Oracle® Communications Network Charging and Control

SIGTRAN Alarms Guide

Release 15.1

April 2025

Copyright

Contents

Alarm Topic Description 1
SIGTRAN Alarms 3

Alarm Topic Description

Alarm Generation

Alarms on each configured node are written to the syslog and are then captured by the smsAlarmDaemon for entry in the SMF database.

For management of these alarms, see *Service Management System Technical Guide*.

Severity Levels

This table describes the alarm severity levels.

Level	Abbreviation	Description
Critical	C	These alarms are raised when the application has encountered an error indicating that the system is unable to function.
Error	E	These alarms indicate the application has encountered a serious problem completing a necessary task and could not complete the task.
Warning	W	Warnings are raised to indicate the application encountered a problem completing a non-mission critical task.
Notice	N	Notices are raised to indicate that the application has completed a task successfully.

Alarm Format

Alarms usually follow this format:

```
Mon DD 24:MM:SS hostname process name: [ID alarmID user.severity] process(PID)
SEVERITY: Alarm text with possible variables
```

Where:

Variable	Description
Mon DD	Month and date the alarm was logged.
24:MM:SS	Time the alarm was logged in 24 hour format.
hostname	Name of the machine on which the alarm was generated.
process name	Name of the process which logged the alarm.
alarmID	ID number of the alarm.
severity	Alarm severity.
process	Name of the process which logged the alarm.
PID	Process ID of the process which logged the alarm.
SEVERITY	Alarm severity.
Alarm text	Alarm text. This may include variables such as node number. **Note:** In some cases, the entire alarm text is generated from variables.

Note: Some alarms from some subsystems may have a different format.

Example: This text shows an smsMaster alarm about pending update queues.

```
Mar 30 13:34:54 prodsmp1 smsMaster: [ID 953149 user.warning] smsMaster(17833)
WARNING: Pending queue now above 15 (Worst Node 317)
```

Alarm Text and Variables

The %d and %s symbols represent variables within the alarm text. These values are generated by the subsystem and added to the message when the alarm is raised.

Usually the %d is a number and the %s is text in the context of the message to complete the alarm message. Occasionally other % symbols are also used (for example, %u) for different variables.

Further Information

For more information about:

- The SMS Alarms subsystem, see *Service Management System Technical Guide*
- Creating and maintaining the SMS Alarm Relay rule set, see *Service Management System User's Guide*

SIGTRAN Alarms

Alarm	Severity	Text	Cause	Resolution	Service
400001	NOTICE	%z \{400001\}%z Connected on FD %d, bringing up %z	SCTP socket connection is complete.	Normal operation. No action required.	sua_if
400002	NOTICE	%z \{400002\}%z connected, not accepting FD %d	An incoming connection is rejected as a duplicate. The connection matched the same remote and local address specifications of an existing connection.	Check configuration of both local interface and of peer. Add remote port specifications to configuration if needed. Specify initiation of connection to be either listen or connect as appropriate.	sua_if
400003	NOTICE	%z \{400003\}%z	An incoming connection is rejected as the connection is disabled.	This may occur during shutdown. Otherwise, if problem persists, contact support.	sua_if
400004	NOTICE	%z \{400004\}%z accepted connection on FD %d	An incoming connection has been accepted.	Normal operation. No action required.	sua_if
400005	NOTICE	%z \{400005\}%z Sending UP	Sending an UP (or ASPUP) packet.	Normal operation. No action required.	sua_if
400006	NOTICE	%z \{400006\}%z remote ASP is DOWN	A DOWN (or ASPDN) has been received. The remote ASP is in the down state.	Normal operation. No action required.	sua_if
400007	NOTICE	%z \{400007\}%z Remote ASP is ACTIVE	The remote ASP is now active.	Normal operation. No action required.	sua_if
400008	NOTICE	%z \{400008\}%z We have reached ACTIVE	The local ASP is now active.	Normal operation. No action required.	sua_if
400009	NOTICE	%z \{400009\}%z	The remote ASP is now inactive.	Normal operation. No action required.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
400010	NOTICE	%z \{400010\}%z Connection in service	The connection is now in service for data traffic.	Normal operation. No action required.	sua_if
400011	NOTICE	%z \{400011\}%z Connection out of service	The connection is now out of service for data traffic.	Normal operation, although may occur as a consequence of earlier errors. No action required.	sua_if
400012	NOTICE	%z \{400012\}%z Connecting.	An outgoing SCTP connection is being initiated.	Normal operation. No action required.	sua_if
400013	NOTICE	%z \{400013\}%z Listening for connections with FD %z	We are listening for incoming SCTP connections.	Normal operation. No action required.	sua_if
400014	ERROR	%z \{400014\}%z Incoming connection from %z was unwanted.	An incoming SCTP connection was received from an unknown remote address.	If the connection from the remote address was wanted, then check and correct interface configuration. Otherwise, disable or block the remote peer.	sua_if
400015	ERROR	%z \{400015\}%z	An incoming SCTP connection was received from a known remote address but was not accepted.	Check previous errors, and fix configuration as needed.	sua_if
400016	NOTICE	%z \{400016\}%z connection closed.	An SCTP connection was closed by the remote host.	This will occur in normal operation. If the connection close is a problem, and persists, then (a) check for previous errors, (b) check error logs on remote host, (c) check configuration.	sua_if
400018	NOTICE	%z \{400018\}%z Sending DOWN	Sending a DOWN (or ASPDN) packet.	Normal operation. No action required.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
400019	NOTICE	%z \{400019\}%z Sending ACTIVE	Sending an ACTIVE (or ASPAC) packet.	Normal operation. No action required.	sua_if
400020	NOTICE	%z \{400020\}%z Sending INACTIVE	Sending an INACTIVE (or ASPIA) packet.	Normal operation. No action required.	sua_if
400021	NOTICE	%z \{400021\}%z streams out; %d streams in.	The SCTP connection is complete. The negotiated number of output and input streams is noted. Note that the remote end-point may reduce the number of streams to be less than the number configured.	Normal operation. No action required.	sua_if
400022	NOTICE	%z \{400022\}%z	The SCTP layer has indicated a change in the state of a remote peer.	Normal operation. No action required. However, if unreachable events are seen regularly, then this may be an indication of an unreliable network link.	sua_if
400023	NOTICE	%z \{400023\}%z Received %z	A SCCP UDTS, XUDTS, LUDTS or a SUA CLDR message has been received.	These may be expected occassionally, especially if a network is overloaded or unreliable. If large numbers of the messages are received, then check your network for connectivity or congestion problems.	sua_if
401001	ERROR	%z \{401001\}%z	An internal error occurred on the socket level API or other system call.	Please report to support.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401002	ERROR	%z \{401002\}%z	I/O error on socket.	This may occur as a transient issue. If persistent, then please refer to a network expert or support.	sua_if
401003	CRITICAL	%z \{401003\}%z	Internal consistency error.	Please report to support.	sua_if
401004	WARNING	%z \{401004\}%z Congested; dropping outbound packet	An SCTP connection is congested. A packet has been dropped.	Refer to network expert. If this occurs regularly, then increase network buffer sizes. Check network for intermittent connectivity problems or excessive latency.	sua_if
401005	ERROR	%z \{401005\}%z Partial packet write %d of %d bytes.	A packet was truncated by the SCTP stack.	Refer to support.	sua_if
401006	ERROR	%z \{401006\}%z socketZZZ failed: %z	Failed to create SCTP socket.	Check that the SCTP stack is enabled. Refer to networking expert or support.	sua_if
401007	ERROR	%z \{401007\}%z connect failed: %z	Failed to initiate SCTP socket connect.	Refer to network expert or support. Check IP network addresses used in configuration.	sua_if
401008	ERROR	%z \{401008\}%z	Failed to bind an SCTP socket to a local address.	Refer to network expert or support. Check IP network addresses used in configuration.	sua_if
401009	ERROR	%z \{401009\}%z Resolving address %z failed: %z	Could not resolve host name.	Check IP network addresses in configuration. Check that DNS is available. Refer to network expert.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401010	ERROR	%z \{401010\}%z listen failed: %z	Listening for new connections on an SCTP socket failed. This may occur (a) if another process is using the same local network address, or (b) if the same local address is configured using multiple different names (e.g., both host name and IP address), or (c) if a connection is configured to both listen and connect, and the SCTP implementation does not support this.	Refer to network expert or support. Check for other use of the same local network address. In configuration, consistently use the same name for the same local network address. In configuration, specify the initiation parameter on connections. Use different port numbers for different connections if necessary.	sua_if
401011	CRITICAL	%z \{401011\}%z Error on accept: %z	A listening socket has failed. We will no longer listen on this address.	Refer to support. Restart SUA/M3UA interface.	sua_if
401012	ERROR	%z \{401012\}%z Insufficient buffer space to send %z	Sending an outgoing message has overflowed the available buffer space. The message could not be sent.	Refer to support.	sua_if
401013	WARNING	%z \{401013\}%z Received %z error: %z	A SUA/M3UA ERR (Error) packet has been received. The error information from the packet is noted.	Refer to networking expert or support.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401014	ERROR	%z \{401014\}%z	A SCCP data payload was too large to be sent. Either segmentation was not enabled, or segmentation resulted in more than 16 segments.	Configure or increase the segmentation_size parameter for the network connection. If using SCCP over M3UA, ensure that the xudtHopCount global parameter is set to a positive number. The protocol limits the number of segments to 16; sending SCCP XUDT packets this gives a payload limit of 4080 bytes.	sua_if
401015	ERROR	%z \{401015\}%z	Due to previous errors, synchronisation of messages over a TCP socket has been lost. The socket will be closed.	Diagnose and correct preceding errors.	sua_if
401016	ERROR	%z \{401016\}%z Attempting to send address with RI=GT,	An attempt has been made to send a network packet with routing indicator set to route-on-global-title, but no global title is present in the address, or the global title is not valid. The address has been changed to route on SSN/PC.	This mostly likely indicates misconfiguration of other software with an illegal address. In particular, note that ANSI Global Titles have a more limited structure that SCCP Global Titles. Refer to networking expert or support.	sua_if
401017	ERROR	%z \{401017\}%z	Incoming network traffic is either corrupt or incompatible with code. An incoming SUA/M3UA message could not be parsed.	Refer to network expert or support.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401018	ERROR	%z \{401018\}%z Invalid SCCP %z	Incoming network traffic is either corrupt or incompatible with code. An invalid SCCP message was received.	Contact support.	sua_if
401019	NOTICE	%z \{401019\}%z Received unhandled packet %z	An unhandled SUA/M3UA message was received. A remote host is attempting to use unsupported features of the SUA/M3UA protocol.	Refer to network expert or support.	sua_if
401020	ERROR	%z \{401020\}%z No point code for GTT of %z	GTT could not be applied to an outgoing packet as no point code would result.	Refer to network expert or support. Check and correct configuration.	sua_if
401021	ERROR	%z \{401021\}%z No subsystem number for GTT of %z	GTT could not be applied to an outgoing packet as no subsystem number would result.	Refer to network expert or support. Check and correct configuration.	sua_if
401022	CRITICAL	%z \{401022\}%z	Fatal internal error. The interface process will exit.	Refer to support. Restart interface process if possible.	sua_if
401023	CRITICAL	%z \{401023\}%z Error reading configuration: %z	Error reading configuration. The error is not recoverable and the process will exit.	Correct configuration and restart interface process.	sua_if
401024	CRITICAL	%z \{401024\}%z SCCP %z unimplemented	An unhandled SCCP message was received. A remote host is attempting to use unsupported features of the SCCP protocol.	Refer to network expert or support.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401025	ERROR	%z \{401025\}%z runt DATA payload (%d bytes, need at least 13).	An under-length M3UA payload was received. This may indicate either corrupt data on the network, or that non-SCCP traffic has been directed to the M3UA interface.	Refer to network expert. Check network configuration.	sua_if
401026	ERROR	%z \{401026\}%z ACTIVE_ACK packet does not contain routing context	A received SUA ACTIVE_ACK packet failed to provide a routing context to use. The routing context is mandatory for SUA.	This is almost certainly a protocol violation by the remote peer. Refer to a network expert.	sua_if
401027	ERROR	%z \{401027\}%z Cannot activate SUA connection without routing context	A remote peer has sent us an SUA ACTIVE packet, but we have no routing context to use. A routing context is mandatory to activate an SUA connection.	Configure a routing context for the connection.	sua_if
401028	ERROR	%z \{401028\}%z address %z already in use.%z	Binding a SCTP socket to a local address failed due to the address already being in use. This may occur to attempting to simultaneously listen for incoming connections and connect to a remote end-point.	Set the initiation parameter for the connection. Refer to network expert or support. Check IP network addresses used in configuration.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
401029	ERROR	%z \{401029\}%z	Error reading configuration. The process will continue, but configuration parameters may not be applied in the expected manner.	Correct configuration and reload or restart interface process.	sua_if
401030	ERROR	%z \{401030\}%z Invalid global title indicator in outgoing address.	An attempt has been made to send a network packet with an invalid global title indicator on an SCCP (or SUA) address.	This mostly likely indicates misconfiguration of other software with an illegal address. In particular, note that ANSI Global Titles have a more limited structure that SCCP Global Titles. Refer to networking expert or support.	sua_if
401031	WARNING	%z \{401031\}%z Incoming global title has incorrect padding.	An incoming data packet has a SUA global title formatted incorrectly, with the length including padding bytes. The SUA layer has attempted to correct this.	The remote peer has sent incorrect data. The software has corrected the problem, and should continue to operate correctly. If appropriate, obtain a fix for the peers software.	sua_if
401032	ERROR	%z \{401032\}%z	An incoming packet was detected to contain invalid ASN.1 data. The packet has been discarded.	Use network tracing tools such as wireshark to determine the origin of the invalid packet, and obtain a fix for that equipment. The validation and level of logging is controlled by the asn1_validate configuration parameter; adjust this if the log message volume is a problem.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402001	WARNING	%z \{402001\}%z Received unexpected UP	Unexpected UP (or ASPUP) packet received. This may occur while starting a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402002	NOTICE	%z \{402002\}%z Remote ASP %z is UP	An UP (or ASPUP) has been received with the given ASP Identifier.	Normal operation. No action required.	sua_if
402003	WARNING	%z \{402003\}%z Received unexpected UP_ACK	Unexpected UP_ACK (or ASPUP_ACK) packet received. This may occur while starting a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402004	WARNING	%z \{402004\}%z received unexpected DOWN	Unexpected DOWN (or ASPDN) packet received. This may occur while starting a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402005	WARNING	%z \{402005\}%z Remote ASP sends ACTIVE without UP	An ACTIVE (or ASPAC) packet has been received without an UP. A remote peer has sent the message out of sequence.	Refer to network expert. It is likely that a remote peer has not correctly implemented the SUA/M3UA protocol.	sua_if
402006	NOTICE	%z \{402006\}%z routing contextZZZ	The routing context that will be used for transmitted data packets is noted.	Normal operation. No action required.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402007	WARNING	%z \{402007\}%z Received traffic_mode_type %d	The traffic mode type parameter received from the remote peer differs from that configured.	The configuration can be corrected either by changing or removing the parameter as desired.	sua_if
402008	WARNING	%z \{402008\}%z Received unexpected ACTIVE_ACK	An unexpected ACTIVE_ACK (or ASPAC_ACK) has been received. This may occurred while starting a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402009	WARNING	%z \{402009\}%z Routing context is different from configured %d	The routing context negotiated with the remote end-point differs from that configured. The negotiated routing context value will be used.	Check configurations of both the interface and the remote peer, and adjust these to be consistent.	sua_if
402010	WARNING	%z \{402010\}%z Received unexpected INACTIVE	An INACTIVE (or ASPIA) was received while the remote ASP was not active. This may occur while stopping a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402011	WARNING	%z \{402011\}%z Received unexpected INACTIVE_ACK	An unexpected INACTIVE_ACK (or ASPIA_ACK) was received. This may occur while stopping a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402012	NOTICE	%z \{402012\}%z	Regular statistics notification.	Normal operation. No action required. If the volume of messages is undesirable, adjust configuration to reduce message frequency or disable altogether.	sua_if
402013	NOTICE	%z \{402013\}%z Notified of AS %z	A SUA/M3UA NTFY packet was received. The details are logged.	Normal operation. No action required.	sua_if
402014	NOTICE	%z \{402014\}%z	Process start-up; the SCTP implementation in use is logged.	Normal operation. No action required.	sua_if
402015	NOTICE	%z \{402015\}%z is now running.	The SUA/M3UA interface is now running normally.	Normal operation. No action required.	sua_if
402016	NOTICE	%z \{402016\}%z Interface is now stopped.	The SUA/M3UA interface is now stopped normally and the process is exiting.	Normal operation. No action required.	sua_if
402017	WARNING	%z \{402017\}%z only one local_host will be used over TCP	Only SCTP connections may have multiple end-point addresses. When operating over TCP, only the first address is used, and any additional addresses are ignored.	Removing the additional end-point addresses will stop the warning message.	sua_if
402018	NOTICE	%z \{402018\}%z Reloading configuration.	The configuration of the interface process is being reloaded, in response to receiving a Unix SIGHUP signal.	Normal operation. No action required.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402019	NOTICE	%z \{402019\}%z	The details of the configuration loaded are logged, both at start-up, and when the configuration is reloaded due to a SIGHUP.	Normal operation. No action required.	sua_if
402020	WARNING	%z \{402020\}%z Received unexpected DOWN_ACK	An unexpected DOWN_ACK (or ASPDN_ACK) packet received. This may occur while starting a connection due to retransmitted packets.	No action required, but if persistent may be a symptom of a network configuration problem.	sua_if
402021	WARNING	%z \{402021\}%z Received %z from SGP	An UP (or ASPUP) or ACTIVE (or ASPAC) packet has been received from a remote peer which the local configuration indicates is a SGP (signalling gateway).	Correct the configuration. If the remote peer really is an ASP, then remove or correct the corresponding remote_role parameter in the local configuration.	sua_if
402022	WARNING	%z \{402022\}%z Address range %z	The interface has been unable to automatically group connections into application servers.	Add explicit application_server names to the configured connections to resolve the problem. [The log files indicate what assignments were made.]	sua_if
402023	NOTICE	%z \{402023\}%z	The current state of the connections are logged, whenever a SIGHUP is received.	Normal operation. No action required.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402025	NOTICE	DEF123sua_if: sua_if(%d) NOTICE =%d sleeTcapIf.cc@%d: Rejected %d calls out of %d in the last 30s	Calling attempt rate from network into the interface has exceeded the configured threshold and the indicated number of calls were rejected. because of this	Refer to application/signalling expert. Reduce rate of queries from network into application on this interface.	sua_if
402026	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL =%d sleeTcapIf.cc@%d: Unknown service key %s %d	Applications request to send TCAP message was rejected by TCAP stack for the reason specified.	Contact support.	sua_if
402027	ERROR	DEF123sua_if: sua_if(%d) ERROR =%d sleeTcapIf.cc@%d: TC_BEGIN with no IDP/ARI (got %d.%d)	A TC-BEGIN from the network was received by an INAP handling i/f that did not contain an IDP nor ARI TC--INVOKE component.	Refer to application/signalling expert. Check interface configurred against the SSN for INAP if so contact support.	sua_if
402029	CRITICAL	DEF123sua_if: sua_if(%d) ERROR =%d sleeTcapIf.cc@%d: Conveyed protocol %d not supported by Slee Tcap i/f	Interface attempted to commence a dialogue with the SLEE with the unknown protocol.	Contact support.	sua_if
402030	ERROR	DEF123sua_if: sua_if(%d) ERROR =%d sleeTcapIf.cc@%d: TC primitive received without any components	A TC-BEGIN from the network was received with no TC--INVOKE component contained within it.	Refer to application/signalling expert. Suspected SSP misconfiguration.	sua_if
402034	ERROR	DEF123sua_if: sua_if(%d) ERROR =%d sleeTcapIf.cc@%d: Unknown correlation id %d	Interface attempted to commence a dialogue with the SLEE with the specified service key which is not configured in the SLEE.	Refer to application expert. Configure the displayed service key in SLEEs configuration file (SLEE.cfg)	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402036	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL =%d TcpConnection.cc@%d:%z	TCP/IP communications failure.	Refer to UNIX/application/LAN expert first (Check the following). 1) TCP/IP connection integrity. 2) Type netstat -na (see man netstat for more information) to determine the status of the listening socket for this connection. (Should be a configuration parameter). Finally contact support.	sua_if
402037	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL SleeException=%d sleeError.cc@%d:%z	Exception raised from SLEE.	Contact support.	sua_if
402038	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL: All STPs are unavailable.	All STPs has become inaccessible.	No resolution. Requires no action on platform.	sua_if
402042	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL SleeCallInstance::new()=%d sleeCallInstance.cc@%d: No available call instances	Error communicating with the SLEE.	Refer to application expert. Increase MAXEVENTS in SLEE.cfg if necessary.	sua_if
402050	CRITICAL	DEF123sua_if: sua_if(%d) CRITICAL SleeDialog::new()=%d sleeDialog.cc@%d: No available dialogs	Cannot process dialog.	Refer to application expert. Increase MAXDIALOGS in SLEE.cfg.	sua_if
402051	NOTICE	ZZZNOTICE =%d TcSccpCommonInterface.cc@%d: SCMG: N-STATE pc=%d, ssn=%d, multi=%d in service	The specified subsystem at the specified point code has come into service.	No resolution. Requires no action on platform.	sua_if
402052	NOTICE	ZZZNOTICE =%d TcSccpCommonInterface.cc@%d: SCMG: PC-STATE pc=%d accessible	The specified subsystem at the specified point code is accessible.	No resolution. Requires no action on platform.	sua_if

Alarm	Severity	Text	Cause	Resolution	Service
402053	NOTICE	ZZZNOTICE =%d TcSccpCommonInterface.cc@%d: SCMG: PC-STATE pc=%d inaccessible	The specified subsystem at the specified point code is inaccessible.	No resolution. Requires no action on platform.	sua_if