devices. This icon indicates that the devices use encrypted signaling.
- The phone displays a lock icon  for calls with encrypted media. This icon indicates that the devices use encrypted signaling and encrypted media.
- Some phone models display only the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints.

The protected phones only play the secure or nonsecure indication tones. The non protected phones never play indication tones. If the overall call status changes during the call, the indication tone changes and the protected phone play the appropriate tone.

Below are few scenarios when a protected phone plays an appropriate tone:

- If you enable the **Play Secure Indication Tone** option.
- When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone—three long beeps with pauses.
- When end-to-end non-secure media is established and the call status is non secure, the phone plays the non secure indication tone—six short beeps with brief pauses.

- If you disable the **Play Secure Indication Tone** option, the tones are not played.

Supported Devices Secure Tones

Use this procedure to obtain a list of phones that support secure tones.

Procedure

- Step 1** From Cisco Unified Reporting, click **System Reports**.
 - Step 2** Click **Unified CM Phone Features List**.
 - Step 3** Click **Generate a New Report**.
 - Step 4** From the **Features** drop-down list, choose **Secure Tone**.
 - Step 5** Click **Submit**.
-

For more information about using Cisco Unified Reporting, see [Administration Guide for Cisco Unified Communications Manager](#).

Protected Devices Secure Tones

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 non secure indication tones when the system determines the protected status of a call.

You can make the following types of calls that use secure and non secure 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

For video calls, the system plays secure and nonsecure indication tones on protected devices.

The protected devices provide the following functions:

- 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 such cases, the call specifies non protected and the system plays non secure indication tone to the phones on the call.
- When a protected phone calls another protected phone, and the media is not encrypted, the system plays a nonsecure indication tone to the phones on the call.

To set a phone to protected state, check the **Protected Device** check box in the **Phone Configuration** window of the **Cisco Unified CM Administration** page.

Secure Icons and Tones Configuration Tasks

You can configure secure icons and secure tones using the following tasks:

Procedure

	Command or Action	Purpose
Step 1	Set Up Secure Icon Policy	Call Secure Status Policy outlines which media streams within a call must be encrypted for the Secure Icon feature to display the call as Encrypted. The default is that audio and video (for video calls) must both be encrypted. You can reconfigure the setting to consider BFCP and iX Channel as well.
Step 2	Enable Secure Indication Tone for Cluster	Enable the secure indication tone on a protected phone.
Step 3	Configure Phone As a Protected Device	Configure supported Cisco Unified IP Phones as protected devices in Unified Communications Manager.

Set Up Secure Icon Policy

Call Secure Status Policy controls display of secure status icon on phones. The following are the policy options:

- All media except BFCP and iX application streams must be encrypted

This is the default value. The security status of the call is not dependent on the encryption status of BFCP and iX application streams.

- All media except iX application streams must be encrypted

The security status of the call is not dependent on the encryption status iX application streams.

- All media except BFCP application streams must be encrypted

The security status of the call is not dependent on the encryption status BFCP.

- All media in a session must be encrypted

The security status of the call is dependent on the encryption status of all the media streams of an established phone session.

- Only Audio must be encrypted

The security status of the call is dependent on the encryption of the audio stream.



Note Changes to the policy impacts display of the secure icon and playing of secure tone on the phone.

Procedure

- Step 1** From Unified Communications Manager Administration, choose **System > Service Parameters**.
 - Step 2** From **Select Server and Service** pane, choose your server and the CallManager service.
 - Step 3** Go to **Clusterwide Parameters (Feature - Call Secure Status Policy)** pane.
 - Step 4** From the **Secure Call Icon Display Policy** field, choose a policy from the drop-down list. A warning message with the impact on video calls and secure tone is displayed.
 - Step 5** Click **Save**.
The window refreshes, and Unified Communications Manager updates the policy in the **Service Parameter Configuration** page.
-

Enable Secure Indication Tone for Cluster

The secure indication tone plays on a protected phone when the overall status of the call specifies protected, when the system determines that the call is encrypted. You have to set the indication tone to True.

Procedure

- Step 1** From Unified Communications Manager Administration, choose **System > Service Parameters**.
 - Step 2** From **Select Server and Service** pane, choose your server and the CallManager service.
 - Step 3** Navigate to **Clusterwide Parameters (Feature - Secure Tone)** pane.
 - Step 4** Set the **Play Tone to Indicate Secure/Non-Secure Call Status** option to **True**. By default, the option is **False**.
After configuring the cluster for Secure Indication Tone, configure individual phones as Protected Phones. Only a protected phone can hear the secure and non secure tones.
-

Configure Phone As a Protected Device

You can configure supported Cisco Unified IP Phones as protected devices in Unified Communications Manager. Only callers on a protected phone can hear the secure and non secure indication tones.

Procedure

- Step 1** From Cisco Unified CM Administration, choose **Device > Phone**.
The list of phone appears.
- Step 2** Click the phone for which you want to set the secure tone parameters.
- Step 3** Navigate to the **Device Information** pane and perform the following:
 - a. From the **Softkey Template** drop-down list, choose **Standard Protected Phone**
 - Note** You must use a new softkey template without supplementary service softkeys for a protected phone.

- b. Check the **Protected Device** check box.

- Step 4** Navigate to the **Protocol Specific Information** pane.
- Step 5** From the **Device Security Profile** drop-down list, choose an encrypted security phone profile that is already configured in the **Phone Security Profile Configuration** page.
- Step 6** Click **Save**.

Secure Calls and Tones Limitations and Restrictions

The following are the limitations and restrictions with reference to the secure calls and tones:

Table 3: Secure Icons and Secure Tones Interactions and Restrictions

Feature	Interactions and Restrictions
H.323 Trunks	Secure icons not supported over H.323 trunks
Call Transfer and Hold	The encryption lock icon may not display on the phone when you perform tasks such as transferring or putting a call on hold. The status changes from encrypted to non-secure if the media streams that are associated with these tasks are not encrypted.
PSTN calls	For calls that involve the PSTN, the security icon shows the security status for only the IP domain portion of the call.
Barge	<p>With secure icons:</p> <ul style="list-style-type: none"> • Non secure or authenticated Cisco IP Phones can barge encrypted calls. The security icon indicates the security status for the conference calls. <p>With secure tones:</p> <ul style="list-style-type: none"> • If a caller barges a secure SIP call, the system provides tone-on-hold, and Unified Communications Manager classifies the call as non secure during the tone. • If a caller barges a secure SCCP call, the system uses an internal tone-playing mechanism at the target device and the status remains secure.

