CHAPTER 12

Malicious Call Identification

The Malicious Call Identification (MCID) supplementary service allows you to report a call of a malicious nature by requesting that Cisco CallManager identify and register the source of an incoming call in the network.

This chapter provides the following information about the Malicious Call Identification feature:

Introducing Malicious Call Identification

Malicious Call Identification (MCID), an internetwork service, allows users to initiate a sequence of events when they receive calls with a malicious intent. The user who receives a disturbing call can invoke the MCID feature by using a softkey or feature code while connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco CallManager administrator. The MCID service flags the call detail record (CDR) with the MCID notice and sends a notification to the off-net PSTN that a malicious call is in progress.

The system supports the MCID service, which is an ISDN PRI service, when using PRI connections to the PSTN. The MCID service includes two components:

- MCID-O—An originating component that invokes the feature upon the user's request and sends the invocation request to the connected network.
- MCID-T—A terminating component that receives the invocation request from the connected network and responds with a success or failure message that indicates whether the service can be performed.

Note Cisco CallManager supports only the originating component at this time.

Using the Malicious Call ID Feature with Cisco CallManager

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco CallManager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user's phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

When the MCID feature is used, the following actions take place:

1. The user receives a threatening call and presses the Malicious Call softkey (or enters the feature code *39).
2. Cisco CallManager sends the user a confirmation tone if the device can play a tone—and a text message on a phone that has a display—to acknowledge receiving the MCID notification.
3. Cisco CallManager updates the CDR for the call with an indication that the call is registered as a malicious call.
4. Cisco CallManager generates the alarm and local syslogs entry that has the event information.
5. Cisco CallManager sends a MCID invocation through the facility message to the connected network. The facility information element (IE) encodes the MCID invocation.
6. After receiving this notification, the PSTN or other connected network can take actions, such as providing legal authorities with the call information.

System Requirements for Malicious Call ID

Malicious Call ID service requires Cisco CallManager 5.0 to operate.

The following gateways and connections support MCID service:

- PRI gateways that use the MGCP PRI backhaul interface for T1 (NI2) and E1 (ETSI) connections
- H.323 trunks and gateways

The Cisco SIP and SCCP IP Phones support MCID by using the Malicious Call Trace softkey in the Standard User softkey template.

The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

Interactions and Restrictions

The following sections describe the interactions and restrictions for Malicious Call Identification.

- Interactions, page 12-2
- Restrictions, page 12-4

Interactions

The following sections describe how Malicious Call Identification interacts with Cisco CallManager applications and call processing:

- Conference Calls, page 12-3
- Extension Mobility, page 12-3

Conference Calls

When a user is connected to a conference, the user can use the MCID feature to flag the call as a malicious call. Cisco CallManager sends the MCID indication to the user, generates the alarm, and updates the CDR. However, Cisco CallManager does not send an MCID invoke message to the connected network that might be involved in the conference.

Extension Mobility

Extension mobility users can have the MCID softkey as part of their user device profile and can use this feature when they are logged on to a phone.

Call Detail Records

To track malicious calls by using CDR, you must set the CDR Enabled Flag to True in the Cisco CallManager service parameter. When the MCID feature is used during a call, the CDR for the call contains “CallFlag=MALICIOUS” in the Comment field.

Alarms

To record alarms for the MCID feature in the Local Syslogs, you must configure alarms in Cisco CallManager Serviceability. Under Local Syslogs, enable alarms for the “Informational” alarm event level.

When the MCID featured is used during a call, the system logs an SDL trace and a Cisco CallManager trace in alarms. You can view the Alarm Event Log by using Cisco CallManager Serviceability. The traces provide the following information:

- Date and time
- Type of event: Information
- Information: Malicious Call Identification feature gets invoked in Cisco CallManager
- Called Party Number
- Called Device Name
- Called Display Name
- Calling Party Number
- Calling Device Name
- Calling Display Name
- Application ID
- Cluster ID
- Node ID

Refer to the *Cisco CallManager Serviceability Administration Guide* for more information about alarms and traces.

Restrictions

The following restrictions apply to Malicious Call Identification:

- Cisco CallManager supports only the malicious call identification originating function (MCID-O). Cisco CallManager does not support the malicious call identification terminating function (MCID-T). If Cisco CallManager receives a notification from the network of a malicious call identification, Cisco CallManager ignores the notification.
- MCID does not work across intercluster trunks because Cisco CallManager does not support the MCID-T function.
- Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.
- MCID does not work over QSIG trunks because MCID is not a QSIG standard.
- The Cisco VG248 Analog Phone Gateway does not support MCID.
- Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.

See the"Configuring Malicious Call ID" section on page 12-4 for configuration details.

Installing Malicious Call ID

Malicious Call Identification, which is a system feature, comes standard with Cisco CallManager software. MCID does not require special installation or activation.

Configuring Malicious Call ID

This section contains the following information:

Malicious Call ID Configuration Checklist

Table 12-1 provides a checklist for configuring Malicious Call Identification. You must configure the softkey template and assign the template to an IP phone to make the feature available to IP phones.

Table 12-1 MCID Configuration Checklist

Configuration Steps		Related procedures and topics
Step 1	Configure the CDR service parameter.	Setting the Service Parameter for Malicious Call ID, page 12-5 Service Parameters Configuration, *Cisco CallManager Administration Guide*
Step 2	Configure the alarm.	Configuring Alarms for Malicious Call ID, page 12-6 *Cisco CallManager Serviceability Administration Guide*
Step 3	Configure a softkey template with the Malicious Call Trace softkey.	Adding a Softkey Template for Malicious Call ID, page 12-6 Softkey Template Configuration, *Cisco CallManager Administration Guide*
Step 4	Assign the MCID softkey template to an IP phone.	Giving the Malicious Call Identification Feature to Users, page 12-7 Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
Step 5	Notify users that the Malicious Call Identification feature is available.	Refer to the phone documentation for instructions on how users access the Malicious Call Identification feature on their Cisco IP Phone.

Setting the Service Parameter for Malicious Call ID

To enable Cisco CallManager to flag a CDR with the MCID indicator, you must enable the CDR flag. Use the following procedure in Cisco CallManager Administration to enable CDR.

Procedure

Step 1 From the CCM Administration window, choose **System > Service Parameters**.

Step 2 Choose the Cisco CallManager server name.

Step 3 In the Service field, choose **Cisco CallManager**. The Service Parameters Configuration window displays.

Step 4 In the System area, set the CDR Enabled Flag field to **True** if it is not already enabled.

Step 5 If you need to make the change, click **Save**.

Configuring Alarms for Malicious Call ID

To ensure that the MCID alarm information appears in the Local Syslogs, you need to enable the alarm event level. Use Cisco CallManager Serviceability and the following procedure to activate alarms for MCID.

Procedure

Step 1 From the Navigation drop-down list box, choose Serviceability and click **Go**. Cisco CallManager Serviceability displays.

Step 2 Choose **Alarm > Configuration**. The Alarm Configuration window displays.

Step 3 From the servers list, choose the Cisco CallManager server.

Step 4 In the Configured Services list box, choose **Cisco CallManager**. The Alarm Configuration window updates with configuration fields.

Step 5 Under Local Syslogs, in the Alarm Event Level drop-down list, choose **Informational**.

Step 6 Under Local Syslogs, check the **Enable Alarm** check box.

Step 7 If you want to enable the alarm for all nodes in the cluster, check the **Apply to All Nodes** check box.

Step 8 Click **Update** to turn on the informational alarm.

Additional Information

See the "Related Topics" section on page 12-8.

Adding a Softkey Template for Malicious Call ID

Use this procedure in Cisco CallManager Administration to add the Malicious Call softkey to a template.

Procedure

Step 1 From CCM Administration, choose **Device > Device Settings > Softkey Template**. The Find and List Softkey Templates window displays.

Step 2 Click the **Add New** button. The Softkey Template Configuration window displays.

Step 3 In the Create a softkey template based on field, choose **Standard User**.

Step 4 Click **Copy**. The Softkey Template Configuration window refreshes with new fields.

Step 5 In the Softkey Template Name field, enter a name that indicates that this is a MCID softkey template.

Step 6 In the Description field, enter a description that indicates that this is a MCID softkey template.

Step 7 Click **Save**. The Softkey Template Configuration window refreshes with additional configuration fields.

Step 8 Click the **Go** button that is next to the **Configure Softkey Layout** related links box. The Softkey Layout Configuration window displays.

Step 9 In the Select a call state to configure field, choose **Connected**. The list of Unselected Softkeys changes to display the available softkeys for this call state.

Step 10 In the Unselected Softkeys list, choose **Toggle Malicious Call Trace**.

Step 11 To move the softkey to the Selected keys list, click the right arrow.

Step 12 Click **Save** to ensure that the softkey template is configured.

Additional Information

See the "Related Topics" section on page 12-8.

Giving the Malicious Call Identification Feature to Users

To provide the Malicious Call Identification feature for users, you assign the MCID softkey template to their IP phone.

Note For users who do not have phones that can use a softkey, give them the feature code information and instructions on how to invoke the feature.

Procedure

Step 1 Choose **Device > Phone**. The Find and List Phones window displays.

Step 2 To locate the phone configuration, enter appropriate phone search information; click **Find**.

Step 3 Choose the phone that you want to update.

Step 4 Locate the Softkey Template field and choose the MCID softkey template that you created from the drop-down list.

Step 5 To save the changes in the database, click **Save**.

Step 6 To activate the changes on the phone, click **Reset**.

Step 7 Notify the user that the Malicious Call Identification feature is available.

Additional Information

See the "Related Topics" section on page 12-8.

Removing the Malicious Call Identification Feature from a User

To remove the Malicious Call Identification feature from users, you assign another softkey template to their IP phone.

Procedure

Step 1 Choose **Device > Phone**. The Find and List Phones window displays.

Step 2 To locate the phone configuration, enter appropriate phone search information and click **Find**.

Step 3 Choose the phone that you want to update.

Step 4 Locate the Softkey Template field and choose a softkey template without MCID from the drop-down list.

Step 5 To save the changes in the database, click **Save**.

Step 6 To activate the changes on the phone, click **Reset**.

Step 7 Notify the user that the Malicious Call Identification feature is no longer available.

Additional Information

See the "Related Topics" section on page 12-8.

Troubleshooting Malicious Call ID

To assist with tracking and troubleshooting the Malicious Call ID feature, the system makes Cisco CallManager SDL traces and alarms available.

For information about using these traces and alarms, refer to the *Cisco CallManager Serviceability Administration Guide*.

Additional Information

See the "Related Topics" section on page 12-8.

Related Topics

- Cisco IP Phone Configuration, *Cisco CallManager Administration Guide*
- Softkey Template Configuration, *Cisco CallManager Administration Guide*
- Malicious Call ID Configuration Checklist, page 12-4
- Setting the Service Parameter for Malicious Call ID, page 12-5
- Adding a Softkey Template for Malicious Call ID, page 12-6
- Configuring Alarms for Malicious Call ID, page 12-6
- Giving the Malicious Call Identification Feature to Users, page 12-7
- Removing the Malicious Call Identification Feature from a User, page 12-7

Additional Cisco Documentation

- *Cisco CallManager Serviceability Administration Guide*
- *Cisco IP Phone Administration Guide for Cisco CallManager*
- Cisco IP Phone user documentation and release notes (all models)