MiCLOUD

RELEASE 4.1

ALARMS DATABASE REFERENCE

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks" appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC or its subsidiaries (collectively "Mitel" or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

MiCloud Alarms Database Reference
Release 4.1
May 2018

MICLOUD ALARMS DATABASE

MIVOICE BUSINESS ALARMS

MIVOICE BORDER GATEWAY ALARMS

MiCloud Alarms Database

Introduction

This Alarms Database consolidates the system alarms that may be raised in the context of the Mitel MiCloud solution. It does not preclude its use by product-specific system administrators.

This Alarms Database is targeted for those Service Providers who have Technical Certification on the Mitel product suite deployed in line with the reference architecture being deployed. Additionally, Service Providers will have followed and completed the MiCloud Business for Service Providers Learning Map.

The system alarms contain constant, up-to-date records of all detected faults. Maintenance personnel may view the system alarms at any time via the System Administration Tool for MiVoice Business, or through the MiVoice Border Gateway interface, as appropriate. If an alarm threshold is reached, the system raises an alarm condition. The alarm condition remains until the fault is corrected. An entry is made in the Maintenance Log upon any change in the alarm status.

There are four classes of alarms: CRITICAL, MAJOR, MINOR, and NONE. Some of the alarm threshold levels are programmable. The following describes the various alarm classes. The color in brackets [color] indicates the color for single alarm LED systems.

Use the 'find-in-page' function of the browser to search for a command based on the page you are viewing. Most browsers launch 'find' using CTRL+F.

Alarm Status	Status Description
Critical [Red]	This is a total loss of service which demands immediate attention. A critical alarm invokes system-fail transfer. This LED is on when there is a critical Alarm, during Power Up, Reset or initialization, or when the license violation level is Critical or System Lock
Major [Orange]	This is a total loss of service which demands immediate attention. A critical alarm invokes system-fail transfer. This LED is on when there is a critical Alarm, during Power Up, Reset or initialization, or when the license violation level is Critical or System Lock.
Minor [Yellow]	A minor alarm is any fault which does not fall in either of the above two classes. Whenever the system is not 100% oper-

Alarm Status	Status Description
	ational, a minor alarm is raised. This may require the attention of a crafts person but is not urgent. Examples of a minor alarm include the loss of a single line or trunk circuit or the loss of one circuit switch link. This LED is on when there is a minor Alarm, during Power Up or Reset, or when the license violation level is Minor.
All [None]	No active alarm, or when the license violation level is Clear or Warning.

If an Alarm is Present on MiVoice Business

If the system is showing an alarm:

1. Log in to MiVoice Business and launch the System Administrator Tool.
2. From the navigation pane, select **Maintenance and Diagnostics > Alarms**.
3. Click **Alarm Details**.

    This will show you any/all alarms on the system.

To see alarms on other systems in the same Administration Group:

1. Select the system from the **Show form on** list in the top-right corner of the window
2. Click **Go**.

If an Alarm is Present on MiVoice Border Gateway (MBG)

1. In the upper right corner of the MSL Server Manager Page, click on the Alarm notification. The Event Log page displays.
2. Click **Clear Alarms** to clear all alarms, or click **Clear** next to the specific alarm to clear.

To view a list of all alarms and events, click **Event viewer** in the left navigation pane under **Administration**.

Supporting Documentation

Performing the corrective actions described in this document requires information from other sources. These sources are available on Mitel Online and on the Mitel Customer Documentation web site. Go here for more information.

Resolving Technical Issues

For advice on how to proceed when technical issues arise, click here.

TSN: Your Technical Support Network

The Mitel Technical Support Network (TSN) provides authorized channel partners with additional resources to help them help their customers.

MiCloud Alarms

The following is a list of MiCloud alarms:

MiVoice Business

- Audit Failure
- Backup Failure
- CESID
- Database Status
- ICP Comms
- Lic Violation
- CC Memory Avail
- SysMem Used (MB)
- SDS Sharing
- Security
- SIP Link
- Stale Tasks
- VM Port Status
- VTG_VM_ERROR
- VTG_VMDISK_FULL

MiVoice Border Gateway

- Bandwidth Limit
- Cluster Disconnected Peer
- Cluster Tug Rejected
- Excessive Jitter
- File Download Failed
- HTML App Missing
- Installer Password Rejected
- License Check
- master conflict
- Max Channels Exceeded
- Max Taps Exceeded
- Max Transcoding Exceeded
- Max Teleworkers Exceeded
- Max Users Exceeded
- One-way Audio
- Progress Alarm

- SIP Call Terminated
- SIP Trunk ICP Side Down
- SIP Trunk Remote Side Down
- Tug Absent
- Tug Crashed
- Tug Error
- UCA SSL Config Failure

Supporting Documentation

Performing the corrective actions described in this document requires information from other documents that are available on Mitel Online and on the Mitel Customer Documentation web site.

Accessing Mitel Online

To access Mitel OnLine:

1. Go to the following URL: http://www.mitel.com
2. Click Login.
3. Enter your Mitel Online username and password.

Access EDOCS for the Latest Documentation

The Mitel Customer Documentation (eDocs) site on Mitel OnLine provides the latest customer documentation.

The documentation for the current and previous product release are available from the main page. The documentation for other past releases are available from the Documentation Library link.

To view the available documentation, you will require:

- Internet access (high-speed is recommended)
- a web browser (e.g., Internet Explorer 7.0 or later)
- Adobe Acrobat Reader 4.0 or later
- Microsoft Word 97 or later
- Folio (for SX-200 ICP, SX-200 EL/ML, or SX-2000 LIGHT)
- your Mitel OnLine user name and password (required to access technical doc-umentation; user documentation is not password protected)

To access a technical document:

1. Log onto Mitel OnLine.
2. Click Support and then click Product Documentation.
3. Bookmark this URL.
4. In the left frame, select the product.
5. In the right frame, click the document.
6. If you click a technical document, you will be prompted for your Mitel OnLine username and password. Enter your username and password and click Login.
7. To access a generic user guide or quick reference card, click User Guides, click the desired language at the top of the frame, and then click the desired guide or quick reference card.

Resolving Technical Issues

Following a process to resolve technical issues can help minimize the impact of the technical issue and potentially identify a solution quickly, without wasting additional resources. Consider the following when analyzing a technical problem:

- If you are not certified on the product and release, ask a technician in your organization, with current certifications, to investigate the problem.
- Check the maintenance and software logs using the Check System section in the Technicians Handbook for instructions.
- Review the troubleshooting charts in the product's troubleshooting guide for a solution to the problem.
- Search the Knowledge Base to determine if a software update is available that remedies the problem.
- Visit Mitel Online and check other related documents and online help files for a potential solution.
- Verify there are no TBs or RNs describing a solution.
- Check the product's Engineering guidelines for any potential networking problems.
- Before you call Mitel technical support, ensure that the problem isn't being caused by another manufacturers equipment.
- Collected all the problem details before making a call to Mitel Support.
- If you have new information regarding the logged problem access the Online Services Desk and update your ticket.

TSN: Your Technical Support Network

The Mitel Technical Support Network (TSN) provides authorized channel partners with the following services:

- access through the Mitel OnLine website to:
  - up-to-date customer documentation
  - the Mitel Knowledge Base
  - the Online Service Desk (OSD) allowing you to view and update your Technical Support Tickets
- standard telephone support with current product releases during normal business hours
- after-hours emergency telephone support
- e-mail notification of new and updated technical documentation.

Before you can become a registered user, you must purchase a minimum of five technical consultation credits. Your technical consultation credits can be used to purchase telephone support (standard and emergency).

Contact Mitel Customer Services for purchasing technical consultation credits.

MiVoice Business Alarms

References

- MiVoice Business Troubleshooting Guide
- MiVoice Border Gateway Installation and Maintenance Guide
- MiVoice Border Gateway Engineering Guidelines
- MiVoice Border Gateway Remote IP Phone Configuration Guide

Audit Failure

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates a corrupted database.

Alarm Status

Major

Possible Cause	Corrective Action
Database Audit or Database Backup has detected a database corruption.	1. Collect required System Diagnostics. 2. Perform a system restore from your last known backup. If restore is successful, the alarm is cleared. 3. If the issue persists, contact Mitel product support for further investigation into the cause.

Backup Failure

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates a database backup failure.

Alarm Status

Major

Possible Cause	Corrective Action
Database Audit has detected a database corruption	1. Collect required System Diagnostics. 2. Perform a system restore from your last known backup. If restore is successful, the alarm is cleared. 3. If the issue persists, contact Mitel product support for further investigation into cause.

The Backup process was unable to stop the embedded voicemail application	1. Run the BUSY command:
	  • BUSY 1 4 27
	  • BUSY 1 4 28
	Note: If the port is in use after issuing the command, use the "Force" option to make sure that the port is in the manbusy state.
	
	2. Run the RTS command:
	  • RTS 1 4 27
	  • RTS 1 4 28
	3. Perform backup.
	4. If the issue persists, Run iPVM_Stop and iPVM_Start on the RTC shell to restart the application. Once the command is complete, attempt a manual backup. Note: this causes an interruption in voicemail services.

Insufficient disk space or file system corruption.	Provide System Diagnostics and any output from the RTC shell during the backup and contact Mitel product support.

CESID

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates that the system has detected a CESID assignment problem in an IP device that has automatic CESID updating enabled in the CESID Assignment form.

Alarm Status

Minor.

Possible Cause	Corrective Action
- A new or known IP device has registered, but no CESID is available for the device. - A device has moved, and no CESID is available for the device at its new location. - At system startup, one or more IP devices that have Automatic CESID Updating enabled but have no CESIDs assigned to them. - A new or known device has registered, but the CESID in the CESID Assignment form is different from the CESID in the L2 to CESID Mapping form.	Assign CESIDs in the CESID Assignment form or the L2 to CESID Mapping form. Once all DN CESID assignments are made, the system will clear the alarm.

Database Status

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates a corrupted database. The alarm is cleared when corruption is resolved.

Alarm Status

Major.

Possible Cause	Corrective Action
DMBS Check has failed	1. Run the SHOW FAULTS DATABASE STATUS command to determine cause of failure. If Corrupted Database is the cause of the failure, rerun DBMS CHECK FULL to see if the problem is resolved. [this is performance impacting command]. 2. If problem persists, perform a database backup and restore. Rerun DBMS CHECK FULL. 3. If problem persists, collect System Diagnostics logs and database backup and contact Mitel product support.
There is file system problem	1. Collect and evaluate the System Diagnostics logs. 2. If the Database is not corrupted, contact Mitel product support.

ICP Comms

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates a problem with IP trunks. The alarm is cleared when issue is resolved.

Alarm Status

Minor: > 0% < 25% of links unavailable.

Major: > 25% < 100% of links unavailable.

Critical: > 100% of links unavailable.

Possible Cause	Corrective Action

There is a network connectivity issue or the far end node is out of service.	1. Check your system logs to determine to which node(s) you have lost IP trunk connectivity.
	2. Check your network connectivity between impacted nodes and confirm that the nodes are in service.
	3. Check your system logs to determine when the trunk went down.
	4. Check your audit logs for any IP trunk configuration changes. If a change has been made, return to the original configuration.
	5. Check your audit logs for any service maintenance commands. For example:
	    • Check if the IP trunk was forced busy by looking for the following maintenance command variance:
	        • BUSY
	        • BUSY XNET
	        • BUSY TRUNK
	    • Enter the following command to bring the IP trunk in service variance:
	        • RTS
	        • RTS XNET
	        • RTS TRUNK
	6. If the alarm is not resolved, collect required System Diagnostics logs and contact Mitel product support.

Lic Violation

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates that a license violation has been detected by the License Manager or the Designated License Manager.

Alarm Status

The alarm can be one of:

- Minor
- Major
- Critical

The License Violation level is determined by the length of time the alarm has been active.

Possible Cause	Corrective Action
- Licenses have been over allocated. - Lost connectivity to the Designated License Manager.	Review the License and Options form and make the necessary changes. Investigate the connectivity between the Designated License Manager and MiVoice Business instance.

CC Memory Avail

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates the Call Control memory in use.

Alarm Status

Major.

Expressed as a percentage (%).

Possible Cause	Corrective Action
Memory or resource leak.	Reboot to reclaim the leaked memory. However, if the leak continues, collect System Diagnostics logs and contact Mitel product support.

SysMem Used (MB)

System/Sub-System

MiVoice Business: Hardware

Description

This alarm indicates the unavailability level of system memory expressed as a percentage (%) of the total system memory.

Alarm Status

Minor: < 50% memory available.

Major: < 25% memory available.

Critical: < 2% memory available.

Possible Cause	Corrective Action
System memory use has passed a threshold	Collect System Diagnostics logs and then reset system during quiet period. If resource recovery is enabled, when memory goes below 15M, a resource recovery reboot will occur.

SDS Sharing

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates System Data Synchronization (SDS) has detected that the number of distribution errors exceeds the threshold.

Alarm Status

Minor: >100 errors.

Major: >1000 errors.

Possible Cause	Corrective Action
- Network connectivity issue between the master and remote nodes. - One or more network nodes is down. - The SDS option is not enabled on the network nodes. - A device associated with the data distribution error is not programmed properly on the network node.	1. Resolve network issues. 2. Ensure remote node is up and running. 3. Ensure SDS option is enabled on all nodes. 4. Review the SDS Distribution Error form and resolve pending updates and distribution errors. If the issue is not resolved, contact Mitel product support.

Security

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates a user login failure.

Alarm Status

Major.

Possible Cause	Corrective Action
DISA user has been locked out of the system after reaching the configured amount of attempts.	1. Enter SHOW FAULT SECURITY maintenance command to help determine cause. Alarm is cleared on next successful DISA login. 2. If there are multiple unsuccessful attempts to access the DISA number, consider disabling the DISA number until the investigation is complete. 3. Review your DISA policy. Consider increasing account code lengths or changing the public DISA number. Consider replacing DISA access with EHDUs.
Several unsuccessful login attempts have been made on the TELNET port.	1. Enter SHOW FAULT SECURITY to clear alarm. 2. Review the software logs to determine the user who entered the incorrect user name. 3. Contact the user to confirm attempts. If it was not the registered user, this indicates a probable hack attempt and you should block the TELNET port access.
Security log failed to generate	1. Clear the alarm by entering the SHOW FAULT SECURITY maintenance command. 2. Collect System Diagnostics logs and contact Mitel product support

SIP Link

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates that the SIP link is not available.

Alarm Status

Minor: 10.

Major: 50.

Critical: 100.

Possible Cause	Corrective Action
Network communications failure	Check your network connectivity between MiVoice Business and the IP address provided by your SIP service provider.
SIP link failed to register	Check your System Diagnostics logs to determine when the link went down. Check your audit logs for any SIP trunk configuration changes. If a change has been made, return to original configuration.

Maintenance is being performed on the SIP links, causing the link to go down. The SIP link may have been brought down intentionally.	Check your audit logs for any service maintenance commands. For example:
	
	• Check if the SIP link status, issue SIP LINK STATUS or SIP LINK STATE PEER <PEER_Name>
	• Check if the SIP link was forced busy by the following maintenance commands:
	   • SIP BUSY FORCE PEER < PEER_NAME>
	   • SIP BUSY PEER

Possible Cause	Corrective Action

	<PEER_NAME>
	• Enter the following command to bring the SIP link in service:
	  • SIP RTS PEER <PEER_Name>) launched
	• If the alarm is not resolved:
	  • Contact your SIP service provider to determine changes that may have been made to your SIP service.
	  • Collect required System Diagnostics and contact Mitel product support.

Stale Tasks

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates if the task or component is suspended and present in the Task and Component Task Restart list, while the system is being monitored.

Alarm Status

Major: A non-critical task is suspended.

Critical: A critical task is suspended.

Possible Cause	Corrective Action
A non-critical or critical task has been suspended.	Reset the system by entering the Programmed Reboot maintenance command with the Resource Recovery time cycle. For a Major alarm, if configured, the system will be reset at the next resource monitoring reboot time. For a Critical alarm, the system will reset immediately.

VM Port Status

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates some Embedded Voice Mail ports are unavailable.

Alarm Status

Minor: When an Embedded Voice Mail port is unavailable.

Possible Cause	Corrective Action
The MiVoice Business instance has lost connection to the Media Server or maintenance is being performed on the ports.	Check logs to see if it is a Media Server issue. If it is a Media Server issue, reboot the MiVoice Business instance.
Maintenance is being performed on the ports.	Check AUDIT logs for maintenance commands on the specified PLIDs. Look for the following BUSY commands, for example: • BUSY 1 4 27 • BUSY 1 4 28 If the PLIDs are BUSY, eturn the ports to service when appropriate.

VTG_VM_ERROR

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates one of the following:

- The embedded voice mail application has failed to start.
- Voicemail database corruption

Alarm Status

Major

Possible Cause	Corrective Action
- The voice mail prompt files are not installed properly, or the voice mail application is unable to communicate with MiVoice Business call control. - Voicemail files are missing or corrupted.	1. Collect System Diagnostics logs. 2. Run iPVM_Stop and iPVM_Start on the RTC shell to restart the application. 3. If not resolved, reboot the MiVoice Business instance. 4. If the issue persists, contact Mitel product support.

VTG_VMDISK_FULL

System/Sub-System

MiVoice Business: Software

Description

This alarm indicates an Embedded Voice Mail disk usage error.

Alarm Status

Minor: >= 95% disk usage.

Major: >= 98% disk usage.

Critical: 100% disk usage.

Possible Cause	Corrective Action
The threshold for embedded voice mail disk use has been exceeded.	1. Increase the amount of disk space available by having users delete old voicemail. Consider configuring EMEM to delete old voicemails using VM Mailboxes form. 2. If issue is not resolved, contact Mitel product support.

MiVoice Border Gateway Alarms

References

- MiVoice Business Troubleshooting Guide
- MiVoice Border Gateway Installation and Maintenance Guide
- MiVoice Border Gateway Engineering Guidelines
- MiVoice Border Gateway Remote IP Phone Configuration Guide

Bandwidth Limit

System/Sub-System

MBG: Software

Description

This alarm indicates a bandwidth limit condition has been reached, and MBG must limit calls.

Note: this alarm presents only if a bandwidth limit has been configured on MBG. Otherwise, it has no knowledge of link capacity.

Alarm Status

Major: When calls are being rejected.

Possible Cause	Corrective Action
The configured bandwidth has been exceeded by the number of active RTP streams.	1. Provision more WAN bandwidth and raise the limit appropriately. 2. Consider reducing the number of configured users on this node. 3. Review MBG bandwidth metrics graph monthly to see if it is approaching the limit.

Cluster Disconnected Peer

System/Sub-System
MBG: Software

Description
This alarm indicates a node in a cluster has disconnected from a peer node (ie. not the master).

Maintenance commands are valid for this alarm.

Alarm Status
None

Possible Cause	Corrective Action
A node in a cluster disconnects from a peer node (ie. not the master)	1. Check your network connectivity between the two MBGs. 2. If the alarm is not resolved, collect required logs and contact Mitel product support.

Cluster Tug Rejected

System/Sub-System
MBG: Software

Description
This alarm indicates an attempt to cluster with another server failed.

Alarm Status
None

Possible Cause	Corrective Action
The remote server has rejected an attempt to cluster.	1. Review tug.log for error messages. 2. If the alarm is not resolved, collect required logs and contact Mitel product support.

Excessive Jitter

System/Sub-System

MBG: Software

Description

This alarm indicates a set has experienced excessive jitter in the voice of a call.

Alarm Status

None

Possible Cause	Corrective Action
Network congestion or network equipment problems. For soft phones and applications, the host PC may be overloaded.	1. Check your network connectivity between the remote set and the WAN side of the MBG. 2. Go to the Events viewer in the MBG Server Manager and clear the alarm. Refer to the Voice Quality Guide for additional details.

File Download Failed

System/Sub-System

MBG: Software

Description

This alarm indicates that a required file from the upstream MiVoice Business instance has failed to download to the server.

Alarm Status

None

Possible Cause	Corrective Action
The requested file is missing on the MiVoice Business instance.	Contact Mitel product support.

HTML App Missing

System/Sub-System

MBG: Software

Description

This alarm indicates a requested HTML application file cannot be found on the upstream MiVoice Business instance.

Alarm Status

None

Possible Cause	Corrective Action
The requested file is missing on the MiVoice Business instance.	1. Ensure the file is available on the upstream MiVoice Business instance. 2. If alarm is not resolved, contact Mitel product support.

Installer Password Rejected

System/Sub-System

MBG: Software

Description

This alarm indicates an unsuccessful registration of a MiNET device using the installer password.

Alarm Status

None

Possible Cause	Corrective Action
An incorrect password was entered.	Enter the correct password on the MiNET device.

License Check

System/Sub-System

MBG: Software

Description

This alarm indicates a failed license check.

Alarm Status

Major

Possible Cause	Corrective Action
License check failure.	1. Ensure system has a valid ARID. 2. Sync with the AMC to refresh license database.

master conflict

System/Sub-System

MBG: Software

Description

This alarm indicates an attempt at cluster synchronization when more than one master node is discovered. This situation must be manually corrected.

Alarm Status

None

Possible Cause	Corrective Action
There is more than one master node.	Review the cluster configuration and ensure one master node is selected.

Max Channels Exceeded

System/Sub-System

MBG: Software

Description

This alarm indicates a user has exceeded their available licenses for SIP trunking.

Alarm Status

Major: When service affecting

Possible Cause	Corrective Action
The number of SIP trunking licenses has been exceeded.	- Acquire more licenses. - Consider reducing the number of simultaneous calls on the trunk. - Review MBG metrics graphs monthly to monitor usage.

Max Taps Exceeded

System/Sub-System

MBG: Software

Description

This alarm indicates the call recording equipment exceeds the available number of tap licenses.

Alarm Status

Major: When service affecting.

Possible Cause	Corrective Action
Call recording equipment has exceeded the available number of tap licenses.	- Acquire more licenses. - Consider reducing the number of simultaneous recorded calls on the call recording equipment. - Review MBG metrics graphs monthly to monitor usage.

Max Transcoding Exceeded

System/Sub-System

MBG: Software

Description

This alarm indicates the number of transcoded calls on proxied sets exceeds the available number of transcoding licenses.

Alarm Status

Major: When service affecting.

Possible Cause	Corrective Action
Number of transcoding licenses exceeded for proxied sets.	• Acquire more licenses. • Consider reducing the number of simultaneous transcoded calls. • Review MBG metrics graphs monthly to monitor usage

Max Teleworkers Exceeded

System/Sub-System

MBG: Software

Description

This alarm indicates the number of supported sets exceeds the maximum number of Teleworker (NAT) licenses.

Note that these licenses are used when a device is behind NAT.

Alarm Status

Major: When service affecting.

Possible Cause	Corrective Action
Number of Teleworker licenses exceeded for supported sets.	• Acquire more licenses. • Consider reducing the number of sets connected to this node or cluster. • Review MBG metrics graphs monthly to monitor usage.

Max Users Exceeded

System/Sub-System

MBG: Software

Description

This alarm indicates the number of supported sets exceeds the maximum number of user (device) licenses. These licenses are used regardless of being behind NAT.

Alarm Status

Major: When service affecting.

Possible Cause	Corrective Action
User device licenses exceeded.	Reduce the number of sets provisioned for this MBG. The number of sets per node is a hardcoded limit.

One-way Audio

System/Sub-System

MBG: Software

Description

This alarm indicates a set has experienced one-way audio and MBG detected impairments in the call. The event is mainly logged to correlate detection with customer complaints.

Alarm Status

None

Possible Cause	Corrective Action
A network or firewall configuration issue. Persistent cases are usually due to a misconfigured firewall.	1. Check your network path between the remote set and the receiving equipment. 2. Check the tug.log to determine which set was experiencing the one-way audio. 3. If the tug.log determines the issue is on the WAN network side, contact your IP service provider to determine changes that may have been made to your IP service. 4. Check that the firewall configuration meets the *MBG Engineering Guidelines* requirements. 5. If the alarm is not resolved, collect required logs and contact Mitel product support.

Progress Alarm

System/Sub-System

MBG: Software

Description

This alarm indicates the event daemon is falling behind attempting to process the event queue.

Alarm Status

None

Possible Cause	Corrective Action
Typically caused by a temporary burst of activity.	Normally, no action is required and the condition will clear itself. However, if the event queue size in the Clustering interface is not decreasing, the system may be overloaded. Review the MBG Engineering Guidelines for performance limits. If the system is within specifications, contact Mitel product support.

SIP Call Terminated

System/Sub-System

MBG: Software

Description

This alarm indicates a SIP call has been terminated due to bandwidth constraints.

Alarm Status

None

Possible Cause	Corrective Action
The call was terminated to make room for an emergency call when bandwidth was low.	Provision more WAN bandwidth or reduce call volume on this pipe. Review bandwidth metrics graph monthly.

SIP Trunk ICP Side Down

System/Sub-System

MBG: Software

Description

This alarm indicates a SIP trunk has gone down on the MiVoice Business instance.

Alarm Status

None

Possible Cause	Corrective Action
The MiVoice Business instance is unreachable or not responding.	1. Check your network connectivity between MiVoice Business and the IP address provided by your SIP service provider. If all MiVoice Business instances are down, the trunk is out of service and incoming calls will be rejected. 2. If the alarm is not resolved, contact your SIP service provider to determine changes that may have been made to your SIP service. 3. If the alarm is not resolved, collect required logs and contact Mitel product support.

SIP Trunk Remote Side Down

System/Sub-System

MBG: Software

Description

This alarm indicates a SIP trunk has gone down on the remote side.

Alarm Status

None

Possible Cause	Corrective Action
The service provider Session Border Controller (SBC) is not responding.	1. Check your network connectivity between MiVoice Business and the IP address provided by your SIP service provider. If all MiVoice Business instances are down, the trunk is out of service and incoming calls will be rejected. 2. If the alarm is not resolved, contact your SIP service provider to determine changes that may have been made to your SIP service. 3. If the alarm is not resolved, collect required logs and contact Mitel product support.

Tug Absent

System/Sub-System

MBG: Software

Description

This alarm indicates the heartbeat checks between the main service and the event daemon exceed the maximum time allowed.

Alarm Status

Critical: When there is no service.

Possible Cause	Corrective Action
Heartbeat checks between the main service and the event daemon exceed the maximum time allowed.	Collect required logs and contact Mitel product support.

Tug Crashed

System/Sub-System

MBG: Software

Description

This alarm indicates a core file is discovered by the event daemon indicating that the main call processing service has gone down.

Note that the main service is automatically restarted in the event of such a crash.

Recovery is rapid.

Alarm Status

Major: When all calls in progress drop.

Possible Cause	Corrective Action
A core file has been created from the main service.	Report the crash to Mitel product support.

Tug Error

System/Sub-System

MBG: Software

Description

This alarm indicates that the main service cannot be brought up to provide service.

Alarm Status

Critical: When there is no service.

Possible Cause	Corrective Action
The main service is misconfigured and cannot provide service.	1. Stop MBG. 2. Confirm that all network interfaces are up. 3. Ensure interfaces do not contain duplicate IP addresses. 4. If all interfaces are in service, contact Mitel product support.

UCA SSL Config Failure

System/Sub-System

MBG: Software

Description

This alarm indicates the SSL configuration for MiCollab Client has failed to work properly.

Alarm Status

Major: When there is no MiCollab Client service.

Possible Cause	Corrective Action
The uploaded certificate is in the wrong format or is missing the intermediate Certificate Authority (CA) certificates.	1. Re-upload the web certificate including the intermediate SSL certificate. 2. Check that the certificate is in the proper format. If it is not, contact CA for a certificate in the proper format.