

MTAS Malicious Communication Identification Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
2.1	Temporary Mode Using Supplementary Service Code Commands	4
2.2	Communication Details Information Capture and Report	4
2.3	MCID Subfunctions	5
2.4	MCID Interaction with Other Services	5
3	MCID Service Configuration	11
3.1	MCID Administrative State Configuration	11
3.2	Reporting Method Configuration	11
3.3	CDS Configuration	12
3.4	Closure of ACR Files for Local Storage Configuration	12
3.5	Disk Full and Disk Not Full Percentage Levels Configuration	12
3.6	File Transfer	13
3.7	Access Rights to Log Files and Directories Configuration	13
3.8	Service Data Configuration	13
3.9	Announcement Configuration	13
3.10	Wholesale for MCID Configuration	13
4	Performance Management	15
5	Fault Management	17





1 Introduction

This document describes how to configure the Malicious Communication Identification (MCID) service in the MTAS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the O&M area, in general.

1.1.1 Licenses

No license is required for the MCID service.

1.1.2 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- *Ericsson Command-Line Interface User Guide*
- *Managed Object Model (MOM)*

1.1.3 Conditions

The following condition must apply:

An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Overview

The MTAS offers the MCID service to its subscribers. The MCID service makes it possible for a subscriber to register a recent incoming\outgoing communication as malicious.

The MCID service is executed on the terminating and originating MTAS and has the following two modes:

- Permanent mode

The details of all incoming communications to the served user are reported.

- Temporary mode

The details of the last two incoming communications to the served user are stored. The served user can use a Supplementary Service Code (SSC) to start the MCID service. Based on the SSC used, the communication details held in either the latest store or the previous store is reported. Permanent MCID service can be started only at terminating MTAS.

The MCID service has two following reporting methods:

- Through CDS interface

Transfer the MCID information to the CDS through the CDS interface.

- Local Storage

Store the MCID information locally on the file systems of the nodes as Accounting Request (ACR) files. They can be later transferred to an external server by the use of file transfer. This reporting method is realized by the local storage function, see Section 2.4 MCID Interaction with Other Services on page 5.

The MCID service is based on the 3GPP standards. The MTAS uses information received in the initial `INVITE` request for identification purposes and does not support the generation of `SIP INFO` requests to obtain identification information that is not present in the `INVITE` request. For the temporary mode in the MCID service, the MTAS does not support the use of a `SIP re-INVITE` request to register a communication as malicious. The MCID service is collocated with other supplementary services on the MTAS node, for example, the Communication Diversion (CDIV).

As an addition to the standard, MTAS also supports MCID service on the originating side. Using MCID as originating service. Permanent mode is also supported on the originating side.



2.1 Temporary Mode Using Supplementary Service Code Commands

For the temporary mode in the MCID service, the served user can use an SSC command to register one of the last two incoming communications as malicious.

For more information about the handling of the SSC services, refer to *MTAS Supplementary Service Codes Management Guide*.

2.2 Communication Details Information Capture and Report

The following communication details are captured for each incoming communication attempt:

- Request URI
- To header
- P-Asserted-Identity headers, if available
- From header
- Contact headers
- History-Info headers, if available
- Referred-By header, if available
- Privacy header, if available
- MCID time stamp

For more information about Diameter communication details, refer to *Diameter Communication Details in MTAS*.

For the permanent mode in the MCID service, the captured communication details together with the Universal Time Coordinated (UTC) time or date that the initial INVITE request was received, are reported.

For the temporary mode in the MCID service, the captured communication details, together with the current UTC time/date, are stored in the latest store on receipt of the first 180 Ringing response to the initial INVITE request. If no 180 Ringing responses are received, the captured communication details, together with the current UTC time/date, are stored in the latest store on receipt of the 200 OK response to the initial INVITE. Information in the communication details store is reported if the served user later registers the communication as malicious.

When interworking with non-3GPP compliant application servers, the MTAS can modify the information contained in the initial INVITE request before



the communication details are captured for MCID purposes. For example, `Diversion` headers can be converted into `History-Info` headers.

2.3 MCID Subfunctions

The subfunctions included in the MCID service are described in this section.

2.3.1 Register Malicious Caller Temporary Mode

This subfunction is the action taken by a served user to register an incoming communication as malicious. Registration is performed using SSCs.

2.3.2 Register Malicious Caller Permanent Mode

This subfunction is the action taken by the MTAS to register an incoming communication to a served user who has the permanent mode in the MCID.

2.3.3 Manage Service Data for Registered Subscribers

This subfunction handles subscriber data management for registered subscribers. When a deregistration is received or when the registration timer expires, the Implicit Registration Set (IRS) and transparent data is purged immediately along with any incoming communication details stored.

For more information about the handling of the subscriber data, refer to *MTAS Subscriber Data Management Guide*.

2.3.4 Local Storage

This subfunction stores the MCID information into the ACR files locally on the file system of the node in the following directories:

`/cluster/storage/no-backup/MtasMcidInfo/PL-<x>`, where `<x>` is 1, 2, 3, and so on, corresponds to the number of PLs in the system, that is PL-1, PL-2, PL-3, and so on.

The subfunction can be turned on and off and configured with triggers for closure of the ACR files (for instance, based on the percentage of used disk). It counts the number of successful and unsuccessful storage requests per file system of the node. The ACR file format is described in *ACR Storage in MTAS*.

2.4 MCID Interaction with Other Services

This section describes the MCID interaction with other services.



2.4.1 Communication Diversion

The MCID interacts with several services included in the CDIV service.

For more information about the CDIV service, refer to *MTAS Communication Diversion Management Guide*.

Communication Deflection

Communication Deflection (CD) can occur immediately or can occur during the period that the served user is being informed of the communication, for example, during ringing.

For immediate CD, the MTAS receives a 302 response without any preceding 180 Ringing responses. Communication details held in the latest store are not updated.

For CD during ringing, the communication details are stored in the latest store on receipt of the first 180 Ringing response. Subsequent forwarding actions do not affect the stored information.

Communication Forwarding No Reply

For the Communication Forwarding No Reply (CFNR), communication details held in the latest store are updated on receipt of the first 180 Ringing response from the served user. Subsequent forwarding actions do not affect the stored information.

Communication Forwarding on Busy

The Communication Forwarding on Busy (CFB) service is started on receipt of a busy response from the served user. The busy response can be received with or without the user being alerted.

If the CFB service is started without the user being alerted, for example, no 180 Ringing response is received, communication details held in the latest store are not updated.

If the user is alerted, the communication details held in the latest store are updated on receipt of the first 180 Ringing response as normal. Subsequent forwarding actions do not affect the stored information.

Communication Forwarding Unconditional

For the Communication Forwarding Unconditional (CFU) service, communication details held in the latest store are not updated.



Communication Forwarding Not Logged

For the Communication Forwarding Not Logged (CFNL) service, communication details held in the latest store are not updated.

Communication Forwarding Not Reachable

For the Communication Forwarding Not Reachable (CFNRc) service, communication details held in the latest store are not updated.

2.4.2 Communication Waiting

For the Communication Waiting (CW) service, communication details held in the latest store are updated on receipt of the first 180 Ringing response from the served user.

For more information about the CW service, refer to *MTAS Communication Waiting Management Guide*.

2.4.3 Communication Completion

For the Communication Completion (CC) service, communication details held in the latest store for the called user are only updated for the original busy communication if a 180 Ringing response is received before the busy condition is identified.

Communication details held in the latest store for the user starting the CC service are not updated during the recall after the original called user has become free.

Communication details held in the latest store for the called user are updated during the recall as for a normal communication request.

For more information about the CC service, refer to *MTAS Communication Completion Management Guide*.

2.4.4 Incoming Communication Barring

For the Incoming Communication Barring (ICB) service, communication details held in the latest store are not updated when a communication request is rejected owing to the ICB or Anonymous Communication Rejection (ACR) service.

For more information about the Communication Barring services, refer to *MTAS Barring and Dial Plan Services Management Guide*.



2.4.5 Forking

For forking, communication details held in the latest store are updated on receipt of the first `180 Ringing` response to the `INVITE` request, or on receipt of a `200 OK` response if no `180 Ringing` responses have been received.

2.4.6 Charging

The MCID service interactions in permanent mode and temporary mode are described in this section.

For more information about the Charging service, refer to the following documents:

- *Diameter Communication Details in MTAS*
- *Diameter Offline Charging in MTAS*
- *Diameter Online Charging in MTAS*
- *MTAS Charging Management Guide*

Charging for MCID Service Use in Permanent Mode

The following service-specific Attribute-Value Pair (AVP) is included when performing terminating/originating session charging for a communication session to a user with the permanent mode in the MCID service:

- Supplementary Service Information Indicating use of MCID (permanent) or indicating use of Originating Permanent.

The following service-specific AVP is included when performing originating session charging for a communication session to a user with permanent mode MCID:

- Supplementary Service Information – indicating use of MCID (originating, permanent).

For offline charging, the AVP is included in the Accounting Request (ACR), Start Record, message generated for a successful communication session or in the ACR, Event Record, message generated for an unsuccessful communication session setup.

For online charging, the AVP is included in the Credit Control Request (CCR), Initial Request, message.



Charging for MCID Service Use in Temporary Mode

The following service-specific AVP is included when the temporary mode in the MCID service has successfully been started:

- Supplementary Service Information – indicating invocation of MCID (temporary)

The AVP is included in the ACR, *Event Record*, message generated for the successful SSC service invocation.





3 MCID Service Configuration

The Managed Object (MO) structure of the MCID service is illustrated in Figure 1. The *MtasMcid* MO is the child to the *MtasMmt* MO. The *MtasFunction* and *MtasMcid* MOs contain attributes that control the MCID service.

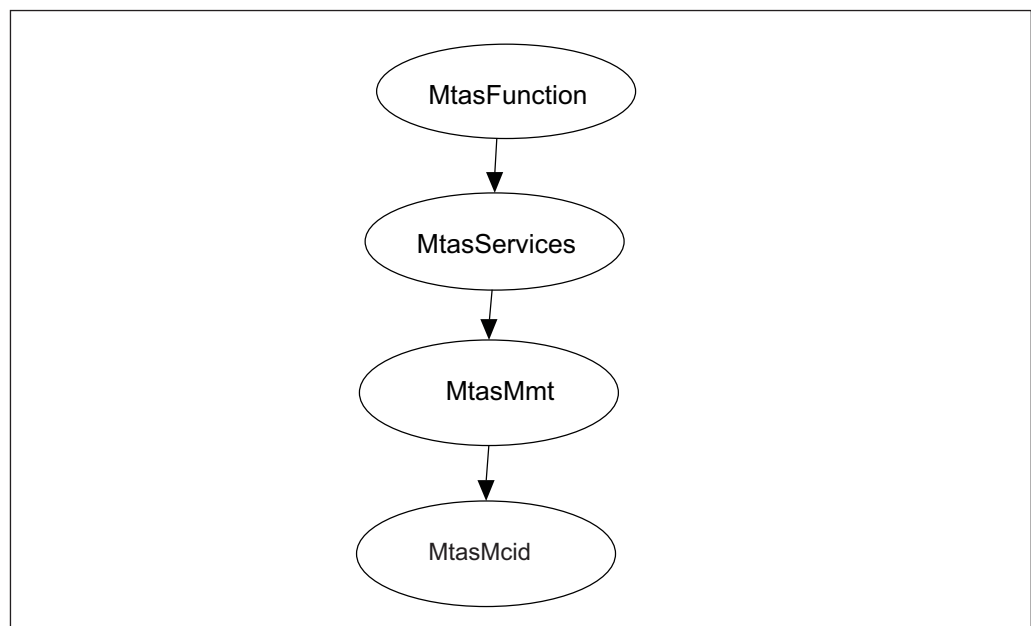


Figure 1 MCID MO Structure

3.1 MCID Administrative State Configuration

The MCID service is enabled by setting the `mtasMcidAdministrativeState` attribute in the *MtasMcid* MO to 1 (Unlocked). If the `mtasMcidAdministrativeState` is set to 0 (Locked), no MCID service is provided by the MTAS.

3.2 Reporting Method Configuration

The `mtasComDetailsReportingType` attribute defines two reporting methods:

- 0 Through CDS interface. The MCID information is sent to the Communication Details Server in a Diameter message format.
- 1 Local storage. The MCID information is stored locally on the node in ACR file format.

The *MtasComDetails* MO provides configuration attributes for Communication Details Reporting service. An overview of the *MtasComDetails* MO structure is shown in Figure 2.

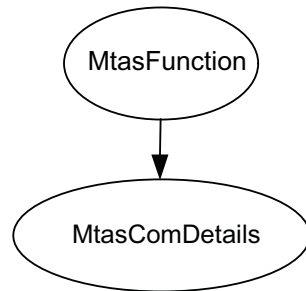


Figure 2 *MtasComDetails* MO Structure

3.3 CDS Configuration

The CDS is configured through the offline charging interface. In case CDS is not configured CDF can take over its role.

For more information about charging configuration, refer to *MTAS Charging Management Guide*.

3.4 Closure of ACR Files for Local Storage Configuration

An ACR file is closed when any of the following attributes are triggered:

- `mtasComDetailsLocalStorageMaxTime`
- `mtasComDetailsLocalStorageMaxNbrAcr`
- `mtasComDetailsLocalStorageMaxFileSize`

These attributes are only applied if the local storage of MCID information is enabled, that is, the `mtasComDetailsReportingType` attribute is set to 1.

3.5 Disk Full and Disk Not Full Percentage Levels Configuration

The attribute `mtasFunctionFullDiskPercentage` is used to define at which percentage level compared to full disk that the disk is considered to be full. When the full disk percentage level is reached, no more ACRs are stored on the file system of the node, and further requests to store ACRs are rejected.

The attribute `mtasFunctionNotFullDiskPercentage` is used to define at which percentage level compared to full disk that the state `diskfull` is changed to `enabled`, that is, more ACRs can be stored.



3.6 File Transfer

When the ACR files have been closed, they can be retrieved by using file transfer, as described in *File Management*.

3.7 Access Rights to Log Files and Directories Configuration

The system administrator can provide access rights, for example, read or write, to other users to the ACR files and directories where the files are stored. The access right is by default the node and platform super administrator accounts.

For more information about access to log files and directories, refer to *File Management*.

3.8 Service Data Configuration

This section describes how to configure the service data.

3.8.1 Operator Subscription Level Service Configuration

The permanent mode and temporary mode is set in the operator part of the subscriber data through the CAI3G protocol, refer to *MTAS CAI3G Interface*.

3.8.2 Subscriber Subscription Level Service Configuration

No service data for the MCID service is configured in the subscriber part of the subscriber data.

3.9 Announcement Configuration

The MCID-related announcements are handled through the SSC service.

For more information about announcement handling and attributes for the SSC service, refer to *MTAS Announcement Management Guide*.

3.10 Wholesale for MCID Configuration

The MCID service supports Wholesale. MCID is configurable on Virtual Telephony Provider level.



Wholesale for MCID is activated when the following attributes are set to 1 (Unlocked):

- The `vtasMcidAdministrativeState` attribute in the *VtasMcid* MO
- The `mtasMcidAdministrativeState` attribute in the *MtasMcid* MO

For more information about the Wholesale service, refer to *MTAS Wholesale Support Management Guide*.



4 Performance Management

Measurements related to the MCID service are detailed in *MTAS Performance Measurements*.

Note: The PM counters are not stepped when executing originating MCID.





5 Fault Management

There are no alarms related to this service.