Malicious Call Identification

This chapter provides information about the Malicious Call Identification feature.

Configure 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.

Perform the following steps to configure malicious call identification. For additional information on malicious call identification, see the Malicious Call Identification Feature, on page 2 and the Malicious Call Identification, on page 1.

Procedure

Step 1 Configure the CDR service parameter.

Step 2 Configure the alarm.

Step 3 If users will access MCID by using a softkey, configure a softkey template with the Toggle Malicious Call Trace (MCID) softkey.

Note The Cisco Unified IP Phones 8900 and 9900 series support MCID with feature button only.

Step 4 Assign the MCID softkey template to an IP phone.

Step 5 If users will access MCID by using a feature button, configure a phone button template with the Malicious Call Identification feature.

Step 6 Assign the MCID phone button template to an IP phone.

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

Related Topics

Set Malicious Call ID Service Parameter, on page 6
Configure Malicious Call ID Alarms, on page 6
Configure a Softkey Template for Malicious Call Identification, on page 7
Associate a Softkey Template with a Phone, on page 8
Configure Malicious Call ID Phone Button Template, on page 8

Malicious Call Identification Feature

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.

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.

Use the Malicious Call ID Feature with CUCM

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 syslogs 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
- H.323 trunks and gateways

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

To determine which IP Phones support the MCID feature, see the Determine Device Support for Malicious Call Identification, on page 3.

Determine Device Support for 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:

Procedure

Step 1 Start Cisco Unified Reporting by using any of the methods that follow. The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application. You can access the application

- 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.

Step 2 Click **System Reports** in the navigation bar.

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

Step 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.

Step 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*.

Interactions and Restrictions

This section describes the interactions and restrictions for Malicious Call Identification.

Interactions

This section describes how Malicious Call Identification interacts with Cisco Unified Communications Manager applications and call processing features.

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 featured 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

See the *Cisco Unified Serviceability Administration Guide* for more information about alarms and traces.

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 Configure Malicious Call ID, on page 6 for configuration details.

Install 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.

Configure Malicious Call ID

This section provides information to configure Malicious Call ID.

Tip Before you configure Malicious Call Identification, review the configuration summary task for this feature.

Related Topics

Configure Malicious Call ID, on page 1

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 6

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 6

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 6

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 Phone

To provide the MCID feature to users, you must assign the MCID softkey template to their IP phone.

Note For users whose phones do not have a softkeys, provide them the feature code information and instructions on how to invoke the feature.

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 7

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.

Remove the Malicious Call Identification Feature from a User

To remove the MCID feature from a user, you must assign another softkey template to their IP phone.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.
The **Find and List Phones** window displays.

Step 2 To locate the phone configuration, enter 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.

Configure Malicious Call ID Phone Button Template

Before you begin

Configure Malicious Call ID Alarms, on page 6

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 8

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 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*.