Silent Monitoring

Silent Monitoring Overview

Silent call monitoring allows a supervisor to eavesdrop on a phone conversation. The most common scenario is in a call center where a call agent is speaking with a customer. Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. With silent monitoring, the supervisor can hear both call participants, but neither of the call participants can hear the supervisor.

Silent monitoring can only be invoked by a CTI application through the JTAPI or TAPI interfaces. Many Cisco applications, such as Cisco Unified Contact Center Enterprise and Cisco Unified Contact Center Express have the ability to use silent monitoring. Any CTI application that monitors calls must have the corresponding monitoring privileges that are enabled for the application-user or end-user account.

Silent monitoring is call based. When a supervisor invokes a silent monitoring session, the following occurs:

- The supervisor selects a specific call to be monitored.
- The start-monitoring request from the application triggers the supervisor phone to go off hook and automatically triggers a monitoring call to the agent.
- The agent phone automatically answers the monitoring call. The monitoring call does not get presented to the agent.

Secure Silent Monitoring

You can also configure secure silent monitoring. Secure silent monitoring allows encrypted media (sRTP) calls to be monitored. Monitoring calls are always established using the highest level of security that is determined by the capabilities of the agent phone regardless of the security status of the call being observed. The highest level of security is maintained by exchanging the secure media key in any call between the customer, agent, and supervisor. Monitoring calls using secured media carries approximately 4000 bits per second of additional bandwidth overhead, same as standard secure media (sRTP) calls.

If the agent phone has encryption that is enabled, the supervisor phone must also have encryption enabled in order to allow secure silent monitoring. If the agent phone has encryption that is enabled, but the supervisor phone does not, the monitoring request fails.

Whisper Coaching

Unified Communications Manager also supports whisper coaching, a CTI enhancement on silent monitoring whereby a supervisor can speak to the agent while the monitoring session is underway without the customer hearing. Whisper coaching can only be initiated by a CTI application. If silent monitoring is already configured, then no additional configuration of Unified Communications Manager is required for whisper coaching.

Silent Monitoring Prerequisites

Silent monitoring can only be invoked by an external CTI application. Cisco applications such as Cisco Unified Contact Center Enterprise or Cisco Unified Contact Center Express can initiate silent monitoring sessions. For details, see the following:

- Cisco Unified Contact Center Enterprise—For details on how to set up silent monitoring in Cisco Unified Contact Center Enterprise, see Cisco Remote Silent Monitoring Installation and Administration Guide.
- Cisco Unified Contact Center Express—This chapter contains a sample configuration to set up Silent Monitoring for Unified Contact Center Express via Cisco Finesse. For additional documentation that is related to your Cisco Unified Contact Center Express deployment, go to https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html.

Configure Silent Monitoring Task Flow

This task flow describes the tasks that you must perform within Unified Communications Manager to allow CTI applications to use the monitoring feature.

Before you begin

- Determine which phones support silent monitoring by running a phone feature list report. For more information,Generate a Phone Feature List

Procedure

	Command or Action	Purpose
Step 1	Perform one of the following procedures: • Enable Built in Bridge for Phones Clusterwide, on page 3 • Enable Built in Bridge for a Phone, on page 3	Turn on the Built in Bridge on agent phones. You can use a service parameter to configure the clusterwide default setting or you can enable the Built in Bridge for individual phones. **Note** The Built in Bridge setting on individual phones overrides the clusterwide default setting.

	Command or Action	Purpose
Step 2	Enable Monitoring Privileges for Supervisor, on page 4	Add the supervisor to a group that allows silent monitoring.
Step 3	Assign a Monitoring Calling Search Space, on page 4	Set up the monitoring calling search space for the supervisor phone.
Step 4	Configure Silent Monitoring Notification Tones, on page 5	Configure whether you want to play notification tones to the call participants.
Step 5	Configure Secure Silent Monitoring, on page 5	**Optional**. If your calls are encrypted, configure secure silent monitoring.
Step 6	Configure Silent Monitoring for Unified Contact Center Express, on page 6	For Unified Contact Center Express deployments, configure Silent Monitoring via Cisco Finesse.

Enable Built in Bridge for Phones Clusterwide

When you set the Built-in-Bridge clusterwide service parameter to enable, the Built-in-Bridge default setting for all phones in the cluster is changed to enabled. However, the Built-in-Bridge setting in the Phone Configuration window for individual phones overrides the clusterwide service parameter.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server on which the CallManager service is running.

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

Step 4 Set the **Builtin Bridge Enable** service parameter to **On**.

Step 5 Click **Save**.

Enable Built in Bridge for a Phone

Use this procedure to enable the Built in Bridge on an individual phone. The Built in Bridge setting on an individual phone overrides the clusterwide service parameter.

Before you begin

Use a service parameter to set the Built in Bridge defaults for all phones in the cluster. For details, see Enable Built in Bridge for Phones Clusterwide, on page 3.

Procedure

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

Step 2 Click **Find** to select the agent phone.

Step 3 From the **Built in Bridge** drop-down list, choose one of the following options:

- **On**—The Built in Bridge is enabled.
- **Off**—The Built in Bridge is disabled.
- **Default**—The setting of the clusterwide **Builtin Bridge Enable** service parameter is used.

Step 4 Click **Save**.

Enable Monitoring Privileges for Supervisor

In order for a supervisor to be able to monitor agent conversations, the supervisor must be part of a group that allows monitoring.

Before you begin

Perform one of the following procedures to enable the Built in Bridge on agent phones:

- Enable Built in Bridge for Phones Clusterwide, on page 3
- Enable Built in Bridge for a Phone, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Select the supervisor from the list of users.

Step 3 In the **Permissions Information** section, click **Add to Access Control Group**.

Step 4 Add the **Standard CTI Allow Call Monitoring** and **Standard CTI Enabled** user groups.

Step 5 Click **Save**.

Assign a Monitoring Calling Search Space

For monitoring to work, you must assign a Monitoring Calling Search Space to the supervisor phone line. The Monitoring Calling Search Space must include both the supervisor phone line and the agent phone line.

Procedure

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

Step 2 Click **Find** and select the supervisor phone.
The left navigation pane displays the available phone lines for the supervisor's phone.

Step 3 Perform the following steps for each of the supervisor's phone lines that are used for monitoring:

a) Click the phone line. The **Directory Number Configuration** window displays configuration information for that phone line.

b) From the **Monitoring Calling Search Space** drop-down list, choose a calling search space that includes both the supervisor phone line and the agent phone line.

c) Click **Save**.

Configure Silent Monitoring Notification Tones

In certain jurisdictions, a notification tone must be played to either the agent, the customer, or both, that indicates that the call is being monitored. By default, Unified Communications Manager does not play notification tones. You must configure a service parameter to allow notification tones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server one which the CallManager service is running.

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

Step 4 Configure values for the following service parameters:

- If you want to play a notification tone to the agent, change the value of the **Play Monitoring Notification Tone To Observed Target** service parameter to **True**.
- If you want to play a notification tone to the customer, change the value of the **Play Monitoring Notification Tone To Observed Connected Parties** service parameter to **True**.

Step 5 Click **Save**.

Step 6 Reset the agent phone, if you changed the service parameter configuration.

Configure Secure Silent Monitoring

To configure secure silent monitoring using sRTP, you must configure phone security profiles that include encryption and apply them to the supervisor phone and to any agent phones that are being monitored.

Procedure

	Command or Action	Purpose
Step 1	Configure an Encrypted Phone Security Profile , on page 5	Configure phone security profiles that include encryption for the agent phone and supervisor phone.
Step 2	Assign Security Profile to Phone, on page 6	Apply the encrypted phone security profile to the agent phone and the supervisor phone.

Configure an Encrypted Phone Security Profile

To configure secure silent monitoring, you must configure the phone security profile for your supervisor phone and any agent phones to specify **Encrypted** as the **Device Security Mode**.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform either of the following steps:

- Click **Add New** to create a new phone security profile.
- Click **Find** and select an existing phone security profile.

Step 3 If you have created a new phone security profile, select your phone model from the **Phone Security Profile Type** drop-down list.

Step 4 Enter a **Name** for the Phone Security Profile.

Step 5 From the **Device Security Mode** drop-down list, choose **Encrypted**.

Step 6 Click **Save**.

Step 7 Repeat the above steps to configure phone security profiles for your supervisor phone and any agent phones.

Assign Security Profile to Phone

Perform the following steps to assign a phone security profile to a phone. For secure silent monitoring to work, you must assign the phone security profile to both the agent phone and the supervisor phone.

Procedure

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

Step 2 Click **Find** and select the agent phone on which you want to configure a phone security profile.

Step 3 From the **Device Security Profile** drop-down list, choose the phone security profile that you have set up.

Step 4 Click **Save**.

Step 5 Repeat the previous steps for the supervisor phone.

Configure Silent Monitoring for Unified Contact Center Express

The following steps contain a sample Silent Monitoring for Cisco Unified Contact Center Express configuration via Cisco Finesse.

Before you begin

Make sure that both the agent and supervisor phone are compatibile for Cisco Finesse. Refer to the *Unified CCX Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Procedure

Step 1 Configure a test agent and supervisor on Unified Contact Center Express.

Note The IP Contact Center (IPCC) Extension for the Agents and Supervisors must be unique. This can be verified from Cisco Unified Communications Manager under **Call Routing** > **Route Plan Report**.

Step 2 Ensure that the agent phone has the Built in Bridge (BIB) On. This can be done on the phone or at the Cluster level (Set the Default Service Parameter to On).

Step 3 Log in to Finesse as an Agent.

Step 4 Log in to Finesse as a Supervisor and ensure that the supervisor is in NOT READY State.

Step 5 Ensure that the Resource Manager Contact Manager (RMCM) user has the required roles for Call Monitoring and Call Recording -- Standard Computer Telephony Integration (CTI) Allow Call Monitoring and Recording.

Note This is automatically done by Unified Contact Center Express at the initial setup of the RMCM user. Ensure the roles exist on the **Application User** window of Cisco Unified Communications Manager.

Step 6 Assign the Monitoring CSS (Calling Search Space) on the Supervisor Phone to contain the Partition of the agent line.

Step 7 Place a call to Unified Contact Center Express so that the call is routed to the agent logged in. Once the agent is in the TALKING state, from the supervisor, start the Silent Monitoring. The supervisor will then be able to hear the conversation between the agent and the caller

Silent Monitoring Interactions and Restrictions

Silent Monitoring Interactions

Feature	Interaction
Call preservation	If the agent call that is being monitored goes to call preservation, Unified Communications Manager also puts the monitoring call into call preservation mode.
Transfer of secure monitoring call	Unified Communications Manager supports transferring a secure monitoring session so long as the destination supervisor device exceeds the security capabilities of the agent that is being monitored.
Recording Tones	Recording Tones take precedence over Monitoring Tones for calls that are both recorded and monitored. If a call is recorded and monitored, only the recording tone plays.
Secure Tones	If Secure Tones are configured and the call is secured, the secure tone plays to both call participants at the outset of the call irrespective of whether Monitoring Tones are configured. If Secure Tones and Monitoring Tones are both configured, the secure tone plays once, followed by the monitoring tones. If Secure Tones, Monitoring Tones, and Recording Tones are all configured, and the call is recorded and monitored, the secure tone plays once followed by the recording tone. The monitoring tone does not play.

Silent Monitoring Restrictions

Feature	Restriction
Barge	Unified Communications Manager does not support barge with silent monitoring. If an agent call is being monitored, the barge-in call from a shared line fails. If the agent call has already been barged, the monitoring call fails.
Transfer of Secure Silent Monitoring over an intercluster trunk	Unified Communications Manager does not support transferring Secure Silent Monitoring calls over an intercluster trunk.