Multi-Access Gateway – controller

Release 25.10

Log Events Reference Guide

3HE 21154 AAAC TQZZA
Edition: 01
October 2025

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

List of tables

1 Getting started

Find general information about this guide.

1.1 About this guide

This guide provides descriptions of event notifications that are forwarded to a destination such as a file or an SNMP trap. Properties that are reported include alarm or raising event name, raising condition, and clearing event information. The information is intended to assist with identifying and responding to the event notifications.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

The CLI trees and command descriptions can be found in the *MAG-c CLI Reference Guide*.

Note: This guide generically covers content for the release specified on the title page of the guide, and may also contain some content that will be released in later maintenance loads. See the applicable *MAG-c Release Notes* for information about features supported in each load of the software release.

Note: The information in this guide is intended to be used in conjunction with the SR OS software user guides. The SR OS software user guides describe SR OS service features that are supported by the MAG-c. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Documentation Suite Overview Card 20.10.R1* for specific guide titles.

1.2 Conventions

This section describes the general conventions used in this guide.

1.2.1 Precautionary and information messages

The following information symbols are used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step.
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
   a. This is one substep.
   b. This is another substep.

2 Log events overview

Log events have common elements or properties but are formatted in a way appropriate for the specific destination whether recorded to a file or sent as an SNMP trap.

Logs can be directed to memory, a console, a session, a local file, a syslog server, or an SNMP manager. All application-generated events have the following properties:

- a time stamp in UTC or local time
- the generating application
- a unique event ID within the application
- a router name identifying the VRF-ID that generated the event
- a subject identifying the affected object
- a short text description

See the associated SNMP notification definition in the SR OS MIBs for more information about the variables found in the message format strings.

The general format for a log event with either a memory, console, or file destination is as follows:

```
nnnn YYYY/MM/DD HH:MM:SS.SS TZONE <severity>: <application> #<event_id> <router-name>
  <subject>
<message>
```

The following is a log event example:

```
252 2013/05/07 16:21:00.76 UTC WARNING: SNMP #2005 Base my-interface-abc
"Interface my-interface-abc is operational"
```

The following table lists the specific elements that compose the general format.

Table 1: Log entry field descriptions

Label	Description
nnnn	The log entry sequence number
YYYY/MM/DD	The UTC or local date stamp for the log entry *YYYY* Year *MM* Month *DD* Date
HH:MM:SS.SS	The UTC time stamp for the event *HH* Hours (24-hour format) *MM* Minutes *SS.SS* Seconds

Label	Description
TZONE	The time zone (for example, UTC, EDT) as configured by the **configure log log-id** *x* **time-format** command
<severity>	The severity level of the event • CRITICAL • MAJOR • MINOR • WARNING • INFO • CLEARED
<application>	The name of the application generating the log message
<event_id>	The application's event ID number for the event
<router>	The router name representing the VRF-ID that generated the event; some examples include: Base, management, and vprn348
<subject>	The subject or affected object for the event
<message>	A text description of the event

The following table lists the sources that trigger an event.

Table 2: Log event sources

Event source	Description
Security events	Events pertaining to attempts to breach system security
Change events	Events pertaining to the configuration and operation of the node
Main events	Events pertaining to applications that are not assigned to other event categories or sources
Debug events	Events pertaining to trace or other debugging information

2.1 Viewing log events

- View all the log events.

```
show log event-control
```

Note:

- You can use this command and specify an application (for example, subscriber management).
- When an L precedes an event, it indicates that this event does not generate an SNMP notification.
- The event severity can be modified whether the event is generated or dropped.
- The severity of an SNMP trap is assigned by the SNMP manager.
- By default, all events are throttled at 2000 per second. System throttle or event-specific throttle can be modified.
- A maximum of 100 log IDs can be configured and filters can be used to specify the application, event ID, event severity, forward or drop the matching event, and so on, by applying those to a set of logs. Each log ID is configured by specifying an event source and the log destination.

Note: Logs with ID 99 and 100 are default logs directed to memory that contain the main events. The log with ID 100 has a filter applied to match events with severity greater than or equal to major.

Example

```
show log event-control
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P    g/s    Logged    Dropped
-------------------------------------------------------------------------------
APPLICATION_ASSURANCE:
   4401 tmnxBsxIsaAaGrpFailureV2          MA   thr         0          0
   4402 tmnxBsxIsaAaGrpFailureClearV2     WA   thr         0          0
<snip>
MOBILE_GATEWAY:
   2001 tmnxMobGwPathMgmtPeerState        WA   thr         0          0
   2002 tmnxMobGwDiameterPeerState        WA   thr         0          0
L  2003 tmnxMobGwCpmRestartUpdate         WA   thr         0          0
...
...
...
===============================================================================
```

- View a specific log event.

```
show log log-id log-id
```

Example

```
show log log-id 99
===============================================================================
Event Log 99
===============================================================================
Description : Default System Log
Memory Log contents [size=500 next event=183 (not wrapped)]
182 2017/09/12 18:46:25.66 EDT WARNING: SNMP #2005 Base xyz
"Interface xyz is operational"
```

```
181 2017/09/12 18:45:53.97 EDT WARNING: SNMP #2005 Base system
"Interface system is operational"
```

- View the log collector information.

```
show log log-collector
```

Example

```
show log log-collector
===============================================================================
Log Collectors
===============================================================================
Main                 Logged : 191                        Dropped : 0
  Dest Log Id: 99    Filter Id: 0       Status: enabled    Dest Type: memory
  Dest Log Id: 100   Filter Id: 1001    Status: enabled    Dest Type: memory
  Dest Log Id: 90    Filter Id: 0       Status: enabled    Dest Type: snmp
  Dest Log Id: 20    Filter Id: 100     Status: enabled    Dest Type: file
  Dest Log Id: 5     Filter Id: 0       Status: enabled    Dest Type: syslog
Security             Logged : 28 Dropped : 0
  Dest Log Id: 90    Filter Id: 0       Status: enabled    Dest Type: snmp
  Dest Log Id: 20    Filter Id: 100     Status: enabled    Dest Type: file
  Dest Log Id: 5     Filter Id: 0       Status: enabled    Dest Type: syslog
Change               Logged : 451 Dropped : 0
  Dest Log Id: 90    Filter Id: 0       Status: enabled    Dest Type: snmp
  Dest Log Id: 20    Filter Id: 100     Status: enabled    Dest Type: file
  Dest Log Id: 5     Filter Id: 0       Status: enabled    Dest Type: syslog
Debug                Logged : 0 Dropped : 0
LI                   Logged : 65 Dropped : 0
===============================================================================
```

- Create and configure filters.

```
configure log filter filter-id
```

Note: The MAG-c also supports log events generated by the 7750 SR OS. See the SR OS documentation for more information about the SNMP notifications from SR OS.

2.2 Log event configuration

2.2.1 Configuring SNMP as the log destination

You can specify SNMP as the destination for log events.

About this task

The MAG-c supports SNMPv1, SNMPv2, and SNMPv3 with the underlying system being based on SNMPv3. SNMPv1 and SNMPv2 are implemented by creating communities based on SNMPv3. Logical objects, for example VPRNs and interfaces, are assigned an index during the boot sequence based on their order in the configuration file. To maintain this index after a reboot, SNMP persistence must be enabled in the BOF. When enabled, and an **admin save** command is issued, the persistent indexes are stored in a `.ndx` file, which has the same name as the configuration file.

Procedure

Step 1. Enable persistent indexes in the BOF.

```
bof persist on
```

Step 2. Save the BOF.

```
bof save
```

Step 3. Configure the SNMP packet size.

```
configure system snmp packet-size bytes
```

Example

```
configure system snmp packet-size 9212
```

Step 4. Enable SNMP.

```
configure system snmp no shutdown
```

Step 5. Configure an SNMP community.

```
configure system security snmp community community-string access-permissions
 version version
```

Example

```
configure system security snmp community test rwa version v2c
```

Step 6. Save the configuration.

```
admin save
```

Step 7. View the SNMP status.

```
show system information
```

If the SNMP configuration is successful, the **SNMP Index Boot Status** field in the output of the command must indicate **Persistent**.

Example

```
# show system information
===============================================================================
System Information
===============================================================================
System Name            : cses-V20
System Type            : 7750 SR-12
Chassis Topology       : Standalone
System Version         : B-0.0.I2946
System Contact         :
System Location        :
System Coordinates     :
System Active Slot     : A
System Up Time         : 64 days, 18:33:04.70 (hr:min:sec)
```

```
Configuration-mode     : classic
Configuration-oper-mode: classic
SNMP Port              : 161
SNMP Engine ID         : 0000197f0000d814ff000000
SNMP Engine Boots      : 1
SNMP Max Message Size  : 1500
SNMP Admin State       : Enabled
SNMP Oper State        : Enabled
SNMP Index Boot Status : Persistent
SNMP Sync State        : N/A
...
...
...
===============================================================================
```

Step 8. View the SNMP counters used for requests, responses, and traps.

```
show snmp counters
```

Example

```
# show snmp counters
===============================================================================
SNMP counters:
===============================================================================
  in packets : 107
-------------------------------------------------------------------------------
    in gets : 46
    in getnexts : 0
    in getbulks : 0
    in sets : 61
  out packets: 107
-------------------------------------------------------------------------------
    out get responses : 107
    out traps : 0
  variables requested: 24
  variables set : 84
-------------------------------------------------------------------------------
  Failed requests due to lock being taken by netconf
    failed sets : 0
===============================================================================
```

2.2.2 Configuring an SNMP trap destination

An SNMP trap destination is a log with SNMP set as the destination.

About this task

In this example, the SNMP trap is configured as follows:

- log ID 90
- target name set to “manager”
- IP address 192.0.2.255
- SNMP version SNMPv2
- community name set to “community”

Procedure

Step 1. Create an SNMP trap group.

```
configure log snmp-trap-group log-id
```

Example

```
configure log snmp-trap-group 90
```

Step 2. Configure the SNMP trap group.

```
snmp-trap-group log-id trap-target name address ip-address [snmpv1|snmpv2|snmpv3]
 notify-community communityName|snmpv3SecurityName
```

Example

```
snmp-trap-group 90 trap-target “manager" address 192.0.2.255 snmpv2c notify-community
 community
```

Step 3. Create a log ID.

```
configure log log-id
```

Use the log ID configured for the SNMP trap group in step 1.

Example

```
configure log 90
```

Step 4. Configure the log ID.

```
log-id log-id to snmp size
```

Specify SNMP as the destination and the number of events.

Example

```
log-id 90 to snmp 3000
```

Step 5. View the configured SNMP trap destination.

```
show log snmp-trap-group log-id
```

Example

```
# show log snmp-trap-group 90
===============================================================================
SNMP Trap Groups
===============================================================================
id        name
  port      address
-------------------------------------------------------------------------------
90        manager
  162       192.0.2.255
===============================================================================
```

Note: By default, Nokia NSP NFM-P uses log ID 98.

2.2.3 Configuring a file as the log destination

You can specify a file as the log destination.

About this task

The filename follows the format `logeeff-timestamp`, where:

ee	The log ID (*log-id*)
ff	The file ID (*log-file-id*)

In this example, the destination file is configured as follows:

- file ID 10
- storage location CF1:
- rollover of records 1440 minutes and retention 168 hours
- linked to log ID 20, which receives event logs from the main, security, and changed source streams (see Table 2: Log event sources)
- log ID 20 directed to file ID 10

Procedure

Step 1. Create a log file.

```
configure log file-id log-file-id
```

Example

```
configure log file-id 10
```

Step 2. Configure the storage location of the log file.

```
configure log file-id log-file-id location
```

Example

```
configure log file-id 10 location cf1:
```

Step 3. Configure the rollover and retention duration of the log file.

```
configure log file-id log-file-id rollover minutes [retention] hours
```

Example

```
configure log file-id 10 rollover 1440 retention 168
```

Step 4. Create a log ID.

```
configure log log-id
```

Example

```
configure log 20
```

Step 5. Configure the source streams for the log ID.

```
configure log log-id from
```

Example

```
configure log 20 from main security change
```

Step 6. Configure the destination type of the log.

```
configure log log-id to file log-file-id
```

Example

```
configure log 20 to file 10
```

2.2.4 Configuring a syslog as the log destination

You can specify a syslog as the log destination.

About this task

In this example, the syslog is configured as follows:

- syslog ID 5
- syslog host address 10.10.1.1
- linked to log ID 5, which receives event logs from the main, security, and changed source streams (see Table 2: Log event sources)

Procedure

Step 1. Create a syslog.

```
configure log syslog syslog-id
```

Example

```
configure log syslog 5
```

Step 2. Configure the storage location of the syslog.

```
configure log syslog syslog-id address ip-address
```

Example

```
configure log syslog 5 address 10.10.1.1
```

Step 3. Create a log ID.

```
configure log log-id
```

Example

```
configure log 5
```

Step 4. Configure the source streams for the log ID.

```
configure log log-id from
```

Example

```
configure log 5 from main security change
```

Step 5. Configure the destination type of the log ID.

```
configure log log-id to syslog syslog-id
```

Example

```
configure log 5 to syslog 5
```

2.2.5 Debugging an application

You can debug an application using a log with the debug trace specified as the event source. Although you can debug an application in the current session window, using a log as the destination is more useful for reviewing the log.

About this task

Note: The steps in this section only describe the procedure for configuring a log file that stores the output of debug commands. See the *MAG-c Control Plane Function Guide* for more information about how to enable and use the **call-insight** and PDN **debug** commands.

In this example, application debugging is configured as follows:

- file ID 10
- storage location CF2:
- linked to log ID 30, which receives event logs from the debug trace (see Table 2: Log event sources)
- log ID 30 directed to file ID 10

Caution: Debug commands must be used with caution. Nokia recommends disabling debugging after any debug operation has been finished. The **no debug** command disables all the enabled debug commands.

Procedure

Step 1. Create a log file.

```
configure log file-id log-file-id
```

Example

```
configure log file-id 10
```

Step 2. Configure the storage location of the log file.

```
configure log file-id log-file-id location
```

Example

```
configure log file-id 10 location cf2:
```

Step 3. Create a log ID.

```
configure log log-id
```

Example

```
configure log 30
```

Step 4. Configure the source stream for the log ID.

```
configure log log-id from
```

Example

```
configure log 30 from debug-trace
```

Step 5. Configure the destination type of the log.

```
configure log log-id to file log-file-id
```

Example

```
configure log 30 to file 10
```

2.3 Sample log event

In this guide, each log event is described in a separate table.

The following table contains a sample log event entry for the tmnxMobGwBngLockoutLimitExceeded log event.

Table 3: tmnxMobGwBngLockoutLimitExceeded properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2007
Event name	tmnxMobGwBngLockoutLimitExceeded
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.120
Default severity	warning
Source stream	main
Message format string	The maximum number of BNG sessions in locked-out or monitored state is exceeded *$tmnxMobGwNtfyInformation$*
Cause	While the maximum number of BNG sessions in monitored or locked-out state is in use, a new session must be monitored or locked out.
Effect	Another session being monitored or locked out is prematurely released to accommodate the new session.
Recovery	Recovery is not necessary.

The table title for a log event entry is the event name. Each entry contains the information described in the following table.

Table 4: Log entry field descriptions

Label	Description
Application name	The name of the application generating the log message
Event ID	The application event ID number for the event
Event name	The name of the event
SNMP notification prefix and OID	The prefix and OID of the SNMP notification associated with the log event
Default severity	The default severity level of the event • CRITICAL • MAJOR • MINOR • WARNING • INFO • CLEARED

Label	Description
Source stream	The event source • main • security • change • debug See Table 2: Log event sources for more information.
Message format string	A text description of the event
Cause	The cause of the event
Effect	The effect of the event
Recovery	How to recover from this event, if necessary

3 Log events

Get a summary of the supported alarms and raising events and detailed descriptions per alarm and event object.

3.1 MC_REDUNDANCY

3.1.1 tmnxMcMobileBothLockedToMaster

Table 5: tmnxMcMobileBothLockedToMaster properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	5002
Event name	tmnxMcMobileBothLockedToMaster
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcMobRedundancy Notifications.6
Default severity	minor
Source stream	main
Message format string	For peers *$tmnxMcPeerIpAddrForNotify$* and *$tmnxMcPeerSrcIpAddr $* both nodes locked to the active operational role
Cause	A misconfiguration occurred because enabling the mc-master-lock on both the primary and secondary geo-redundancy nodes is only permitted when the mc-mobile link between these nodes is down, and both nodes have assumed the active operational role. When the mc-mobile link is restored (reaches the UP state), the system triggers a tmnxMcMobileBothLockedToMaster notification indicating that both the primary and secondary nodes are locked in the active operational role. However, when the mc-mobile link between the geo-redundancey nodes is operationally UP and peering is successful, the mc-master-lock CLI configuration is restricted to the node with the active operational role.
Effect	The geo-redundancy link is not established because peering of these nodes is not possible.
Recovery	Diagnose and fix the mc-master-lock misconfiguration.

3.1.2 tmnxMcMobileGeoRedChgInfo

Table 6: tmnxMcMobileGeoRedChgInfo properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	2040
Event name	tmnxMcMobileGeoRedChgInfo
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcMobRedundancy Notifications.2
Default severity	major
Source stream	main
Message format string	Gw- *$tmnxMcPeerMobileMGId$* ,Src Address- *$tmnxMcPeerSrcIpAddr $*, CPM Geo-Red State-*$tmnxMcPeerMobileMGCPMGeoRedState $*, Mob GW Geo Red State- *$tmnxMcPeerMobileMGGeoRedState $*, Number of Hot Groups-*$tmnxMcPeerMobileMGNumHotGroups$* (*$tmnxMcPeerMGHotGroupList$*), Number Of Warm Groups- *$tmnx McPeerMobileMGNumWarmGroups$* (*$tmnxMcPeerMGWarmGroup List$*), Number Of Cold Groups-*$tmnxMcPeerMobileMGNumCold Groups$* (*$tmnxMcPeerMGColdGroupList$*), Peer Address-*$tmnx McPeerIpAddr$*, Peer State-*$tmnxMcPeerMobileMGPeerState$*, Peer State Reason- *$tmnxMcPeerMobileMGPeerStChgRsn$*
Cause	The chassis or the CPM changed its geo-redundancy state, or the peer connection status changed.
Effect	If the chassis or CPM state changes to cold or warm, or the peer state is disconnected, the system is no longer in a geo-redundant state.
Recovery	Diagnose the cause of the state change, restore the UP state for the peer, the peer link, or both, and ensure the chassis and the CPM geo-redundancy are in the hot state.

3.1.3 tmnxMcMonitorMcIcrAlarm

Table 7: tmnxMcMonitorMcIcrAlarm properties

Property name	Value
Application name	MC_REDUNDANCY
Event ID	5001

Property name	Value
Event name	tmnxMcMonitorMcIcrAlarm
SNMP notification prefix and OID	TIMETRA-MC-REDUNDANCY-MIB.tmnxMcMobRedundancy Notifications.5
Default severity	minor
Source stream	main
Message format string	The monitor-mc-icr alarm occurred on interface *$vRtrIfIndex$* for the reason *$tmnxMcMonitorMcIcrAlarmRsnCode$*.
Cause	The alarm was generated with the following reason codes: 1. 'tmnx McMonitorMcIcrAlarmRsnCode trafficDetected' - the reference point traffic detected on the standby node reaches the configured monitor-mc-redirect high threshold vRtrIfMonMcRedirectHighThresh. 2. 'tmnx McMonitorMcIcrAlarmRsnCode trafficCleared' - the reference point traffic is below the configured monitor-mc-redirect low threshold vRtr IfMonMcRedirectLowThresh.
Effect	A network configuration issue or a partial network failure is detected.
Recovery	Diagnose and fix the issue or the partial network failure.

3.2 MOBILE_CUPS_BNG

3.2.1 tmnxMobBngStaticSeOperStateUp

Table 8: tmnxMobBngStaticSeOperStateUp properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2012
Event name	tmnxMobBngStaticSeOperStateUp
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.150
Default severity	warning
Source stream	main
Message format string	Static session *$tmnxMobGwNtfySessionName$* is *$tmnxMobGwNtfy TruthValue$*operational
Cause	The operational state of a static CUPS BNG session changed.

Property name	Value
Effect	When the operational state of a static CUPS BNG session is down, the system disconnects the user associated with the session.
Recovery	The recovery action depends on the cause.

3.2.2 tmnxMobGwBngLockoutLimitExceeded

Table 9: tmnxMobGwBngLockoutLimitExceeded properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2007
Event name	tmnxMobGwBngLockoutLimitExceeded
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.120
Default severity	warning
Source stream	main
Message format string	The maximum number of BNG sessions in locked-out or monitored state is exceeded *$tmnxMobGwNtfyInformation$*
Cause	A new session is monitored or locked out when the maximum number of monitored or locked-out BNG sessions is already in use.
Effect	The system prematurely releases a currently monitored or locked-out BNG session to accommodate the new session.
Recovery	Recovery is not necessary.

3.2.3 tmnxMobGwBngNatPrefixRevocation

Table 10: tmnxMobGwBngNatPrefixRevocation properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2009
Event name	tmnxMobGwBngNatPrefixRevocation
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.133

Property name	Value
Default severity	minor
Source stream	main
Message format string	CUPS BNG NAT Prefix revocation : MSCP *$tmnxMobGwNtfyMscpId $* Realm *$tmnxMobGwNtfyNwRealmName$* pool *$tmnxMobGwNtfy PoolName$* Gw *$tmnxMobGwNtfyGatewayId$*, UP *$tmnxMobGwNtfy UpPeerAddress$*, prefix *$tmnxMobGwNtfyAddr$*/*$tmnxMobGwNtfyPfx Length$*, reason ' *$tmnxMobGwNtfyRevocationReason$*'
Cause	An error occurred during a NAT audit between MSCP and OAM or MSCP and ODSA, and the system cannot acknowledge the prefix.
Effect	The session is deleted. [RECOVERY]
Recovery	N/A

3.2.4 tmnxMobGwBngResFsgUpfChange

Table 11: tmnxMobGwBngResFsgUpfChange properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2010
Event name	tmnxMobGwBngResFsgUpfChange
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.134
Default severity	warning
Source stream	main
Message format string	UP resiliency: UP change: Gw *$tmnxMobGwNtfyGatewayId$*, UP group *$tmnxMobGwNtfyCupsBngUpGroup$*, FSG *$tmnxMobGwNtfy FsgId$*, primary UP *$tmnxMobGwNtfyUpf1$* (health *$tmnxMobGwNtfy Upf1Health$*), secondary UP *$tmnxMobGwNtfyUpf2$* (health *$tmnx MobGwNtfyUpf2Health$*), previous primary UP *$tmnxMobGwNtfy Upf1Prev$*, previous secondary UP *$tmnxMobGwNtfyUpf2Prev$*
Cause	The value changed for TIMETRA-MOBILE-PDN-CUPS-MIB::tmnxMob PdnBngResFsgActUpf or TIMETRA-MOBILE-PDN-CUPS-MIB::tmnx MobPdnBngResFsgStdbyUpf.
Effect	If the primary UPF changes, the traffic associated with this fate sharing group (FSG) goes through another UPF. If the secondary UPF changes and the pair is in hot-standby mode, another UPF tracks the session state. .

Property name	Value
Recovery	No recovery actions are required.

3.2.5 tmnxMobGwBngResFsgUpfError

Table 12: tmnxMobGwBngResFsgUpfError properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2011
Event name	tmnxMobGwBngResFsgUpfError
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.149
Default severity	warning
Source stream	main
Message format string	UP resiliency: UP error: Gw *$tmnxMobGwNtfyGatewayId$*, UP group *$tmnxMobGwNtfyCupsBngUpGroup$*, FSG *$tmnxMobGwNtfyFsgId$*, *$tmnxMobGwNtfyTruthValue$* UP *$tmnxMobGwNtfyUpf1$*: *$tmnxMobGwNtfyError$$tmnxMobGwNtfyInformation$*
Cause	The UP reported an error when the system, acting as a CUPS Control Plane (CP), requested a UP to modify (create, delete, or change) an FSG.
Effect	If the UP is active for the FSG, the system transfers the active role to the previously active UP.
Recovery	No recovery actions are required.

3.2.6 tmnxMobGwBngSessCreateUpfNonResp

Table 13: tmnxMobGwBngSessCreateUpfNonResp properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2002
Event name	tmnxMobGwBngSessCreateUpfNonResp
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.106

Property name	Value
Default severity	minor
Source stream	main
Message format string	CUPS BNG Session create UP non-response for: Gw *$tmnxMobGwNtfyGatewayId$*, VRtr *$tmnxMobGwNtfyVrtrId$*, UP *$tmnxMobGwNtfyUpPeerAddress$*, node-ID *$tmnxMobGwNtfyPeerNodeId$*, session key: L2-access-id *$tmnxMobGwNtfyCupsBngSessKeyL2Acc$*, s-vlan *$tmnxMobGwNtfyCupsBngSessKeySVlan$*, c-vlan *$tmnxMobGwNtfyCupsBngSessKeyCVlan$*, mac *$tmnxMobGwNtfyCupsBngSessKeyMac$*, circuit-id '0x*$tmnxMobGwNtfyCupsBngSessKeyCirId$*', remote-id '0x *$tmnxMobGwNtfyCupsBngSessKeyRemId$*'
Cause	The UP did not send a response message to acknowledge a Create Session Request.
Effect	The CP cancels the session setup and the UP may have a lingering session state.
Recovery	The operator's assistance is needed to remove any session state lingering on the UP.

3.2.7 tmnxMobGwBngSessDuplAttr

Table 14: tmnxMobGwBngSessDuplAttr properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2008
Event name	tmnxMobGwBngSessDuplAttr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.132
Default severity	minor
Source stream	main
Message format string	CUPS BNG Session setup duplicate session identification attribute detected: Gw *$tmnxMobGwNtfyGatewayId$*, VRtr *$tmnxMobGwNtfyVrtrId$*, UP *$tmnxMobGwNtfyUpPeerAddress$*, node-ID *$tmnxMobGwNtfyPeerNodeId$*, L2-access-id *$tmnxMobGwNtfyCupsBngSessKeyL2Acc$*, s-vlan *$tmnxMobGwNtfyCupsBngSessKeySVlan$*, c-vlan *$tmnxMobGwNtfyCupsBngSessKeyCVlan$*, mac *$tmnxMobGwNtfyCupsBngSessKeyMac$*, circuit-id '0x*$tmnxMobGwNtfyCupsBngSessKeyCirId$*', remote-id '0x *$tmnxMobGwNtfyCupsBngSessKeyRemId$*', up-group '*$tmnxMobGwNtfyCupsBngUpGroup$*'

Property name	Value
Cause	A session setup used attributes that conflict with unique session identification attributes, or attribute combinations of other active sessions.
Effect	The session is not available for external targeting based on session attribute identification.
Recovery	In case external targeting capability is required, the operator's assistance is needed to clear the session.

3.2.8 tmnxMobGwBngSessTermBySystem

Table 15: tmnxMobGwBngSessTermBySystem properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2001
Event name	tmnxMobGwBngSessTermBySystem
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.105
Default severity	warning
Source stream	main
Message format string	CUPS BNG session terminated by the system: Reason *$tmnxMobGwNtfyCupsBngSessTermReas$*, extra info '*$tmnxMobGwNtfyCupsBngSessTermInfo$*', Gw *$tmnxMobGwNtfyGatewayId$*, VRtr *$tmnxMobGwNtfyVrtrId$*, UP-ip *$tmnxMobGwNtfyUpPeerAddress$*, L2-access-id *$tmnxMobGwNtfyCupsBngSessKeyL2Acc$*, s-vlan *$tmnxMobGwNtfyCupsBngSessKeySVlan$*, c-vlan *$tmnxMobGwNtfyCupsBngSessKeyCVlan$*, mac *$tmnxMobGwNtfyCupsBngSessKeyMac$*, circuit-id '0x *$tmnxMobGwNtfyCupsBngSessKeyCirId$*', remote-id '0x*$tmnxMobGwNtfyCupsBngSessKeyRemId$*', up-group ' *$tmnxMobGwNtfyCupsBngUpGroup$*'
Cause	The system found a reason indicated by tmnxMobGwNtfyCupsBngSessTermReas for terminating a session.
Effect	The established session is terminated or the session being set up is cancelled.
Recovery	None.

3.2.9 tmnxMobGwBngSubscriberCreate

Table 16: tmnxMobGwBngSubscriberCreate properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2003
Event name	tmnxMobGwBngSubscriberCreate
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.111
Default severity	warning
Source stream	main
Message format string	CUPS BNG new subscriber created: Sub-Id '*$tmnxMobGwNtfyCupsBngSubId$*', externally assigned alias (if any) ' *$tmnxMobGwNtfyCupsBngSubExtAlias$*, UP IP *$tmnxMobGwNtfyAddr$*'
Cause	A session setup, for which there wasn't any subscriber state yet, is successful.
Effect	The subscriber state is created.
Recovery	Not applicable.

3.2.10 tmnxMobGwBngSubscriberDelete

Table 17: tmnxMobGwBngSubscriberDelete properties

Property name	Value
Application name	MOBILE_CUPS_BNG
Event ID	2004
Event name	tmnxMobGwBngSubscriberDelete
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.112
Default severity	warning
Source stream	main
Message format string	CUPS BNG subscriber deleted: Sub-Id '*$tmnxMobGwNtfyCupsBngSubId$*', externally assigned alias (if any) ' *$tmnxMobGwNtfyCupsBngSubExtAlias$*, UP IP *$tmnxMobGwNtfyAddr$*'

Property name	Value
Cause	The last session of an active subscriber was terminated.
Effect	The subscriber state is deleted.
Recovery	Not applicable.

3.3 MOBILE_GATEWAY

3.3.1 tmnxMcRedundancyTrafficReceived

Table 18: tmnxMcRedundancyTrafficReceived properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2084
Event name	tmnxMcRedundancyTrafficReceived
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.82
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Ref point-*$tmnxMobGwNtfy RefPointType$*, RefPointName- *$tmnxMobGwNtfyRefPointName$*, InterfaceType-*$tmnxMobGwNtfyIfType$*.
Cause	Traffic was detected at the ICR node because of a network issue.
Effect	Traffic coming to the ICR node is dropped if shunting is not used, or forwarded accordingly if shunting is used.
Recovery	Check the cause of the routing change in the network, and fix it if possible. If the traffic cannot be directed back, but the routing works towards the node, perform an ICR switchover.

3.3.2 tmnxMobDbRedRoleActive

Table 19: tmnxMobDbRedRoleActive properties

Property name	Value
Application name	MOBILE_GATEWAY

Property name	Value
Event ID	2151
Event name	tmnxMobDbRedRoleActive
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.153
Default severity	warning
Source stream	main
Message format string	Database *$tmnxMobDbId$* with IP address *$tmnxMobDbIpAddr$* is now active
Cause	The redundancy role of a database changed from standby to active.
Effect	The database is actively used.
Recovery	Not applicable.

3.3.3 tmnxMobDbStatusChanged

Table 20: tmnxMobDbStatusChanged properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2152
Event name	tmnxMobDbStatusChanged
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.154
Default severity	minor
Source stream	main
Message format string	Database *$tmnxMobDbId$* with IP address *$tmnxMobDbIpAddr$* is now *$tmnxMobDbStatus$*
Cause	The state of a database changed.
Effect	When the new state is 'up', the connection with the database is available. When the new state is 'down', the connection with the database is not available.
Recovery	If the new state is 'down' and there is no subsequent 'tmnxMobDbRed RoleActive' notification, an ICR switchover is recommended.

3.3.4 tmnxMobGwApnMaxAttachLmtAlrm

Table 21: tmnxMobGwApnMaxAttachLmtAlrm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2124
Event name	tmnxMobGwApnMaxAttachLmtAlrm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.124
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, APN Name- *$tmnxMobGwNtfyApnName$*, attach request rate reached maximum limit.
Cause	The GTP-based attach rate exceeded the configurable max-session-attach limit for tmnxMobGwNtfyApnName.
Effect	If there is a new GTP-based attach session and the attach rate has been exceeded, the new attach session is rejected.
Recovery	The alarm will be cleared when the rate goes back below the max-session-attach limiti value.

3.3.5 tmnxMobGwApnMaxAttachLmtAlrmClr

Table 22: tmnxMobGwApnMaxAttachLmtAlrmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2125
Event name	tmnxMobGwApnMaxAttachLmtAlrmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.125
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, APN Name- *$tmnxMobGwNtfyApnName$*, attach request rate goes below maximum limit.

Property name	Value
Cause	The GTP-based attach rate dropped below the configurable max-session-attach limit for this tmnxMobGwNtfyApnName.
Effect	The GTP-based attach rate drops below the configured max-session-attach limit value.
Recovery	No further action is required.

3.3.6 tmnxMobGwAssociationPeerState

Table 23: tmnxMobGwAssociationPeerState properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2075
Event name	tmnxMobGwAssociationPeerState
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.73
Default severity	minor
Source stream	main
Message format string	Association state changed to *$tmnxMobGwNtfyPeerAssociatnState$* for *$tmnxMobGwNtfySigPlaneType$* Peer *$tmnxMobGwNtfyPeerNodeId$* on GW *$tmnxMobGwNtfyGatewayId$* Reference Point *$tmnxMobGwNtfyRefPointType$ $tmnxMobGwNtfyRefPointName$* (IP Address: *$tmnxMobGwNtfyRfPtPeerAddr$*). Recovery Time: *$tmnxMobGwNtfyRecoveryTimestamp$* cp func *$tmnxMobGwNtfyPeerCPFuncFeatures$* up func *$tmnxMobGwNtfyPeerUPFuncFeatures$* bbf up func *$tmnxMobGwNtfyPeerBbfUPFuncFeats$*
Cause	The Association state changed when the association is set up or released. The association can be set up or released by association-related node-level messages triggered by either the gateway or the peer. The gateway initiates Association Messages if the peer is configured in the association peer list.
Effect	Path management for PFCP peers and UPF selection can occur after the association is established. Path management or UPF selection does not happen if the association state is down.
Recovery	If the association state is down when the gateway initiates a release, the gateway state must come up for the association to be reestablished. If the release was initiated by the peer, the peer triggers the setup when it comes up again.

3.3.7 tmnxMobGwAssocNodeIdFail

Table 24: tmnxMobGwAssocNodeIdFail properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2121
Event name	tmnxMobGwAssocNodeIdFail
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.121
Default severity	major
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, epc-node not configured for *$tmnxMobGwPdnNtfySxAssociation$*
Cause	A PFCP Association Setup procedure failed because of a missing node ID.
Effect	The PFCP Association Setup procedure continues to fail while the node ID is missing.
Recovery	Configure a valid string for the configure mobile-gateway pdn epc-node command.

3.3.8 tmnxMobGwAssocNodeIdFailClr

Table 25: tmnxMobGwAssocNodeIdFailClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2123
Event name	tmnxMobGwAssocNodeIdFailClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.123
Default severity	major
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, configured epc-node re-established for *$tmnxMobGwPdnNtfySxAssociation$*

Property name	Value
Cause	PFCP Association Setup re-established after the node ID became available.
Effect	There is no effect for this notification.
Recovery	No further action is required.

3.3.9 tmnxMobGwAssocNodeIdMismatch

Table 26: tmnxMobGwAssocNodeIdMismatch properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2143
Event name	tmnxMobGwAssocNodeIdMismatch
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.143
Default severity	major
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, node ID mismatched for *$tmnx MobGwPdnNtfySxAssociation$* PFCP association setup
Cause	A PFCP Association Setup failed to establish because a mismatch occurred between the provided node ID and the configured PFCP association peer list.
Effect	The PFCP Association Setup procedure continues to fail while the provided node ID does not match an entry in the association peer list.
Recovery	Ensure there is a valid entry in the peer list configuration that matches the node ID in the PFCP association.

3.3.10 tmnxMobGwAssocNodeIdMismatchClr

Table 27: tmnxMobGwAssocNodeIdMismatchClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2144

Property name	Value
Event name	tmnxMobGwAssocNodeIdMismatchClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.144
Default severity	cleared
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, node ID match found for *$tmnx MobGwPdnNtfySxAssociation$* PFCP association
Cause	A PFCP Association Setup was re-established after the provided node ID matched a valid peer list configuration.
Effect	The PFCP Association Setup is established.
Recovery	No further action is required.

3.3.11 tmnxMobGwAssocPfcpNdIdIpTypErClr

Table 28: tmnxMobGwAssocPfcpNdIdIpTypErClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2146
Event name	tmnxMobGwAssocPfcpNdIdIpTypErClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.146
Default severity	cleared
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, PFCP node ID IP type match occurred after a prior mismatch for *$tmnxMobGwPdnNtfySxAssociation $* PFCP association
Cause	A PFCP Association Setup was re-established after the provided node ID IP-type value matched a valid Sx reference point peer interface address configuration.
Effect	The PFCP Association Setup is established.
Recovery	No further action is required.

3.3.12 tmnxMobGwAssocPfcpNodeIdIpTypErr

Table 29: tmnxMobGwAssocPfcpNodeIdIpTypErr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2145
Event name	tmnxMobGwAssocPfcpNodeIdIpTypErr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.145
Default severity	major
Source stream	main
Message format string	Gw - *$tmnxMobGwNtfyGatewayId$*, pfcp node ID IP type mismatched for *$tmnxMobGwPdnNtfySxAssociation$* PFCP association
Cause	A PFCP Association Setup procedure failed because of a mismatch between the provided node ID IP-type value and the configured interface address types for all Sx reference point entries.
Effect	The PFCP Association Setup procedure continues to fail while the provided PFCP node ID IP-type continues to mismatch any address in all the Sx reference point interface configurations.
Recovery	Provide a valid node ID IP-type configuration in the TIMETRA-MOBILE-PDN-MIB::tmnxMobPdnPfcpNodeIdIpType, or create an equivalent IP-type address interface for the Sx reference point configuration.

3.3.13 tmnxMobGwBngChfFailAlmClr

Table 30: tmnxMobGwBngChfFailAlmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2156
Event name	tmnxMobGwBngChfFailAlmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.158
Default severity	major
Source stream	main

Property name	Value
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the CHF failure handling threshold alarm is cleared because upper limit of *$tmnxMobGwNtfyFhAlarm LowerThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$*
Cause	The lower limit of the CHF failure handling threshold was reached.
Effect	Enough sessions (determined by the threshold) recover from failure handling and are once again being charged as intended.
Recovery	Not applicable.

3.3.14 tmnxMobGwBngChfFailAlmSet

Table 31: tmnxMobGwBngChfFailAlmSet properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2155
Event name	tmnxMobGwBngChfFailAlmSet
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.157
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the CHF failure handling threshold alarm is set because upper limit of *$tmnxMobGwNtfyFhAlarmUpperThr $*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMob GwNtfyVmId$*
Cause	The upper limit of the CHF failure handling threshold was reached.
Effect	A significant number of sessions (determined by the threshold) enter failure handling, and those sessions are not being charged as intended.
Recovery	Restore the CHF servers to provide full connectivity and functionality.

3.3.15 tmnxMobGwBngPcfFailAlmClr

Table 32: tmnxMobGwBngPcfFailAlmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2158
Event name	tmnxMobGwBngPcfFailAlmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.160
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the PCF failure handling threshold alarm is cleared because upper limit of *$tmnxMobGwNtfyFhAlarm LowerThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$*
Cause	The lower limit of the PCF failure handling threshold was reached.
Effect	Enough sessions (determined by the threshold) recover from failure handling and are once again subject to PCF policy management.
Recovery	Not applicable.

3.3.16 tmnxMobGwBngPcfFailAlmSet

Table 33: tmnxMobGwBngPcfFailAlmSet properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2157
Event name	tmnxMobGwBngPcfFailAlmSet
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.159
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the PCF failure handling threshold alarm is set because upper limit of *$tmnxMobGwNtfyFhAlarmUpperThr*

Property name	Value
	$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$
Cause	The upper limit of the PCF failure handling threshold was reached.
Effect	A significant number of sessions (determined by the threshold) enter failure handling, and those sessions are not subject to PCF policy management.
Recovery	Restore the PCF servers to provide full connectivity and functionality.

3.3.17 tmnxMobGwBngUdmSdmFailAlmClr

Table 34: tmnxMobGwBngUdmSdmFailAlmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2160
Event name	tmnxMobGwBngUdmSdmFailAlmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.162
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the UDM SDM failure handling threshold alarm is cleared because upper limit of *$tmnxMobGwNtfyFhAlarmLowerThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$*
Cause	The lower limit of the UDM failure handling threshold was reached.
Effect	Enough sessions (determined by the threshold) have recovered from failure handling and are once again using UDM subscription parameters.
Recovery	Not applicable.

3.3.18 tmnxMobGwBngUdmSdmFailAlmSet

Table 35: tmnxMobGwBngUdmSdmFailAlmSet properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2159
Event name	tmnxMobGwBngUdmSdmFailAlmSet
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.161
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the UDM SDM failure handling threshold alarm is set because upper limit of *$tmnxMobGwNtfyFhAlarmUpperThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$*
Cause	The upper limit of the UDM failure handling threshold was reached.
Effect	A significant number of sessions (determined by the threshold) enter failure handling and are not using UDM subscription parameters.
Recovery	Restore the UDM servers to provide full connectivity and functionality.

3.3.19 tmnxMobGwBngUdmUecmFailAlmClr

Table 36: tmnxMobGwBngUdmUecmFailAlmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2162
Event name	tmnxMobGwBngUdmUecmFailAlmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.164
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the UDM UECM failure handling threshold alarm is cleared because upper limit of *$tmnxMobGwNtfy*

Property name	Value
	FhAlarmLowerThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$
Cause	The lower limit of the UDM UECM failure handling threshold was reached.
Effect	Enough sessions (determined by the threshold) recover from failure handling, and for those sessions, the MAG-c is registered as the serving SMF.
Recovery	Not applicable.

3.3.20 tmnxMobGwBngUdmUecmFailAlmSet

Table 37: tmnxMobGwBngUdmUecmFailAlmSet properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2161
Event name	tmnxMobGwBngUdmUecmFailAlmSet
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.163
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, the UDM UECM failure handling threshold alarm is set because upper limit of *$tmnxMobGwNtfyFhAlarmUpperThr$*% is reached for APN *$tmnxMobGwNtfyApnName$* on VM-*$tmnxMobGwNtfyVmId$*
Cause	The upper limit of the UDM UECM failure handling threshold was reached.
Effect	A significant number of sessions (determined by the threshold) enter failure handling, and for those sessions, the MAG-c is not registered as the serving SMF.
Recovery	Restore the UDM servers to provide full connectivity and functionality.

3.3.21 tmnxMobGwCfCapacityAlarmMinor

Table 38: tmnxMobGwCfCapacityAlarmMinor properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2011
Event name	tmnxMobGwCfCapacityAlarmMinor
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.7
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Flash ID- *$tmnxMobGwNtfyFlash Id$*, Flash Limit-*$tmnxMobGwNtfyCfLimit$*, GTP Prime Server Group-*$tmnxMobGwNtfyGtpPriGrpName$*.
Cause	The compact flash capacity reaches the 85% limit.
Effect	N/A
Recovery	N/A

3.3.22 tmnxMobGwCfCapacityAlmMjrClear

Table 39: tmnxMobGwCfCapacityAlmMjrClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2014
Event name	tmnxMobGwCfCapacityAlmMjrClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.10
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Flash ID- *$tmnxMobGwNtfyFlash Id$*, Flash Limit-*$tmnxMobGwNtfyCfLimit$*, GTP Prime Server Group-*$tmnxMobGwNtfyGtpPriGrpName$*.
Cause	The compact flash capacity drops below the 90% limit.

Property name	Value
Effect	N/A
Recovery	N/A

3.3.23 tmnxMobGwCfCapacityAlmMnrClear

Table 40: tmnxMobGwCfCapacityAlmMnrClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2012
Event name	tmnxMobGwCfCapacityAlmMnrClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.8
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Flash ID- *$tmnxMobGwNtfyFlash Id$*, Flash Limit-*$tmnxMobGwNtfyCfLimit$*, GTP Prime Server Group-*$tmnxMobGwNtfyGtpPriGrpName$*.
Cause	The compact flash capacity drops below the 80% limit.
Effect	N/A
Recovery	N/A

3.3.24 tmnxMobGwCntrlFabricPartialFail

Table 41: tmnxMobGwCntrlFabricPartialFail properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2100
Event name	tmnxMobGwCntrlFabricPartialFail
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.98
Default severity	minor
Source stream	main

Property name	Value
Message format string	Detected *$tmnxMobGwNtfyFailureDirection$* failure for slot *$tmnxMobGwNtfySlot$* on control fabric *$tmnxMobGwNtfyFabricId$*
Cause	A tmnxMobGwCntrlFabricPartialFail is generated when a card loses connectivity to other cards in a particular direction over a particular control fabric. The card ID is indicated in tmnxMobGwNtfySlot, the failed fabric ID is indicated in tmnxMobGwNtfyFabricId and the direction of the failure (transmit/receive) is indicated in tmnxMobGwNtfyFailureDirection.
Effect	The system uses a different operational control fabric to communicate with the affected card.
Recovery	Manual intervention may be required to restore the connectivity.

3.3.25 tmnxMobGwControlFabricFailure

Table 42: tmnxMobGwControlFabricFailure properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2101
Event name	tmnxMobGwControlFabricFailure
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.99
Default severity	minor
Source stream	main
Message format string	Detected *$tmnxMobGwNtfyFailureDirection$* failure for slot *$tmnxMobGwNtfySlot$* on all control fabrics
Cause	A loss of connectivity to other cards occurred in a particular direction over all available control fabrics.
Effect	The card cannot function properly as part of the system.
Recovery	Attempt to restore connectivity by rebooting the affected card.

3.3.26 tmnxMobGwDdnThrottlingStart

Table 43: tmnxMobGwDdnThrottlingStart properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2033
Event name	tmnxMobGwDdnThrottlingStart
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.29
Default severity	warning
Source stream	main
Message format string	Acct Application: Throttling DDN: Gw- *$tmnxMobGwNtfyGatewayId$*, Ref point-*$tmnxMobGwNtfyRefPointType$*, Ref protocol-*$tmnxMobGwNtfyRefPointProtocol$*, RefPointName- *$tmnxMobGwNtfyRefPointName$*, address type-*$tmnxMobGwNtfyRfPtPeerAddrType$*, peer address-*$tmnxMobGwNtfyRfPtPeerAddr$*, port- *$tmnxMobGwNtfyRfPtPeerPort$*, duration-*$tmnxMobGwNtfyDdnThrotDuration$*, factor-*$tmnxMobGwNtfyDdnThrotFactor$*
Cause	The SGW starts throttling the DDN when it receives a throttling instruction carried in the "downlink (DL) low priority traffic Throttling" IE from a peer node.
Effect	The SGW starts throttling the DDN based on a priority threshold value. The traffic with a priority value higher than or equal to the threshold value is considered as a bearer for non-priority traffic.
Recovery	When the throttling time is over, the SGW stops throttling the DDN.

3.3.27 tmnxMobGwDdnThrottlingStop

Table 44: tmnxMobGwDdnThrottlingStop properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2034
Event name	tmnxMobGwDdnThrottlingStop
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.30
Default severity	warning

Property name	Value
Source stream	main
Message format string	Acct Application: Throttling DDN: Gw- *$tmnxMobGwNtfyGatewayId$*, Ref point-*$tmnxMobGwNtfyRefPointType$*, Ref protocol-*$tmnxMobGwNtfyRefPointProtocol$*, RefPointName- *$tmnxMobGwNtfyRefPointName$*, address type-*$tmnxMobGwNtfyRfPtPeerAddrType$*, peer address-*$tmnxMobGwNtfyRfPtPeerAddr$*, port- *$tmnxMobGwNtfyRfPtPeerPort$*, duration-*$tmnxMobGwNtfyDdnThrotDuration$*, factor-*$tmnxMobGwNtfyDdnThrotFactor$*
Cause	The SGW stops throttling the DDN when the throttling time is over.
Effect	The SGW stops throttling the DDN based on a priority threshold value. All DDNs are sent to the peer node.
Recovery	When another throttling instruction is received from a peer node, the SGW starts throttling the DDN.

3.3.28 tmnxMobGwDnsSnpFqdnIpLimitAlarm

Table 45: tmnxMobGwDnsSnpFqdnIpLimitAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2102
Event name	tmnxMobGwDnsSnpFqdnIpLimitAlarm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.100
Default severity	minor
Source stream	main
Message format string	Gw:*$tmnxMobGwNtfyGatewayId$* Number of server addresses learned by DNS Snooping reached *$tmnxMobGwDnsSnpFqdnThres$* % of maximum *$tmnxMobGwDnsSnpFqdnIpMax$*
Cause	The number of stored DNS-resolved IP addresses approaches a threshold limit of the maximum number of cacheable addresses. The threshold is indicated by tmnxMobGwDnsSnpFqdnThres as a percentage, and the maximum size of stored IP addresses is indicated by the tmnxMobGwDnsSnpFqdnIpMax value.
Effect	The PGW may reach the maximum limit and may not be able to store new IP addresses.
Recovery	Clear the resolved filters for the specified FQDN list.

3.3.29 tmnxMobGwLciOverload

Table 46: tmnxMobGwLciOverload properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2080
Event name	tmnxMobGwLciOverload
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.78
Default severity	minor
Source stream	main
Message format string	Mobile Gateway in GTP-C LCI 100%
Cause	The resources for the mobile gateway group reached their limit.
Effect	The mobile gateway group resources are at critical levels. The system attempts to lower resource usage for this mobile gateway group.
Recovery	None

3.3.30 tmnxMobGwLciOverloadClear

Table 47: tmnxMobGwLciOverloadClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2081
Event name	tmnxMobGwLciOverloadClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.79
Default severity	minor
Source stream	main
Message format string	Mobile Gateway GTP-C no longer at LCI 100%
Cause	The resources for the mobile gateway group are back to normal operating levels.
Effect	The mobile gateway group is back to normal operating levels.

Property name	Value
Recovery	None, the system is back to the normal operating levels.

3.3.31 tmnxMobGwMcRedPurgeRebootStandby

Table 48: tmnxMobGwMcRedPurgeRebootStandby properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2063
Event name	tmnxMobGwMcRedPurgeRebootStandby
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.61
Default severity	minor
Source stream	main
Message format string	MC_RED purge: Active card- *$tmnxMobGwNtfyActiveCardSlotNum$* initialized reboot on standby card-*$tmnxMobGwNtfyStandbyCardSlotNum$*
Cause	In the case of a multi-chassis redundancy purge, if the RED state is not 'hot', the active card initializes a reboot on the standby card after the purge finishes on the active card.
Effect	The standby card reboots.
Recovery	No further action is required.

3.3.32 tmnxMobGwNnrfBlocklistAlarm

Table 49: tmnxMobGwNnrfBlocklistAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2126
Event name	tmnxMobGwNnrfBlocklistAlarm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.126
Default severity	warning

Property name	Value
Source stream	main
Message format string	NRF peer for service *$tmnxMobGwNtfyNnrfServiceType$* on GW-*$tmnxMobGwNtfyGatewayId$* is block-listed
Cause	All the NRF peers for the nnrf-nfm or nnrf-disc service are block-listed after failure responses or response timeouts.
Effect	The block-list duration is not applied. All NRF peers are sending failure responses or the responses time out. The gateway continuously retries service requests to all peers.
Recovery	The alarm is cleared when the first NRF peer from the block list is successfully contacted (a success HTTP status is received).

3.3.33 tmnxMobGwNnrfBlocklistAlarmClear

Table 50: tmnxMobGwNnrfBlocklistAlarmClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2127
Event name	tmnxMobGwNnrfBlocklistAlarmClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.127
Default severity	warning
Source stream	main
Message format string	NRF peer for service *$tmnxMobGwNtfyNnrfServiceType$* on GW-*$tmnxMobGwNtfyGatewayId$* is no longer block-listed
Cause	All the NRF peers for the nnrf-nfm or nnrf-disc service are no longer block-listed.
Effect	The block-list duration is applied.
Recovery	No further action required.

3.3.34 tmnxMobGwNrfHeartbeatAlarm

Table 51: tmnxMobGwNrfHeartbeatAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2094
Event name	tmnxMobGwNrfHeartbeatAlarm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.90
Default severity	major
Source stream	main
Message format string	NRF heartbeat failed for peer *$tmnxMobGwNtfyRfPtPeerAddr$* on GW *$tmnxMobGwNtfyGatewayId$* with error: *$tmnxMobGwNtfyNrfHbAlarmReason$*
Cause	Loss of connectivity to the NRF (NRF failure).
Effect	The NRF does not consider the MAG-c SMF or UPF to be registered and eligible for discovery anymore. The NRF may also consider the MAG-c SMF or UPF to be out of service and may notify the subscribed peer NF instances.
Recovery	Recovery is determined according to the failure handling of the failed HB responses, and failover to the next NRF is concluded.

3.3.35 tmnxMobGwNrfHeartbeatAlarmClear

Table 52: tmnxMobGwNrfHeartbeatAlarmClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2095
Event name	tmnxMobGwNrfHeartbeatAlarmClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.91
Default severity	major
Source stream	main

Property name	Value
Message format string	NRF heartbeat succeeded for peer *$tmnxMobGwNtfyRfPtPeerAddr$* on GW *$tmnxMobGwNtfyGatewayId$* with error: *$tmnxMobGwNtfyNrfHbAlarmReason$*
Cause	Successful Heartbeat message request/response sequence with the NRF.
Effect	The NRF considers the MAG-c SMF or UPF to be registered and eligible for discovery.
Recovery	No further action is required.

3.3.36 tmnxMobGwOciOverload

Table 53: tmnxMobGwOciOverload properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2082
Event name	tmnxMobGwOciOverload
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.80
Default severity	major
Source stream	main
Message format string	Mobile Gateway in GTP-C OCI overload
Cause	The resources for the mobile gateway group were almost exhausted because of high load.
Effect	The mobile gateway group resources are at critical levels. The system attempts to lower resource usage on this mobile gateway group.
Recovery	None.

3.3.37 tmnxMobGwOciOverloadClear

Table 54: tmnxMobGwOciOverloadClear properties

Property name	Value
Application name	MOBILE_GATEWAY

Property name	Value
Event ID	2083
Event name	tmnxMobGwOciOverloadClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.81
Default severity	major
Source stream	main
Message format string	Mobile Gateway no longer in GTP-C overload
Cause	The resources for the mobile gateway group returned to normal operating levels.
Effect	The mobile gateway group returns to normal operating levels.
Recovery	None, the system is back to the normal operating levels.

3.3.38 tmnxMobGwOciOvldThrtStart

Table 55: tmnxMobGwOciOvldThrtStart properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2103
Event name	tmnxMobGwOciOvldThrtStart
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.101
Default severity	major
Source stream	main
Message format string	The mobile gateway has started throttling incoming call flows due to local overload.
Cause	The resources for the mobile gateway group were almost exhausted because of high load.
Effect	The mobile gateway group resources are at a critical level. The system attempts to lower the resource usage on this mobile gateway group.
Recovery	The mobile-gateway stops throttling incoming call flows when it is out of local overload.

3.3.39 tmnxMobGwOciOvldThrtStop

Table 56: tmnxMobGwOciOvldThrtStop properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2104
Event name	tmnxMobGwOciOvldThrtStop
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.102
Default severity	major
Source stream	main
Message format string	The mobile gateway has stopped throttling incoming call flows due to local overload.
Cause	Incoming call flows have not been received for the last 30 seconds or the resources for the mobile gateway group have returned to normal operating levels for the last 30 seconds.
Effect	The mobile gateway is no longer throttling incoming call flows because of local overload.
Recovery	Not applicable.

3.3.40 tmnxMobGwPathMgmtPeerState

Table 57: tmnxMobGwPathMgmtPeerState properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2001
Event name	tmnxMobGwPathMgmtPeerState
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.1
Default severity	major
Source stream	main
Message format string	Path Management: Peer State: *$tmnxMobGwNtfyPathMgmtPeerState $*: Gw-*$tmnxMobGwNtfyGatewayId$*, Ref point-*$tmnxMobGwNtfyRef PointType$*, protocol- *$tmnxMobGwNtfyRefPointProtocol$*, RefPoint Name-*$tmnxMobGwNtfyRefPointName$*,peer-*$tmnxMobGwNtfyRfPt*

Property name	Value
	PeerAddr$*, port- *$tmnxMobGwNtfyRfPtPeerPort$*, Local address - *$tmnxMobGwNtfyPathLocAddress$*, Previous Restart Counter- *$tmnxMobGwNtfyPrevRestartCounter$*, Current Restart Counter-*$tmnxMobGwNtfyCurrRestartCounter$*, Peer Restart Reason- *$tmnxMobGwNtfyPeerRestartReason$*, Pkt Seq Number-*$tmnxMobGwNtfyPeerRestPktSeqNum$*, Peer Type-*$tmnxMobGwNtfySigPeerType$*, Plane Type- *$tmnxMobGwNtfySigPlaneType$.
Cause	There has been a change in the reference point peer state during path management. The supported trap event values are the following: Added - raised when a new peer is identified by incoming messages GUp - raised when a peer moves to the UP state, for an SGW peer, this state change happens when a CS Req is received. for PGW peers, this state change happens when a CS Resp from the PGW peer is received (this is to make sure that Path UP trap is generated only for a real PGW peer in case of GTP-C redirection) Down - raised when a peer moves to the FAULT state while detecting a path management failure. Idle - raised when a peer moves to the IDLE state after a session cleanup is done because of a path management Failure, Detach or Admin delete. Restart - raised when a peer restart is detected. It is associated with the Peer RESTART state. Deleted - raised when a peer entry is deleted because of a peer aging out. A peer ages out when it is Idle for more than the Age Out Interval.
Effect	N/A
Recovery	N/A

3.3.41 tmnxMobGwPcmdOperStateChange

Table 58: tmnxMobGwPcmdOperStateChange properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2045
Event name	tmnxMobGwPcmdOperStateChange
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.43
Default severity	minor
Source stream	main
Message format string	PCMD: Oper State: *$tmnxMobGwNtfyPcmdOperState$*: Gw- *$tmnxMobGwNtfyGatewayId$*, PCMD profile-*$tmnxMobGwNtfyPcmdProfile$*

Property name	Value
Cause	The PCMD operational state changes when the destination address reachability changes.
Effect	When the PCMD state is down, the generated PCMD packets are not sent to the destination address. When the PCMD state is up, the PCMD packets are sent to the destination address.
Recovery	If the PCMD state is down, the generated PCMD packets are dropped.

3.3.42 tmnxMobGwPfcpRestoreInProg

Table 59: tmnxMobGwPfcpRestoreInProg properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2122
Event name	tmnxMobGwPfcpRestoreInProg
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.122
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$* VRtr- *$tmnxMobGwNtfyVrtrId$* Ref PointType-*$tmnxMobGwNtfyRefPointType$* RefPointName-*$tmnxMob GwNtfyRefPointName$* PFCP restoration in progress for RemotePeer Address- *$tmnxMobGwNtfyRfPtPeerAddr$* LocalPeerAddress-*$tmnx MobGwNtfyPeerLocAddress$* RestoreTimer-*$tmnxMobGwNtfyRestore Timer$* NodeId- *$tmnxMobGwNtfyPeerNodeId$*
Cause	A PFCP keepalive failure between UP and CP has been detected.
Effect	The restoration timer starts.
Recovery	Restore the path between the UP and the CP to allow keepalives to succeed again. If keepalives recover before the restoration timer times out, the CP and the UP perform an audit and recover from the failure automatically.

3.3.43 tmnxMobGwPfcpViaUpFuncFailureClr

Table 60: tmnxMobGwPfcpViaUpFuncFailureClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2129
Event name	tmnxMobGwPfcpViaUpFuncFailureClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.129
Default severity	cleared
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, *$tmnxMobGwNtfyGrpName$* detected a PFCP-u tunnel connectivity re-established between the CP function and UP function.
Cause	The PFCP-u tunnel used for via-up-function (radius-group or dhcp-server-group) traffic between the CP and the UP function is failing to be re-established.
Effect	Any traffic routed over the PFCP-u tunnel will no longer fail.
Recovery	No further action required.

3.3.44 tmnxMobGwRadGrpFailAlarm

Table 61: tmnxMobGwRadGrpFailAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2024
Event name	tmnxMobGwRadGrpFailAlarm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.20
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Radius Server Group- *$tmnxMob GwNtfyRadGrpName$*, Group State-*$tmnxMobGwNtfyRadGrpState$*.

Property name	Value
Cause	All the RADIUS servers for the group are in a down state.
Effect	When the group of RADIUS servers fails, RADIUS messages may not be sent to the group.
Recovery	The RADIUS server group recovers from this failure mode when one of its servers returns to the up state.

3.3.45 tmnxMobGwRadGrpFailAlarmClrd

Table 62: tmnxMobGwRadGrpFailAlarmClrd properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2025
Event name	tmnxMobGwRadGrpFailAlarmClrd
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.21
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Radius Server Group- *$tmnxMob GwNtfyRadGrpName$*, Group State-*$tmnxMobGwNtfyRadGrpState$*.
Cause	The RADIUS server group recovered from the previous failure mode and at least one of its servers has transitioned to the up state.
Effect	The operation for the RADIUS group returns to normal.
Recovery	No further action is required.

3.3.46 tmnxMobGwRadPeerFailAlarm

Table 63: tmnxMobGwRadPeerFailAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2022
Event name	tmnxMobGwRadPeerFailAlarm

Property name	Value
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.18
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Radius Server Group- *$tmnxMobGwNtfyRadGrpName$*, Address-*$tmnxMobGwNtfyRadPeerAddr$*, Authentication port-*$tmnxMobGwNtfyRadPeerAuthPort$*, Accounting port- *$tmnxMobGwNtfyRadPeerAcctPort$*, Peer State-*$tmnxMobGwNtfyRadPeerState$*.
Cause	The state for the RADIUS server changed to down.
Effect	RADIUS messages may not be sent to the RADIUS server.
Recovery	RADIUS messages can continue to be sent to a RADIUS server after the RADIUS server's state changes back to up or the dead timer expires.

3.3.47 tmnxMobGwRadPeerFailAlarmClrd

Table 64: tmnxMobGwRadPeerFailAlarmClrd properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2023
Event name	tmnxMobGwRadPeerFailAlarmClrd
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.19
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Radius Server Group- *$tmnxMobGwNtfyRadGrpName$*, Address-*$tmnxMobGwNtfyRadPeerAddr$*, Authentication port-*$tmnxMobGwNtfyRadPeerAuthPort$*, Accounting port- *$tmnxMobGwNtfyRadPeerAcctPort$*, Peer State-*$tmnxMobGwNtfyRadPeerState$*.
Cause	The RADIUS server recovered from the previous failure mode, and one of its servers has transitioned to the up state.
Effect	The operation for the RADIUS server returns to normal.
Recovery	No further action is required.

3.3.48 tmnxMobGwSbiPeerState

Table 65: tmnxMobGwSbiPeerState properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2130
Event name	tmnxMobGwSbiPeerState
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.130
Default severity	warning
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, Group ID- *$tmnxMobGwNtfySbi GroupId$*, NF service name- *$tmnxMobGwNtfySbiNfServiceName $*, Service Instance- *$tmnxMobGwNtfySbiNfServiceIns$*, peer UUID- *$tmnxMobGwNtfySbiPeerUuid$*, peer ip address- *$tmnxMobGwNtfySbi PeerIpAddress$*, peer port- *$tmnxMobGwNtfySbiPeerPort$*, connection state- *$tmnxMobGwNtfySbiConnectionState$*, NF service state- *$tmnx MobGwNtfySbiNfServiceState$*.
Cause	A change occurred in the NF peer connection status or a peer was deleted from the peer list.
Effect	N/A.
Recovery	N/A.

3.3.49 tmnxMobPdnApnMaxPdnConnAlarm

Table 66: tmnxMobPdnApnMaxPdnConnAlarm properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2035
Event name	tmnxMobPdnApnMaxPdnConnAlarm
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.33
Default severity	major
Source stream	main

Property name	Value
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, APN Name- *$tmnxMobGwNtfyApnName$*.
Cause	The maximum number of PDN connections for this APN on the gateway was reached.
Effect	New PDN connections are not accepted until the limit drops below the value of TIMETRA-MOBILE-PDN-MIB::tmnxMobPdnApnMaxPdnConnections.
Recovery	To accept new PDN connections, the system has to wait until the maximum PDN connections number drops below the threshold.

3.3.50 tmnxMobPdnApnMaxPdnConnAlarmClr

Table 67: tmnxMobPdnApnMaxPdnConnAlarmClr properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2036
Event name	tmnxMobPdnApnMaxPdnConnAlarmClr
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.34
Default severity	major
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, APN Name- *$tmnxMobGwNtfyApnName$*.
Cause	The existing number of PDN connections for this APN on the gateway drops below the value of TIMETRA-MOBILE-PDN-MIB::tmnxMobPdnApnMaxPdnConnections.
Effect	New PDN connections are accepted.
Recovery	No further action is required.

3.3.51 tmnxMobPdnBearerContextClear

Table 68: tmnxMobPdnBearerContextClear properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2153
Event name	tmnxMobPdnBearerContextClear
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.155
Default severity	warning
Source stream	main
Message format string	Clear bearer context in PDN *$tmnxMobGwNtfyGatewayId$ $tmnxMobGwNtfyLongText$ $tmnxMobGwNtfyStartEnd$* (*#$tmnxMobGwNtfyNumber$*)
Cause	The system started or terminated the processing a request to clear a PDN bearer context. The request can be made with the clear mobile-gateway pdn bearer-context CLI command or one of the appropriate rows in the TIMETRA-CLEAR-MIB::tmnxClearTable, for example the 'clearMobPdnBearerContext' row.
Effect	In the time interval between the start and end notification, the system clears a number of PDN bearer contexts that match the specified parameters. The UEs associated with the bearer contexts lose their connection with the PDN.
Recovery	None.

3.3.52 tmnxMobPdnLaaPfxInsufficientMem

Table 69: tmnxMobPdnLaaPfxInsufficientMem properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2113
Event name	tmnxMobPdnLaaPfxInsufficientMem
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.113
Default severity	warning

Property name	Value
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, network realm *$tmnxMobGwNtfyNwRealmName$*, pool *$tmnxMobGwNtfyPoolName$*, prefix *$tmnxMobGwNtfyAddr$*/*$tmnxMobGwNtfyPfxLength$* not operational due to insufficient memory
Cause	There is insufficient memory for an IP address prefix and all of its micronets.
Effect	The IP address prefix is not activated, and its operational state goes down.
Recovery	Add memory to the system, or reduce the number of the prefix micronets.

3.3.53 tmnxMobPdnLaaPlNoFreeMnets

Table 70: tmnxMobPdnLaaPlNoFreeMnets properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2136
Event name	tmnxMobPdnLaaPlNoFreeMnets
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.136
Default severity	minor
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, network realm *$tmnxMobGwNtfyNwRealmName$*, pool *$tmnxMobGwNtfyPoolName$* IPv6 type *$tmnxMobGwNtfyIpv6AssignmentType$*: no more free *$tmnxMobGwNtfyLaaUnfragmentedMn$* micronets *$tmnxMobGwNtfyTruthValue$*
Cause	The last available micronet of its kind in the pool is activated.
Effect	Setup of new end user sessions starts to fail.
Recovery	Add prefixes to the pool.

3.3.54 tmnxMobPdnLaaPlNumFreeMnetsLow

Table 71: tmnxMobPdnLaaPlNumFreeMnetsLow properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2110
Event name	tmnxMobPdnLaaPlNumFreeMnetsLow
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.108
Default severity	warning
Source stream	main
Message format string	Gw-*$tmnxMobGwNtfyGatewayId$*, network realm *$tmnxMobGwNtfy NwRealmName$*, pool *$tmnxMobGwNtfyPoolName$* IPv6 type *$tmnx MobGwNtfyIpv6AssignmentType$*: running low on *$tmnxMobGwNtfy LaaUnfragmentedMn$* micronets *$tmnxMobGwNtfyTruthValue$*
Cause	A micronet is activated while the number of free micronets in the pool is already low.
Effect	None.
Recovery	No recovery is immediately required. However, it is recommended to add prefixes to avoid complete depletion of the pool.

3.3.55 tmnxMobProfNodeSelTrgtSugstRebal

Table 72: tmnxMobProfNodeSelTrgtSugstRebal properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2149
Event name	tmnxMobProfNodeSelTrgtSugstRebal
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.151
Default severity	warning
Source stream	main

Property name	Value
Message format string	Evaluate target-profile *$tmnxMobGwNtfyProfileName$* and rebalance if necessary - new UP=*$tmnxMobGwNtfyUpPeerAddress$*, surviving number of UPs= *$tmnxMobGwNtfyNumber$*
Cause	The system reconnected to a UPF after having been disconnected.
Effect	While the UPF connection was down session distribution among the UPFs in a target profile may have become unbalanced. This event indicates session load rebalancing may be necessary.
Recovery	Evaluate session load among the available UPFs in the target profile, and if necessary, rebalance using a clear operation.

3.3.56 tmnxMobProfNodeSelTrgtSugstRevrt

Table 73: tmnxMobProfNodeSelTrgtSugstRevrt properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2150
Event name	tmnxMobProfNodeSelTrgtSugstRevrt
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.152
Default severity	warning
Source stream	main
Message format string	Evaluate target-profile *$tmnxMobGwNtfyProfileName$* and revert if necessary
Cause	The number of available UPFs in a target profile entry reached the necessary minimum threshold.
Effect	While the number of available UPF connections was below the minimum threshold new sessions are directed to backup UPFs. This event indicates it may be appropriate to revert sessions to primary UPFs.
Recovery	Session load among primary and secondary UPFs of the target profile should be evaluated and if necessary, reverted using a clear operation.

3.3.57 tmnxOverlayFabricFailure

Table 74: tmnxOverlayFabricFailure properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2072
Event name	tmnxOverlayFabricFailure
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.70
Default severity	minor
Source stream	main
Message format string	Detected *$tmnxMobGwNtfyFailureDirection$* failure for slot *$tmnxMobGwNtfySlot$* on all overlay fabrics
Cause	A loss of connectivity occurred to other cards in a particular direction over all available overlay fabrics.
Effect	The card cannot function properly as part of the system.
Recovery	Attempt to restore connectivity by rebooting the affected card.

3.3.58 tmnxOverlayFabricPartialFailure

Table 75: tmnxOverlayFabricPartialFailure properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2073
Event name	tmnxOverlayFabricPartialFailure
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.71
Default severity	minor
Source stream	main
Message format string	Detected *$tmnxMobGwNtfyFailureDirection$* failure for slot *$tmnxMobGwNtfySlot$* on overlay fabric *$tmnxMobGwNtfyFabricId$*
Cause	Loss of connectivity between the affected card and the other cards in a particular direction over a particular overlay fabric.

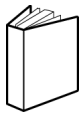
Property name	Value
Effect	The system uses a different operational overlay fabric to communicate with the affected card, but the capacity is reduced.
Recovery	Manual intervention may be required to restore the connectivity.

3.3.59 tmnxOverlayFabricStatus

Table 76: tmnxOverlayFabricStatus properties

Property name	Value
Application name	MOBILE_GATEWAY
Event ID	2060
Event name	tmnxOverlayFabricStatus
SNMP notification prefix and OID	TIMETRA-MOBILE-GATEWAY-MIB.tmnxMobGatewayNotifications.58
Default severity	major
Source stream	main
Message format string	Operational state of last overlay fabric port transitioned to *$tmnxMobGwNtfyOverlayFabricState$* state for VM *$tmnxMobGwNtfyVmId$*
Cause	A change occurred in the operational state of the overlay fabric switch, either when the last operational overlay fabric port transitioned to the down state or the first overlay fabric port transitioned to an up state.
Effect	If the value of tmnxMobGwNtfyOverlayFabricState is down, the VM fails (crashes) and ceases to process any new packets.
Recovery	If the value of tmnxMobGwNtfyOverlayFabricState is down, the VM fails to process new packets and reboots. The VM remains in the booting state until the value of tmnxMobGwNtfyOverlayFabricState changes to up.

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback