Malicious Call Identification

- Malicious Call Identification Overview, on page 1
- Malicious Call Identification Prerequisites, on page 1
- Malicious Call Identification Configuration Task Flow, on page 2
- Malicious Call Identification Interactions, on page 8
- Malicious Call Identification Restrictions, on page 9
- Malicious Call ID Troubleshooting, on page 10

Malicious Call Identification Overview

You can configure the Malicious Call Identification (MCID) feature to track troublesome or threatening calls. Users can report these calls by requesting that Cisco Unified Communications Manager identify and register the source of the incoming call in the network.

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

1. The user receives a threatening call and presses Malicious call (or enters the feature code *39 if using a POTS phone that is connected to an SCCP gateway).
2. Cisco Unified Communications Manager sends the user a confirmation tone and a text message, if the phone has a display, to acknowledge receiving the MCID notification.
3. Cisco Unified Communications Manager updates the call details record (CDR) for the call with an indication that the call is registered as a malicious call.
4. Cisco Unified Communications Manager generates the alarm and local syslogs entry that contains the event information.
5. Cisco Unified Communications Manager sends an 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.

Malicious Call Identification Prerequisites

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

- IP Phones that support MCID

Malicious Call Identification Configuration Task Flow

Before you begin

- Review Malicious Call Identification Prerequisites, on page 1

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List	Generate a report to identify devices that support the MCID feature.
Step 2	Set Malicious Call ID Service Parameter, on page 3	Enable Cisco Unified Communications Manager to flag a call detail record (CDR) with the MCID indicator.
Step 3	Configure Malicious Call ID Alarms, on page 3	Configure alarms to ensure that alarm information displays in the system logs.
Step 4	Configure a Softkey Template for Malicious Call Identification, on page 4	Configure a softkey template with MCID. **Note** The Cisco Unified IP Phones 8900 and 9900 Series support MCID with feature button only.
Step 5	To Associate a Softkey Template with a Common Device Configuration, on page 4, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration, on page 5 • Associate a Common Device Configuration with a Phone, on page 6	Optional. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 6	Associate a Softkey Template with a Phone, on page 6	Optional. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 7	To Configure Malicious Call Identification Button, on page 6, complete the following subtasks:	Perform this step to add and configure the MCID button to a phone.

	Command or Action	Purpose
	• Configure Malicious Call ID Phone Button Template, on page 7 • Associate a Button Template with a Phone , on page 7	

Set Malicious Call ID Service Parameter

To enable Unified Communications Manager to flag a CDR with the MCID indicator, you must enable the CDR flag.

Before you begin

Configure Malicious Call ID Alarms, on page 3

Procedure

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

Step 2 From the **Server** drop-down list, choose the Unified Communications Manager server name.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.
The **Service Parameter Configuration** window displays.

Step 4 In the System area, set the **CDR Enabled Flag** field to **True**.

Step 5 Click **Save**.

Configure Malicious Call ID Alarms

In the Local Syslogs, you must set the alarm event level and activate alarms for MCID.

Before you begin

Set Malicious Call ID Service Parameter, on page 3

Procedure

Step 1 From Cisco Unified Serviceability, choose **Alarm** > **Configuration**.
The **Alarm Configuration** window displays.

Step 2 From the **Server** drop-down list, choose the Unified Communications Manager server and click **Go**.

Step 3 From the **Service Group** drop-down list, choose **CM Services**. The **Alarm Configuration** window updates with configuration fields.

Step 4 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 5 Under Local Syslogs, in the **Alarm Event Level** drop-down list, choose **Informational**.
The **Alarm Configuration** window updates with configuration fields.

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 To turn on the informational alarm, click **Update**.

Configure a Softkey Template for Malicious Call Identification

Note Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.

Before you begin

Configure Malicious Call ID Alarms, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 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 7 In the **Unselected Softkeys** drop-down list, choose **Toggle Malicious Call Trace (MCID)**.

Step 8 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 9 Click **Save.**

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone, on page 6.

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 4

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to a Common Device Configuration, on page 5	
Step 2	Associate a Common Device Configuration with a Phone, on page 6	

Add a Softkey Template to a Common Device Configuration

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 4

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.

- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add a Softkey Template to a Common Device Configuration, on page 5

Procedure

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

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

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

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Malicious Call Identification Button

The procedures in this section describe how to configure the Malicious Call Identification button.

Before you begin

Configure Malicious Call ID Alarms, on page 3

Procedure

	Command or Action	Purpose
Step 1	Configure Malicious Call ID Phone Button Template, on page 7.	Perform this step to assign Malicious Call Identification button features to line or speed dial keys.
Step 2	Associate a Button Template with a Phone , on page 7	Perform this step to configure the Malicious Call Identification button for a phone.

Configure Malicious Call ID Phone Button Template

Before you begin

Configure Malicious Call ID Alarms, on page 3

Procedure

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

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Before you begin

Configure Malicious Call ID Phone Button Template, on page 7

Procedure

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

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Malicious Call Identification Interactions

Table 1: Malicious Call Identification Interactions

Feature	Interaction
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 Unified Communications Manager sends the MCID indication to the user, generates the alarm, and updates the CDR. However, Cisco Unified Communications Manager 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.

Feature	Interaction
Alarms	To record alarms for the MCID feature in the Local Syslogs, you must configure alarms in Cisco Unified Serviceability. Under **Local Syslogs**, enable alarms for the **Informational** alarm event level. When the MCID feature is used during a call, the system logs an SDL trace and a Cisco Unified Communications Manager trace in alarms. You can view the **Alarm Event Log** by using Cisco Unified Serviceability. The traces provide the following information: • Date and time • Type of event: Information • Information: The Malicious Call Identification feature is invoked in Cisco Unified Communications Manager • Called Party Number • Called Device Name • Called Display Name • Calling Party Number • Calling Device Name • Calling Display Name • Application ID • Cluster ID • Node ID For more information about alarms and traces, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
Cisco ATA 186 analog phone ports	The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

Malicious Call Identification Restrictions

Table 2: Malicious Call Identification Restrictions

Feature	Restriction
Malicious Call Identification Terminating (MCID-T) function	Cisco Unified Communications Manager supports only the malicious call identification originating function (MCID-O). Cisco Unified Communications Manager does not support the malicious call identification terminating function (MCID-T). If Cisco Unified Communications Manager receives a notification from the network of a malicious call identification, Cisco Unified Communications Manager ignores the notification.

Feature	Restriction
Intercluster trunks	MCID does not work across intercluster trunks because Cisco Unified Communications Manager does not support the MCID-T function.
Cisco MGCP FXS gateways	Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.
QSIG trunks	MCID does not work over QSIG trunks because MCID is not a QSIG standard.
Cisco VG248 Analog Phone Gateway	Cisco VG248 Analog Phone Gateway does not support MCID.
SIP trunks	MCID does not support SIP trunks.
Immediate Divert	System does not support using MCID and Immediate Divert features together.

Malicious Call ID Troubleshooting

To track and troubleshoot Malicious Call ID, you can use Cisco Unified Communications Manager SDL traces and alarms. For information about setting traps and traces for MCID, see the *Cisco Unified Serviceability Administration Guide*. For information about how to generate reports for MCID, see the *Cisco Unified CDR Analysis and Reporting Administration Guide*.