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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Generate a Phone Feature List</td>
<td>Generate a report to identify devices that support the MCID feature.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set Malicious Call ID Service Parameter, on page 3</td>
<td>Enable Cisco Unified Communications Manager to flag a call detail record (CDR) with the MCID indicator.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Malicious Call ID Alarms, on page 3</td>
<td>Configure alarms to ensure that alarm information displays in the system logs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure a Softkey Template for Malicious Call Identification, on page 4</td>
<td>Configure a softkey template with MCID.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>The Cisco Unified IP Phones 8900 and 9900 Series support MCID with feature button only.</td>
</tr>
<tr>
<td>Step 5</td>
<td>To Associate a Softkey Template with a Common Device Configuration, on page 5, complete the following subtasks:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Add a Softkey Template to a Common Device Configuration, on page 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Associate a Common Device Configuration with a Phone, on page 6</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Associate a Softkey Template with a Phone, on page 6</td>
<td>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.</td>
</tr>
<tr>
<td>Step 7</td>
<td>To Configure Malicious Call Identification Button, on page 7, complete the following subtasks:</td>
<td>Perform this step to add and configure the MCID button to a phone.</td>
</tr>
<tr>
<td></td>
<td>• Configure Malicious Call ID Phone Button Template, on page 7</td>
<td></td>
</tr>
</tbody>
</table>
### Set Malicious Call ID Service Parameter

To enable Cisco 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Associate a Button Template with a Phone, on page 8</td>
<td></td>
</tr>
</tbody>
</table>

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

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

**What to do next**

Configure Malicious Call ID Alarms, on page 3

### 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 Cisco 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.

What to do next
Configure a Softkey Template for Malicious Call Identification, on page 4

**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. The Softkey Template Configuration window appears.
**Step 2** Perform this step 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) In the Softkey Template Name field, enter a new name for the template.
   d) Click Save.
**Step 3** Perform this step to add softkeys to an existing template.
   a) Enter search criteria and click Find.
   b) Choose an existing template.
   The Softkey Template Configuration window appears.
**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Add a Softkey Template to a Common Device Configuration, on page 5</td>
</tr>
<tr>
<td>Step 2</td>
<td>Associate a Common Device Configuration with a Phone, on page 6</td>
</tr>
</tbody>
</table>

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. The Find and List Common Device Configuration window appears.

Step 2 Perform this step 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) In the Name field, enter a name for the Common Device Configuration.
c) Click Save.

Step 3 Perform this step to add the softkey template to an existing Common Device Configuration.

a) Enter search criteria and click Find.
b) Choose an existing Common Device Configuration. The **Common Device Configuration** window appears.

**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 created a new Common Device Configuration, associate the configuration with devices and then restart them. See the What to Do Next section for more information.
- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.

---

**What to do next**

**Associate a Common Device Configuration with a Phone**

---

**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**. The **Find and List Phones** window appears.

**Step 2** Find the phone to which 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**

This procedure is optional. You can 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: 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**. The **Find and List Phones** window appears.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure Malicious Call ID Phone Button Template, on page 7.</td>
<td>Perform this step to assign Malicious Call Identification button features to line or speed dial keys.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Associate a Button Template with a Phone, on page 8</td>
<td>Perform this step to configure the Malicious Call Identification button for a phone.</td>
</tr>
</tbody>
</table>

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. The Find and List Phone Button Templates window appears.

**Step 2** Click Find.
The window displays a list of templates for the supported phones.

**Step 3** Perform this step 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 this step if you want to add phone buttons to an existing template.
a) Enter search criteria and click Find.
b) Choose an existing template.
The Phone Button Template Configuration window appears.
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:

- If you modified a template that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. See the What to Do Next section for more information.

---

**What to do next**

*Associate a Button Template with a Phone*, on page 8

---

**Associate a Button Template with a Phone**

**Before you begin**

*Configure Malicious Call ID Phone Button Template*, on page 7

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From Cisco Unified CM Administration, choose <strong>Device &gt; Phone</strong>. The <strong>Find and List Phones</strong> window is displayed.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the <strong>Find and List Phones</strong> window, click <strong>Find</strong>. A list of phones that are configured on the Unified Communications Manager is displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the phone to which you want to add the phone button template. The <strong>Phone Configuration</strong> window appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Phone Button Template</strong> drop-down list, choose the phone button template that contains the new feature button.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>. A dialog box is displayed with a message to press <strong>Reset</strong> to update the phone settings.</td>
</tr>
</tbody>
</table>
Malicious Call Identification Interactions and Restrictions

Malicious Call Identification Interactions

Table 1: Malicious Call Identification Interactions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Calls</td>
<td>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.</td>
</tr>
<tr>
<td>Extension Mobility</td>
<td>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.</td>
</tr>
<tr>
<td>Call Detail Records</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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  
**Interaction Feature**

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**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Call Identification Terminating (MCID-T) function</td>
<td>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.</td>
</tr>
<tr>
<td>Intercluster trunks</td>
<td>MCID does not work across intercluster trunks because Cisco Unified Communications Manager does not support the MCID-T function.</td>
</tr>
<tr>
<td>Cisco MGCP FXS gateways</td>
<td>Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.</td>
</tr>
<tr>
<td>QSIG trunks</td>
<td>MCID does not work over QSIG trunks because MCID is not a QSIG standard.</td>
</tr>
<tr>
<td>Cisco VG248 Analog Phone Gateway</td>
<td>Cisco VG248 Analog Phone Gateway does not support MCID.</td>
</tr>
<tr>
<td>SIP trunks</td>
<td>MCID does not support SIP trunks.</td>
</tr>
<tr>
<td>Immediate Divert</td>
<td>System does not support using MCID and Immediate Divert features together.</td>
</tr>
</tbody>
</table>

---

### 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*. 