Malicious Call Identification

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

- Configuration Checklist for Malicious Call ID, page 33-1
- Introducing Malicious Call Identification, page 33-2
- System Requirements for Malicious Call ID, page 33-3
- Devices That Support Malicious Call Identification, page 33-4
- Interactions and Restrictions, page 33-4
- Installing Malicious Call ID, page 33-6
- Configuring Malicious Call ID, page 33-6
- Troubleshooting Malicious Call ID, page 33-10
- Related Topics, page 33-11

Configuration Checklist for Malicious Call ID

The malicious call identification (MCID) feature allows a user to report a call of a malicious nature by requesting that Cisco Unified Communications Manager identify and register the source of an incoming call in the network.

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 button while the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager 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.
Introducing Malicious Call Identification

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

Table 33-1 provides a checklist for configuring malicious call identification. For additional information on malicious call identification, see the “Introducing Malicious Call Identification” section on page 33-2 and the “Related Topics” section on page 33-11.

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related procedures and topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Configure the CDR service parameter.</td>
</tr>
<tr>
<td></td>
<td>Setting the Service Parameter for Malicious Call ID, page 33-7</td>
</tr>
<tr>
<td></td>
<td>Service Parameter Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure the alarm.</td>
</tr>
<tr>
<td></td>
<td>Configuring Alarms for Malicious Call ID, page 33-7</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Serviceability Administration Guide</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>If users will access MCID by using a softkey, configure a softkey template with the Toggle Malicious Call Trace (MCID) softkey.</td>
</tr>
<tr>
<td></td>
<td>Adding a Softkey Template for Malicious Call ID, page 33-8</td>
</tr>
<tr>
<td></td>
<td>Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Cisco Unified IP Phones 8900 and 9900 series support MCID with feature button only.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Assign the MCID softkey template to an IP phone.</td>
</tr>
<tr>
<td></td>
<td>Giving the Malicious Call Identification Feature to Users, page 33-8</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>If users will access MCID by using a feature button, configure a phone button template with the Malicious Call Identification feature.</td>
</tr>
<tr>
<td></td>
<td>Adding a Phone Button Template for Malicious Call ID, page 33-9</td>
</tr>
<tr>
<td></td>
<td>Phone Button Template Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Assign the MCID phone button template to an IP phone.</td>
</tr>
<tr>
<td></td>
<td>Giving the Malicious Call Identification Feature to Users, page 33-10</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Notify users that the Malicious Call Identification feature is available.</td>
</tr>
<tr>
<td></td>
<td>See the phone documentation for instructions on how users access the Malicious Call Identification feature on their Cisco Unified IP Phone.</td>
</tr>
</tbody>
</table>
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 the user is connected to the call. The MCID service immediately flags the call as a malicious call with an alarm notification to the Cisco Unified Communications Manager 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 it is using PRI connections to the PSTN. The MCID service includes two components:

- **MCID-O**—An originating component that invokes the feature upon the user 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 Unified Communications Manager supports only the originating component.

### Using the Malicious Call ID Feature with Cisco Unified Communications Manager

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified Communications Manager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user 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 Malicious Call (or enters the feature code *39).
2. Cisco Unified Communications Manager 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 Unified Communications Manager updates the 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 sylogs entry that has 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.

### System Requirements for Malicious Call ID

Malicious Call ID service requires Cisco Unified Communications Manager 5.0 or later 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
Devices That Support Malicious Call Identification

Use the Cisco Unified Reporting application to generate a complete list of IP Phones that support MCID. To do so, follow these steps:

1. Start Cisco Unified Reporting by using any of the methods that follow.
   - by choosing Cisco Unified Reporting in the Navigation menu in Cisco Unified Communications Manager Administration and clicking Go.
   - by choosing File > Cisco Unified Reporting at the Cisco Unified Real Time Monitoring Tool (RTMT) menu.
   - by entering https://<server name or IP address>:8443/cucreports/ and then entering your authorized username and password.

2. Click System Reports in the navigation bar.

3. In the list of reports that displays in the left column, click the Unified CM Phone Feature List option.

4. Click the Generate a new report link to generate a new report, or click the Unified CM Phone Feature List link if a report already exists.

5. To generate a report of all IP Phones that support MCID, choose these settings from the respective drop-down list boxes and click the Submit button:
   - Product: All
   - Feature: Malicious Call Identification

   The List Features pane displays a list of all devices that support the MCID feature. You can click on the Up and Down arrows next to the column headers (Product or Protocol) to sort the list.

For additional information about the Cisco Unified Reporting application, see the Cisco Unified Reporting Administration Guide, which you can find at this URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Interactions and Restrictions

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

- Interactions, page 33-5
- Restrictions, page 33-6
Interactions

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

- Conference Calls, page 33-5
- Extension Mobility, page 33-5
- Call Detail Records, page 33-5
- Alarms, page 33-5

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.

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: Malicious Call Identification feature gets invoked in Cisco Unified Communications Manager
- Called Party Number
- Called Device Name
- Called Display Name
- Calling Party Number
- Calling Device Name
- Calling Display Name
Installing Malicious Call ID

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

Configuring Malicious Call ID

This section contains the following information:

- Setting the Service Parameter for Malicious Call ID, page 33-7
- Configuring Alarms for Malicious Call ID, page 33-7
- Adding a Softkey Template for Malicious Call ID, page 33-8
- Giving the Malicious Call Identification Feature to Users, page 33-8
- Removing the Malicious Call Identification Feature from a User, page 33-9
- Adding a Phone Button Template for Malicious Call ID, page 33-9
- Giving the Malicious Call Identification Feature to Users, page 33-10

Restrictions

The following restrictions apply to Malicious Call Identification:

- 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.
- MCID does not work across intercluster trunks because Cisco Unified Communications Manager 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.
- MCID does not support SIP trunks.

See the “Configuring Malicious Call ID” section on page 33-6 for configuration details.
Tip
Before you configure Malicious Call Identification, review the “Configuration Checklist for Malicious Call ID” section on page 33-1.

Setting the Service Parameter for Malicious Call ID

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

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose System > Service Parameters.
Step 2 Choose the Cisco Unified Communications Manager 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 Unified Serviceability and the following procedure to activate alarms for MCID.

Procedure

Step 1 From the Navigation drop-down list box, choose Cisco Unified Serviceability and click Go. Cisco Unified Serviceability displays.
Step 2 Choose Alarm > Configuration. The Alarm Configuration window displays.
Step 3 From the servers list, choose the Cisco Unified Communications Manager 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 To turn on the informational alarm, click Update.

Additional Information
See the “Related Topics” section on page 33-11.
Adding a Softkey Template for Malicious Call ID

Use this procedure in Cisco Unified Communications Manager Administration to add the Malicious Call softkey to a template.

**Procedure**

**Step 1**
From Cisco Unified Communications Manager 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 an MCID softkey template.

**Step 6**
In the Description field, enter a description that indicates that this is an 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 (MCID).

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

**Step 12**
To ensure that the softkey template is configured, click Save.

**Additional Information**
See the “Related Topics” section on page 33-11.

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 33-11.

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 soft key 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 33-11.

Adding a Phone Button Template for Malicious Call ID

Use this procedure in Cisco Unified Communications Manager Administration to add the Malicious Call button to a phone button template.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose Device > Device Settings > Phone Button Template. The Find and List Phone Button Templates window displays.
Step 2 Click the Add New button. The Phone Button Template Configuration window displays.
Step 3 In the Phone Button Template drop-down list box, choose the phone button template for the IP phone.
Step 4 Click Copy. The Phone Button Template Configuration window displays.
Step 5 In the Button Template Name field, enter a name that indicates that this is an MCID phone button template.
Step 6 Click Save. The Phone Button Template Configuration window redisplayes with new fields.
Step 7    Choose a line button that you want the MCID feature assigned; for example button 3.
Step 8    From the drop-down list box for the line button you chose, choose Malicious Call Identification.
Step 9    Click **Save**. The Phone Button Template Configuration window refreshes.

**Additional Information**
See the “Related Topics” section on page 33-11.

### Giving the Malicious Call Identification Feature to Users

To provide the Malicious Call Identification feature for users, you assign the MCID phone button 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; click **Find**.
Step 3    Choose the phone that you want to update.
Step 4    Locate the Phone Button Template field and choose the MCID phone button 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 33-11.

### Troubleshooting Malicious Call ID

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

For information about using these traces and alarms, see the *Cisco Unified Serviceability Administration Guide*.

**Additional Information**
See the “Related Topics” section on page 33-11.
Related Topics

- Configuration Checklist for Malicious Call ID, page 33-1
- Introducing Malicious Call Identification, page 33-2
- System Requirements for Malicious Call ID, page 33-3
- Interactions and Restrictions, page 33-4
- Installing Malicious Call ID, page 33-6
- Configuring Malicious Call ID, page 33-6
- Troubleshooting Malicious Call ID, page 33-10
- Cisco Unified IP Phone Configuration, Cisco Unified Communications Manager Administration Guide
- Softkey Template Configuration, Cisco Unified Communications Manager Administration Guide
- Configuration Checklist for Malicious Call ID, page 33-1
- Setting the Service Parameter for Malicious Call ID, page 33-7
- Adding a Softkey Template for Malicious Call ID, page 33-8
- Configuring Alarms for Malicious Call ID, page 33-7
- Giving the Malicious Call Identification Feature to Users, page 33-8
- Removing the Malicious Call Identification Feature from a User, page 33-9

Additional Cisco Documentation

- Cisco Unified Serviceability Administration Guide
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone user documentation and release notes (all models)