

ST AS Malicious Communication Identity Service Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016. 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	Communication Details Information Capture and Report	3
2.2	ST MCID Subfunctions	4
2.3	ST MCID Interaction with Other Services	5
3	ST MCID Service Configuration	7
3.1	ST MCID Administrative State Configuration	7
3.2	Reporting Method Configuration	7
3.3	CDS Configuration	8
3.4	Closure of ACR Files for Local Storage Definition	8
3.5	Service Data Configuration	8
4	Performance Management	11
5	Fault Management	13





1 Introduction

This document describes how to configure the SIP Trunking Malicious Communication Identification (ST MCID) service in the ST AS.

It describes how to configure the Managed Objects (MOs) for the ST MCID service, how this service is co-located with other services in ST AS, and the interaction between them.

This document is intended for personnel configuring and fine-tuning the ST AS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area, in general.

1.1.1 Licenses

No license is required for the ST 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 ST MCID service is based on the 3GPP standards. The terminating MCID in permanent mode is supported in the ST AS. The service is executed at the terminating ST AS for the served Private Branch Exchange (PBX), and only the content of the initial `INVITE` requests is used for the communication identification purposes.

The captured ST MCID information is configured either to be reported to the Communication Details Server (CDS) through the `ComDetails` interface, or to be stored locally on the file system.

The `ComDetails` interface is based on the offline charging interface. The ST MCID information is reported in the `Communication-Details` Attribute-Value Pairs (AVPs) group in the `ACR[Event]` Diameter messages.

The local storage function is based on the Accounting-Request (ACR) Storage functionality. The ST MCID information is stored as ACR files that follow the ACR file format.

The ST MCID service is co-located with other services on ST AS, for example, ST Communication Diversion (ST CDIV), and ST Communication Barring (ST CB), but there is no direct interaction between them.

2.1 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.
- Coordinated Universal Time (UTC) time and date at which the initial `INVITE` request was received



- AS-type identifying the ST AS as the source

2.2 ST MCID Subfunctions

This section describes the subfunctions in the ST MCID.

2.2.1 Register Malicious Caller Permanent Mode

Subfunction Register Malicious Caller Permanent Mode is the action taken by the ST AS to register an incoming communication to a served user who has the permanent mode in the ST MCID.

2.2.2 Send ST MCID Information to CDS

Subfunction Send ST MCID Information to CDS is the action taken by the ST AS to send ST MCID information to a CDS.

2.2.3 Local Storage

The Local Storage 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*.

2.2.4 Configure Service

The ST MCID service is configured through the Operations, Administration, and Maintenance (OAM) interface. For more information, refer to *Managed Object Model (MOM)*.

2.2.5 Charging for ST MCID

For a description of charging for successful and unsuccessful communication sessions, refer to *Diameter Offline Charging in MTAS*.

For the following service, a specific AVP is included when performing terminating session charging for a communication session to a user with permanent mode ST MCID:



- Supplementary Service Information – indicating use of ST MCID (permanent mode).

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

2.3 ST MCID Interaction with Other Services

ST MCID has no service interactions in permanent mode.





3 ST MCID Service Configuration

The ST MCID service is controlled by the *MtasStMcid* MO. An overview of the ST MCID MO structure is shown in Figure 1.

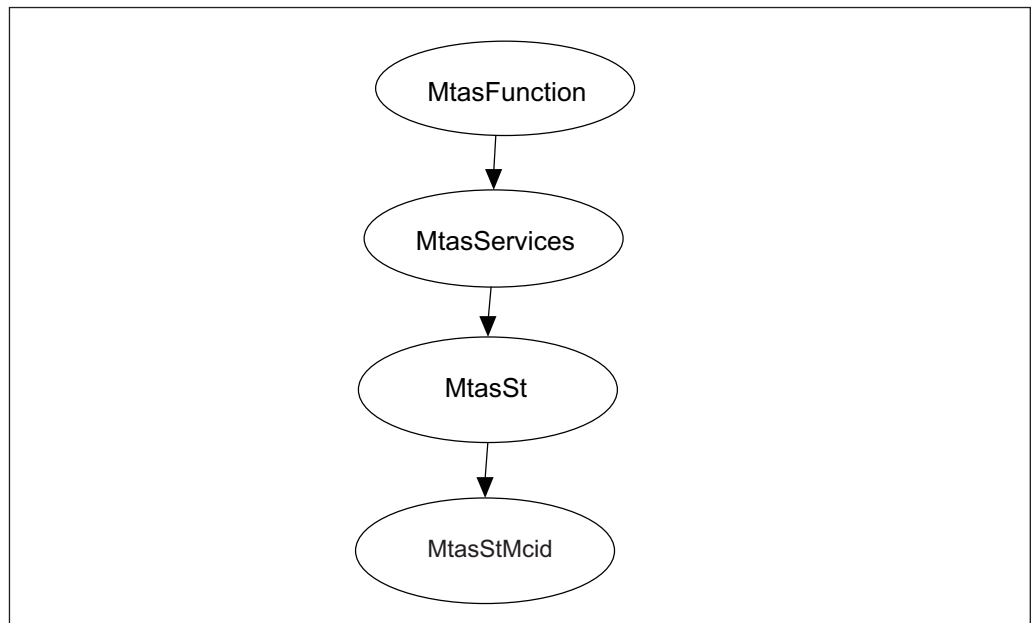


Figure 1 ST MCID MO Structure

3.1 ST MCID Administrative State Configuration

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

3.2 Reporting Method Configuration

The `MtasComDetailsReportingType` attribute defines the following two reporting methods:

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

The `MtasComDetails` MO provides configuration attributes for Communication Details Reporting service. The MO structure of `MtasComDetails` is shown in Figure 2.

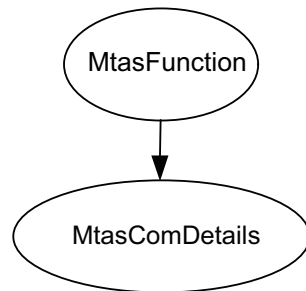


Figure 2 *MtasComDetails Structure*

3.3 CDS Configuration

The CDS is configured through the offline charging interface. If CDS is not configured, the Charging Data Function (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 Definition

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

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

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

3.5 Service Data Configuration

This section describes how to configure the service data.

3.5.1 Operator Subscription Level Service Configuration

The operator can provision or withdraw the ST MCID subscription for the PBX by setting the operator service data using the CAI3G protocol. The operator can also manage the list of PBX extension numbers that trigger the service. The service is triggered for any PBX extension number, if the list is empty.



For more information about the CAI3G protocol and the schema definition, refer to *MTAS CAI3G Interface for ST AS*.

3.5.2 Subscriber Subscription Level Service Configuration

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





4 Performance Management

For information on measurements related to the ST MCID service, refer to *Managed Object Model (MOM)*.





5 Fault Management

There are no alarms related to the ST MCID service.