OpenScape Session Border Controller

OpenScape SBC V11
OpenScape Branch

Troubleshooting Guide
August 2025

A31003-S5300-S101-04-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. 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), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

2. History of Changes

Version	Date	Description
1.0	2023-08-01	Initial release
2.0	2024-07-30	Rebranded to the Mitel layout
3.0	2025-02-20	Added Chapter 7 Cloudlink troubleshooting
4.0	2025-02-20	Added the Zoom troubleshooting guide

3. SBC / OSB common logs

3.1 Sip signaling issues

To troubleshoot **Signaling** issues, collect the required logs and perform the actions mentioned below:

1. Collect specific timestamps and Call-IDs.

2. Collect Network (NW) traces for the SIP (Session Initiation Protocol) and MGCP (Media Gateway Control Protocol) interfaces: Navigate to **Diagnostics & logs → Debugging → Debugging Tools → Tool → Network Tracer → Interface SIP/MGCP Trace**.

3. Set **SipServer** and **Session State Manager** (**SSM)** to **Info** or **Debug** Level (Out of BH) mode: Navigate to **Diagnostics & logs → Settings.** Click **Apply changes** to enable the selected logging level.

4. Set **Rapidstat** to **level 5.**

5. If possible, include a good (trouble-free) case.

3.2 Payload issues (RTP / SRTP)

To troubleshoot **RTP** issues, collect the required logs and perform the actions mentioned below:

1. Collect specific timestamps and Call-IDs.

2. Collect Network (NW) traces for SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol), and RTP (Real-time Transport Protocol): Navigate to **Diagnostics & logs → Debugging → Debugging Tools → Tool → Network Tracer → Interface SIP/MGCP/RTP Trace.**

3. Set **SipServer** and **Session State Manager** (**SSM)** to **Info** or **Debug** Level (Out of BH) mode. Navigate to: **Diagnostics & logs → Settings.** Click **Apply changes** to enable the selected logging level.

6. Set **Rapidstat** to **level 5.**

7. If possible, include a good (trouble-free) case.

For OSB the NW capture **Interface** selection includes also Q931 for calls over PSTN, i.e., PRI & BRI

3.3 GUI-related errors

If local GUI is unresponsive or malfunctioning, follow these steps:

1. Check CPU usage: Use the **top** command to monitor if there is a High CPU load reported for the **httpd2-prefork** process.
2. To recover, execute the following command in the terminal:

```
/usr/sbin/httpd2-prefork -k restart
```

3. Check the **php.log** located under **/var/log/apache2/** for errors.

3.4 System errors

To identify and resolve system errors:

1. Collect **Coredumps** and **Memdumps** with Rapidstat.
2. Session State Manager (SSM) dumps can be found under **/osb/var/core(/opt/openbranch/var/core.**
3. Log files can be found under **/var/log/.**
   Specifically, check the following files:
   - **Messages**
   - **systemd.log**
   - **warn**

System Resources depletion can lead to system stuck or service degradation. This can be identified if in the **pm.log** file the following entries are logged:

```
[alert] Command "/sbin/reboot" aborted: Wait Timeout

[alert] Reboot failed (1): Wait Timeout
```

In that case, the following log is additionally needed for analysis:

1. **report.log** under **/osb/var/log/openbranch.**

2. Running processes status

   - **Single process:**

     ```
     pmc show <process name>
     ```

     i.e., `pmc show ssm`

     ```
     State: SCAN Redmod: MASTER Opmod: CSBC Reboot: ALLOWED Runs: 10463

     Scan: ON    Stable: STABLE DBChk: STOPPED Licref: ALLOWED Cmds: ALLOWED
     SFlags:

     name (Status, State, Stable) Alarm Grps Starts PID    IOE Uptime

     ssm (STARTED, running, STABLE) NO  4 0  s-1392 ...  476682 PM-Done
     ```

   - **All process:**

     ```
     pmc show
     ```

     i.e., System status, Redundancy mode & Operation mode

     ```
     State: SCAN Redmod: S.ALONE Opmod: CSBC   Reboot: ALLOWED  Runs: 32847

     Scan: ON    Stable: STABLE DBChk: STOPPED Licref: ALLOWED Cmds: ALLOWED
     SFlags: PM-Done
     ```

3.5 Network issues

To troubleshoot network issues like connectivity with other NW endpoints (i.e., OSV, SSPs, redundant node, devices etc.), follow these steps:

1. Collect timestamps.

2. Set **Rapidstat** to **level 5.**

3. Check dos logs**: `/var/log/dos.log`** and **`/var/log/dos_quarantine_history.log.`**

4. Collect Network (NW) traces: Navigate to **Diagnostics & logs -> Debugging → Debugging Tools → Tool → Network Tracer → Interface** "**All**".

5. Check and collect the results of network commands:

- Routel
- ip link
- ip route
- ip addr
- ping GW / endpoints that are not responding
- iptables -L
- route -n

6. Execute the command arping and check if this endpoint responds to ARP requests:

```
(Endpoint/GW) -c 4 -f -I eth2 2>/dev/null
```

For redundancy-specific issues, you will also need the following from both nodes:

1. Check **`/var/log/openbranch/redmng.log`.**
2. Set the redundancy logs to debug level:
   Navigate to **Diagnostics & logs** → **Settings** → **Redundancy**.
3. Collect **Rapidstat** data from the backup node at **level 5**.

3.6 Update / Upgrade issues

To troubleshoot update or upgrade issues:

1. Gather information from the update log found at: **`/var/log/openbranch/.`**
   In case an update cannot be performed, the error message "*The restart operation has failed. Try again in 10s"* is displayed.
2. Check if the following file is present: **`/etc/openbranch/flags/pm.backup.blocked`**. In case there is no active upgrade in process, the file can safely be removed, and you can try again the new upgrade.
3. Execute the appropriate command to run **RapidStat** from the CLI.
4. Export RapidStat Output: Once **RapidStat** has been executed, the output will be displayed in the CLI. To save the **RapidStat** data for further analysis, you can copy and paste the output into a text file or use any available file transfer method to move the data to another system for storage.

Remember that taking a **RapidStat** manually is essential in situations where network connectivity is not available, or the GUI cannot be accessed. This will provide valuable diagnostic information that can help in troubleshooting and resolving hardware and software-related issues.

To collect **Rapidstat** at **level 5** follow these steps:

1. Run as root (default is level 5):

```
/osb/bin/sc.sh
```

2. If there is no way to transfer out the **Rapidstat** a USB can be used:
   - Connect an USB drive to the system.
   - Run the following command:

```
mount.osb usb
```

   - The USB must be available in **`/mnt/system/usbstick.`**
   - Copy the result file:

```
cp /osb/var/upload/* /mnt/system/usbstick
```

3.7 SSP Registration or connectivity issues

To troubleshoot SSP (Sip Service Provider) registration or connectivity issues, follow these steps:

- If possible, collect specific Timestamps and Call-IDs.

- Collect Network (NW) traces: Navigate to **Diagnostics & logs → Debugging → Debugging Tools → Tool → Network Tracer → Interface All**.
  For SIP layer issues, enable the **SIP/MGCP Trace** interface in the Network Tracer. This provides decoded SIP messages in case there is signaling encryption: Navigate to **Diagnostics & logs → Debugging → Debugging Tools → Tool → Network Tracer → Interface SIP/MGCP Trace.**

4. Set **SipServer** and **Session State Manager** (**SSM)** to **Info** or **Debug** Level (Out of BH) mode. Navigate to: **Diagnostics & logs → Settings.** Click **Apply changes** to enable the selected logging level.

5. Set **Rapidstat** to **level 5.**

6. If possible, include a good (trouble-free) case.

4. OSB common issues

4.1 Unresponsive hardware OSB (500/50i)

In case the OSB becomes unresponsive, follow these steps:

1. Perform a power cycle by shutting down the system and then turning it back on. This action can help bring the system back to a responsive state.
2. If the OSB is a non-redundant configuration, after the recovery, ensure that the watchdog feature is not enabled. Watchdog is used to monitor system processes and automatically restart the system in case of failures. However, in certain cases, it may interfere with troubleshooting efforts and lead to recurring issues.
3. After the system has recovered, gather **Rapidstat data** at **level 5**. This will help identify any underlying issues contributing to the unresponsiveness.

If the issue is recurring, please contact the next level of support (GVS/DEV teams) to verify if **SystemCollector** must be enabled or to ask them to provide instructions on enabling **Serial output** for kernel messages.

5. Licenses issues

5.1 General Info

To gather general information and check for possible license component issues, follow these steps:

1. Check **pm.log** for possible license component issues.
2. To get status and license info (i.e., SIEL, license type, etc.), run the following command:

```
pmc lic
```

5.2 Floating licenses

To troubleshoot communication issues and errors between OSB/SBC Assistant and the current appliance, check and collect **soap.log** for communication issues and errors between OSB / SBC assistant and current appliance.

5.2.3 Workarounds

If there are authentication statement expiration issues or communication problems, follow the workarounds described below.

Renegotiating the OSBs to allow insecure communication:

1. Navigate to **Configuration→OpenScape Branch or OpenScape SBC → Branch office list or OpenScape SBC list**.
2. Choose one endpoint and click **Edit**.
3. Uncheck the **Communicating over Secured channel** and click **OK**.
4. Select again the same endpoint and click **Refresh Selected**.
5. Continue with the same endpoint and click **Manage**.
6. In the new pop-up window click **Device license update**.

   The license should be successfully updated to OSB or SBC.

Assistant soaphandler issue:

If assistant's **SoapSupportHandler** is malfunctioning licenses cannot be retrieved. In that case the following error will be reported at the symphonia logs:

> *Service instance: com.siemens.ob.interfaces.generated.interf.SoapSupportHandler not found in registration.*

To address the Assistant **SoapSupportHandler** issue and retrieve licenses, check the handler status, and restart the assistant:

1. Navigate to **Maintenance→ Inventory → Nodes.**
2. Select the offboard (type: **Application**).
3. Click **Show Services Status.**
4. In the popup message, type ***SoapSupport*** on the filter textbox.
5. Check the relevant service and then click **Restart**.

If the restart of the **SoapSupportHandler** does not resolve the problem, consider restarting Symphonia as a further step to address the issue.

Nevertheless, regardless which of the two workarounds will solve the problem, it may be necessary to renegotiate the OSBs / SBCs to ensure they can communicate effectively after the issue is resolved.

6. Loggers (per available component) and Levels

6.1 Common Loggers for SBC/OSB

Log Viewer

The Log data drop-down box allows the user to select the application for which to retrieve the log. After selecting the desired log, click **Show** to view it in a new window. The **Clear** button is used to clear the selected log file in the Log data field. Note that the Log Settings section allows the user to choose the level of information to capture in a log.

While viewing a log, it is possible to clear the file, export it to a local file, or close the window. Possible choices for log data viewing are shown in **Table 1**.

Table 1: Log data overview

Log data viewing choices	Description
Alarm History	Alarm history displays details about triggered alarms in the system, such as activation or clearance time and threshold information.
Alarm Manager	Alarm Manager Log displays application events, aiding in troubleshooting scenarios like untriggered alarms, false activations, or incomplete clearances.
Boot	Last system boot log helps debug issues with incorrectly installed processes or driver modules and identifies hardware failures. It also ensures proper detection and configuration of system capabilities.
Continuous Tracing	Continuous trace is responsible for collecting the logs from the applications performing log rotation, compression, and aging tasks.
Current processes	A list of the current processes running on the Branch.
Media Server Adapter	Media Server Adapter log, MGCP Adapter and SIPMGCP converter applications.
Install/Update/Upgrade	The provided logs by the software installation tools track system upgrades or updates via local files, SSH or SFTP and initial installations via USB stick or software image.
Process Manager	Process Manager logs monitor the system's sanity, including status checks, starting, or stopping processes when necessary. It is also responsible for deployment configuration, facilitating fallback to a previous system partition in cases of upgrade issues, invalid configuration or corrupted current system partitions.

Redundancy	The Redundancy Manager Log provides details about the Redundancy Manager application. It handles debugging issues related to redundancy process functionalities, such as switchover failures.
RTP Proxy	The RTP Proxy Log is responsible for relaying RTP packets between different interfaces and enabling VoIP features interworking, such as transcoding, transrating (forced packetization time – ptime), SRTP, ICE, STUN, etc. These logs help debug issues related to these features, particularly voice quality problems, DTMF, FAX T.38, rtcp-mux, and other related matters.
SIP Server	The SIP Server Log, a Kamailio application running in the system, handles SIP signaling and serves as the external SIP interface for the system. It helps in debugging call processing issues, SIP connection problems, and various other challenges, including registration, port mapping, number modification, DNS, NAT, Options Heartbeat, and more.
SIP Service Provider	SIP Service Provider log shows details about the SSPs Registration process.
SSM	The SSM (Session State Manager) collaborates with SIP Server to provide some SIP functionalities and interworking with SIP Service providers. Their logs are needed for troubleshooting call failures related to SSPs (SIP Service Providers), MoH (Music on Hold) for subscribers on SM (Session Manager), SipRec (SIP Recording), and calls using anchored SBC (Session Border Controller) sessions, such as codec transcoding.
Survivability Provider	The Survivability Provider application is responsible for the OPTIONs heartbeat functionality, that indicates the system operational mode (SM, NM, etc.). It also handles SSP registration and BCF Notifications functionalities.
System	The System log includes the Kernel logs and helps in debugging issues related to the operational system and device drivers (sensors, ethernet, etc.).
Web Server	Local Web Server application logs help in debugging the local management, GUI interface and XML-related issues.

6.2 OSB extra Loggers

Table 2 displays OSB loggers and other component-related loggers.

The **Show** button opens a new window or tab to present the log information.

The **Clear** button clears the selected log file. The **Alarm History**, **Boot**, **Current processes,** and **Web Server** logs cannot be cleared.

The **Clear All Logs** button clears all logs, except for **Alarm History**, **Boot**, **Current processes,** and **Web Server**.

NOTE: It is recommended not to clear all logs because any critical information may be missed.

Table 2: OSB loggers

OSB logger	Description
B2BUA	B2BUA is an Asterisk running in the system. It has three main functions: work as a B2BUA for gateways and SSPs in Survivability Mode; provide some functionalities like ACD, Auto Attendant, MLHG and Voicemail; provide the Integrated Gateway functionality for PRI, BRI, FXS and FXO boards. This log is useful for debugging all these functions, regarding the Integrated Gateway it is necessary to investigate call processing, DTMF detection, FAX T.38, voice quality issues, etc.
CAS MFC R2	Log of the CAS MFC R2 signaling. This signaling is applicable only for E1 interface. This log is useful to debug all CAS MFC R2 call establishment and features issues.
CAS E&M/Ring Down	Log of the CAS E&M/Ring Down signaling. This signaling is applicable for both T1 and E1 interfaces. This log is useful to debug all CAS E&M/Ring Down call establishment issues
CDR	Logs from Call Detail Recording that is the application that records in a ticket the information regarding caller, called parties call duration etc., for a call that was done during the survivable mode. The tickets are internally stored until the external server retrieved them.
DAHDI	Log of the DAHDI driver. Applies to the OSB 50i and OSB 500i only. This log is useful to debug problem in the PRI, BRI, FXS and FXO ports alarms. It is also useful to debug FXO and FXS signaling, along with B2BUA logs.
ISDN	Log of the ISDN Layer 2 and Layer 3 ISDN messages (BRI and PRI ports). This log is also included in the B2BUA logs when set to level INFO or DEBUG. Level INFO includes Layer 3 messages, and it is useful to debug call processing issues, along with B2BUA logs. Level

	DEBUG includes Layer 3 and Layer 2 messages. This level is very verbose and must only be activated to debug Layer 2 issues, like link establishment and BRI PTMP issues.

6.3 SBC extra Loggers

Table 3 displays SBC loggers and other component-related loggers.

Table 3: SBC loggers

SBC logger	Description
GTC App	Logs for the GTC Client application, which are needed for troubleshooting failures related to phone calls to/from Circuit.
QoS Application	This is the log of QoS send TRAP application that sends over SNMP the QoS information to the QDC server that monitors the quality of voice calls.
The Circuit Zookeeper Client	It is enabled using the **Enable Circuit Zookeeper Client** check box.

6.4 Call Log Settings (only for SBC)

This setting upgrades the log level to DEBUG for the **SIP Server, SSM** and **RTP Proxy** applications, based on the criteria selected:

1. Log call started from number.
2. Log call to the destination number.
3. Log call initiated from remote address.
4. Log call received on host address.
5. Log for SIP methods.

All other settings will remain as configured.

6.5 Logs location

- **OpenScape Branch logs:**

  You may find the OSB logs under the following file path:

  /var/log/openbranch

  ctrace.log, netctl.log, pkimng.log, swphone.log, alarm.log, rtpproxy.log, sp.log, ssm.log, wdt.log, alarm.hist.log, redmng.log, pm.log, osbpasswd.log, cdr.log

- **Storage of old logs:**

  /osb/var/log

  b2bua.log_XXXXXX.log.bz2, boot.log_ XXXXXX.log.bz2, db_upd_ip_from_fqdn.log_ XXXXXX.log.bz2, firewall_ XXXXXXX.log.bz2, kernel.log_XXXXXX.log.bz2, messages_XXXXXX.log.bz2, secure_XXXXXXX.log.bz2, sipserver.log_XXXXXXX.log.bz2, sudo.log_XXXXXXX.log.bz2, systemd.log_XXXXXXX.log.bz2, timers.log_XXXXXXX.log.bz2, warn_XXXXXXX.log.bz2

- **Storage of old logs (2nd storage):**

  /osb/var/log/openbranch

  alarm.hist.log_XXXXXX.log.bz2, alarm.log_ XXXXXX.log.bz2, alert.log, cdr.log_ XXXXXX.log.bz2
  ctrace.log_ XXXXXX.log.bz2, gw_report.log, osbpasswd.log_ XXXXXX.log.bz2, pm.log_ XXXXXX.log.bz2
  redmng.log_ XXXXXX.log.bz2, report.log, report.log_ XXXXXX.log.bz2, rtpproxy.log_ XXXXXX.log.bz2
  shell.log, sp.log_ XXXXXX.log.bz2, ssm.log_ XXXXXX.log.bz2, ssp.log_ XXXXXX.log.bz2, update.log_ XXXXXX.log.bz2

7. Zoom

For Zoom troubleshooting, refer to the Zoom troubleshooting guide: **Zoom, Mitel Phone System Integration (PSI) with Zoom Troubleshooting , Service Documentation.**