A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

Troubleshooting Guide

Service Documentation
06/2026

A31003-P3040-S100-01-7620

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

1 History of changes

Changes mentioned in the following list are cumulative.

Changes in V4

Impacted chapters	Change description
-	Initial creation of the document

1.1 History of improvements

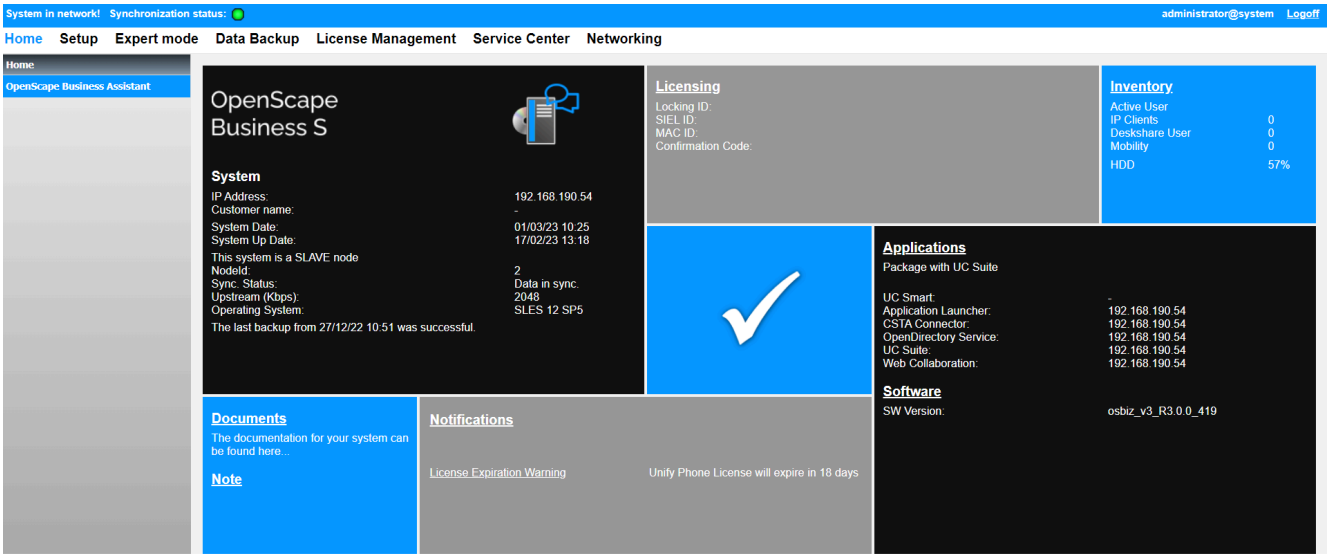
Changes mentioned in the following list are cumulative.

Changes in V3R4

Service case ID	Date of change	Description of change	Impacted chapters
PRB000080374	12 Nov 2024	Correction of link under step 5	UC Suite Clients Crash or Freeze – Process Dump on page 24

2 What can I do in case of an issue?

Check hints and warnings on the landing-page first.



3 Which information and data is needed for an efficient clearing within Unify

- Detailed description of the customer's problem scenario
  - Is the issue reproducible?
  - Describe exactly what happens, including details
  - Call handling via Handset/Headset/Application?
  - Which user (subscriber no.) was involved? When (exact time stamp)? Other users involved as well?
  - Try again with another device or PC. Is the issue reproducible here as well?
  - Check call flow and try to simplify the scenario
- List of all involved components including corresponding software versions
  - including Client PC details for OS 32/64bit and MS Office versions/ service packs
- Provide at least default traces of system and applications
  - UC-Suite/MyPortal/MyAttendant/MyAgent/MyPortalSmart
- Make use of additional trace profiles / trace info
  - Depending on the problem scenario, additional trace profiles can be used
  - For sporadic issues that are solved with a system restart and come up again after some time, corresponding traces should be activated AND **customer should provide traces from the system restart until the problem happens again**
  - Specific to undesirable System Restarts, it is vital to collect also Core Logs from the faulty environment.
- Always download complete trace data package
  - Diagnostic backup / KDS / trace data

4 Trace settings / recommendations

Basic Trace- / Ticket data which is required

- If possible please activateRSP.servicelink
  - Please enable remote access for Unify and provide credentials
- Manager E user credentials and password
- WBM user credentials and password
- If applicable: Linux user credentials and root access password
- Customer KDS
- Diagnostic backup
- **Plus** : additional trace data, depending on problem scenario. More details on subsequent pages.

  Remark: For scenarios where OSBiz environment contains multiple nodes interworking in a Network configuration, it is required that diagnostics are collected from all involves nodes that take part in a specific scenario.
- To reduce the amount of data to be transferred to Unify, trace slices for certain time frames can be downloaded from the system. Check that you've captured the correct time frame on when the issue has occurred.
- **After downloading all trace data it's mandatory to switch trace profiles back to default!!**
  - **Only Trace Profile** Basic **and** Voice_Fax_connection **are allowed to stay active**

Certified Environments:

Prior to escalating a customer ticket, please consult the Overview Certification portal for compliance.

Compliant VoIP Providers by Countries:

https://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers#Tested_VoIP_Providers_by_Countries

5 Add-on trace profiles depending on problem scenario

SIP phone issues

- Basic
  - Voice_Fax_connection
  - SIP_Interconnection_Subscriber_ITSP
  - SIP_Registration

Add-on trace profiles depending on problem scenario

- Network plan overview
- List of network components involved
- Wireshark traces
- Firewall configuration
- Device trace (see trace guide SIP phone Wiki.unify.com)

https://wiki.unify.com/images/a/a7/Service_Info_How_to_trace_SIP_2.pdf

6 Additional trace data depending on the use-case scenario

6.1 HFA phone issues

Trace Profiles

- Basic
- Voice_Fax_connection
- Calls_with_System_Device_HFA

Add-on trace profiles depending on problem scenario

- Display_problems

  issues with phone display notifications
- Gateway_stream_overview

  issues with payload
- Wireshark traces
- Full Network Topology
- Device trace (see *trace guide HFA phone, wiki.unify.com*

https://wiki.unify.com/images/c/c7/Service_Info_How_to_trace_HFA-Update_V3R0.pdf

https://wiki.unify.com/wiki/File:Service_Info_How_to_trace_CP-HFA.pdf

6.2 TDM/Analog/ISDN phone issues

Trace Profiles

- Basic
- Voice_Fax_connection
- For TDM related issues activate: `Calls_with_System_Device_Upn`
- For analog trunk telephony or analog trunk card related issues activate: `Calls_with_Analog_Subscriber_Trunks`
- For ISDN trunk telephony or ISDN trunk card related issues activate: `Calls_with_ISDN_Subscriber_Trunks`

Add-on trace profiles depending on problem scenario

- Display_problems

  issues with phone display notifications
- Device trace (see trace guide TDM phone Wiki.unify.com)

  https://wiki.unify.com/images/0/0f/Service_Info_How_to_trace_OST_TDM_3.pdf

6.3 General telephony issues

Trace Profiles

- Basic

- Voice_Fax_connection

Add-on trace profiles depending on problem scenario

- Feature_Service_activation

  issues with feature activation from phone or application side and issues with call processing in general such as CDL, CFU, Path Replacement, etc.
- Network_Call_Routing_LCR

  issues with call routing
- Actors_Sensors_Door-Opener

  issues with actors/sensors/door opener
- CDR_Charging_data

  issues with CDR

6.4 Poor voice quality/dropped calls

Trace Profiles

- Basic
- Voice_Fax_connection
- Trace Profile Gateway_Stream_detailed
- Resources_MOH_Conferencing

  (only in case of MOH or announcement issues)
- TCP dump/Wireshark

After consultation with support team

- Network plan overview
- List of network components involved
- Firewall configuration

6.5 Device Tones issues, Tones within the call, MoH issues

- Check **Always use DSP** flag: must be deactivated for network trunks, applies only for ITSP with enabled encryption:

  Expert mode > **Trunks/Routing** > **Rout** > **Networking** > **Change routing parameters** > **Always use DSP**
- Check **Tones from CO** flag: generally must be deactivated – it assumes that tones will always be generated within payload from the CO:

  Expert mode > **Basic Settings** > **System Flags**
- **Internal Music On Hold** flag under:

  Expert Mode > **Auxiliary Equipment** > **Music on Hold (MoH)**

6.6 Display Handling issues

The 'Display_problems' trace profile is needed to get meaningful information logged for such use cases.

6.7 CDR issues per individual Output Format

Indicate the CDR system output format under:

Expert Mode > **Telephony Server** > **Basic Settings** > **Call Charges** > **Call Charges - Output Format**

- When the Output Format is set as **HTTPS**, the system acts as a server. (gez.txt also required)
- If option **LAN-TCP-Client** is chosen then the PBX acts as a client .

Per individual setup, troubleshooting requires that the problematic scenario is captured with the following additional components/levels:

- While PBX acts as a server:
  - Default logs plus:
  - CDR_Charging_data Trace Profile in Level 9
  - FP_CHARGE-DATA in Level 9
  - FP_CP-NET in Level 9
  - FP_CP-SUB in Level 9
- While PBX acts as a client:
  - All the above plus:
  - FP_API-IWU in Level 9
  - FP_API-SPU in Level 9

6.8 ITSP (SIP provider) issues

Trace Profiles

- Basic
- Voice_Fax_connection
- SIP_Interconnection_Subscriber_ITSP
- SIP_Registration

In case of poor voice quality/dropped calls please set SPP trace component level to 9 temporarily

Expert Mode > **Maintenance** > **Traces** > **Trace Components** > **SPP** > **9**

After consultation with support team

- TCP dump/Wireshark
- Media Server Trace
- Network plan overview
- List of network components involved
- Firewall configuration

6.9 General payload issues or interworking scenarios

Including SIP/SIPQ connections, scenarios where OpenScape Business interacts with ITSPs, network systems, OSV system, Skype4Business, Unify Phone, Microsoft Teams, and so on.

Trace Profiles

- Basic
- Voice_Fax_connection
- SIP_Interconnection_Subscriber_ITSP
- SIP_Registration
- Feature_Service_activation

Extra info

- TCP dump/Wireshark
- Network plan overview
- List of network components involved
- Firewall configuration

6.10 Encrypted payload and encrypted signaling issues

For encrypted payload and encrypted signaling cases the following traces are required:

Trace Profiles

- Wireshark traces with secure trace certificate are mandatory

Add-on trace profiles depending on the problem:

- When SIP stations are involved
  - Basic traces with SIP interconnection subscriber ITSP profile active.
- When HFA stations are involved
  - Basic traces with Voice Fax connection profile active.
- When TDM stations are involved
  - Basic traces with Gateway Stream detailed profile active.

6.11 FAX issues with analog or ISDN fax devices

Trace Profiles

- Basic
- Voice_Fax_connection
- SIP_Interconnection_Subscriber_ITSP

  (only in case of ITSP trunks)
- TCP dump

  (only in case of ITSP trunks)

Additional Data

- fax file transmitted
- fax file received
- involved components (fax device type/fax server type, ISDN or ITSP trunk)

6.12 FAX issues with UC Suite Fax

Trace Profile(s)

- Basic
- Voice_Fax_connection
- TCP dump/Wireshark
- SIP_Interconnection_Subscriber_ITSP
- CSTA_application

Additional data

- Fax file transmitted
- Fax file received

Please ensure that during trace download the following flags are set

- UC Suite Protocols
- Application Protocols

  (add also CSTA_application traces)

Since OpenScape Business V2 R2, UC Suite Logging is enhanced. With this change most of the errors can be analysed with default traces.

The enhanced UC Traces should be only activated if GVS / development requests it. Please deactivate them directly after finishing the trace scenario.

6.13 CMI Cordless

Trace Profile

- Basic
- Voice_Fax_connection
- CMI (For OSBiz X systems)

Additional data

Expert mode > **Maintenance** > **Cordless** > **BS Diagnostic data**, download file.

Provide:

- Software version and handset id/name from CMI mobile device (Menu *#06#)
- Site plan with overview of the stations
- In case there are trace data needed from the SLCN/SLMUC/SLC16N board as well please follow the the guidelines on the next pages (Checklists for CMI in OSBIZ) and add those to the system trace package

Descriptive data needed

- The history of the problem: in which Software version did the problem appear
- Provide software version and handset id/name from CMI mobile device (Menu *#06#)_

- Are there any HW, SW or configuration changes took place in the meantime?

  E.g. a change in the network of the customer should not be related to DECT, even a SW update if there is no new version of the DECT code. In general this is very critical information as the the CMI team insists to have this as it helps to speed up their investigation.
- Site network plan with overview of the stations.

Hint for GO

Identify with customer similar scenarios with other phone devices: i.e. if a problem is reproducible with a UP0, then it does not look like to be a DECT specific problem so it needs to be escalated in OSBiz GVS instead of CMI GVS.

6.14 Checklists for CMI in OSBIZ

Requests for OSBiz Tracedata *Version: 2.01, Issue Date: the 13th of November 2018, Mircea Mucha*.

NOTICE: “SLC” term implies either SLC16N for X5 or SLCN or SLMUC for X8.

6.14.1 OSBiz-Systems (X8/X5/X1) Cordless Diagnostics requirements

General requirements

In case of Cordless problems please turn on the following tracer settings:

- System: X8/X5/X1: CMI-Trace profile (this enables at least FP_DH-CMI and FP_ILW-DECT with Level 9)
- System: X and BS are connected to SLC line cards (collect SLC-Trace directly after problem occurred; see description below)

Call related problems

The following info is required for call and handset related problems:

- The detailed, actual problem description including the following info:
  - Who has called whom including:
  - Extension numbers
  - Display Names
  - Problem time
  - Terminal-types (phone type S4, SL4 and so on)
  - Software Version of System (e.g.osbizv2 R0.4.0_xxx)
  - If possible software version of the terminals
  - Info if it is an external or internal call (DECT/DECT DECT/internal DECT/external)
  - Description about the call progress (who has initiated the call, a call back, etc.)

- If a call was disconnected unexpected then:
  - Info seen on display of the DECT handset/partner phone
  - tones heard on both sides e. g. "busy tone, ringing tone …"
- If the connection has a bad quality, please describe the malfunction
  - Like clicking noise, voice dropouts, echo, voice delay, low noise [you can hear your partner, but with noise in background] or strong noise [you can hear only a loud noise and not your partner])
  - Noise duration (instant noise e.g. ~1 second or during the whole call). If possible provide a recording of the noise.
- Additional info
- Is the problem reproducible?
- Is possible to take a photo from the display content or a video from the total problem sequence
- Info about the position of the DECT user at the site plan (BS location)
- Info if the DECT user has moved during the call
- For internal users' info about configured call distribution features like Teams, MULAP, Call Pickup, and so on.
- Did problem occur after a new BS was reached?

The statistical distribution of the problem:

- How often does the problem occur on a day?
- What is the relationship between good and bad DECT calls?
- Is there a relationship between DECT problems and a dedicated location, e.g. a staircase?
- Is there a relationship between DECT problems and a determinate base station?

The current site plan (position plan) of the base stations including information about special environment conditions, e.g. reinforced concrete ceiling, wire-reinforced glass wall, closeness of strong electric consumers, closeness of other radio technology like WLAN, other DECT systems or medical equipment like X-Ray, CT, etc. Please check the radio coverage at the location where the problem occurs (FRAQ and RSSI values concerningOSBizV2 service documentation).

Minimum needed data from system:

- Trace from problem time (see min. Tracer settings)
  - System trace
  - SLC-trace in case of BS connected to SLC-card
- BS-Statistic data (please specify time; like last data collection at 2015-11-10 15:20)
- Answered questionnaire (see above)
- KDS of actual system at problem time (collected when the problem occurred)
- Remote connection details e.g. RSP should they exist
- Network plan (location of BSS) mandatory in case of voice quality problems, call disconnections, coverage issues.

6.14.2 Example of call related problems

This is a sample of call related problems. It is given only as an example.

- the DECT user “Meyer with the internal phone number 123 with an SL4 with SW Version V1 R2.1.0 has called the external partner “Lehmann” with the number 00987654321
- user 123 calls 00987654321
- user 123 got a ringing tone
- user 00987654321 accepts the call and is successfully connected with 123
- the user talks five minutes without problems
- after five minutes hears the user 123 a strong noise and user 00987654321 was disconnected
- the problem occurs at 2015-11-19 at 17:50
- the problem is not reproducible
- the user with the handset 123 sits during telephone call in the room number 9
- the user 123 is in a MULAP with the OpenStage Phone 100
- the problem occurs two times per day.
- there is an average of 500Dectcalls per day.
- the problem occurs mostly at the seventh floor.
- the problem occurs mostly at the proximity of base station two.

Floor plan: /Network plan:

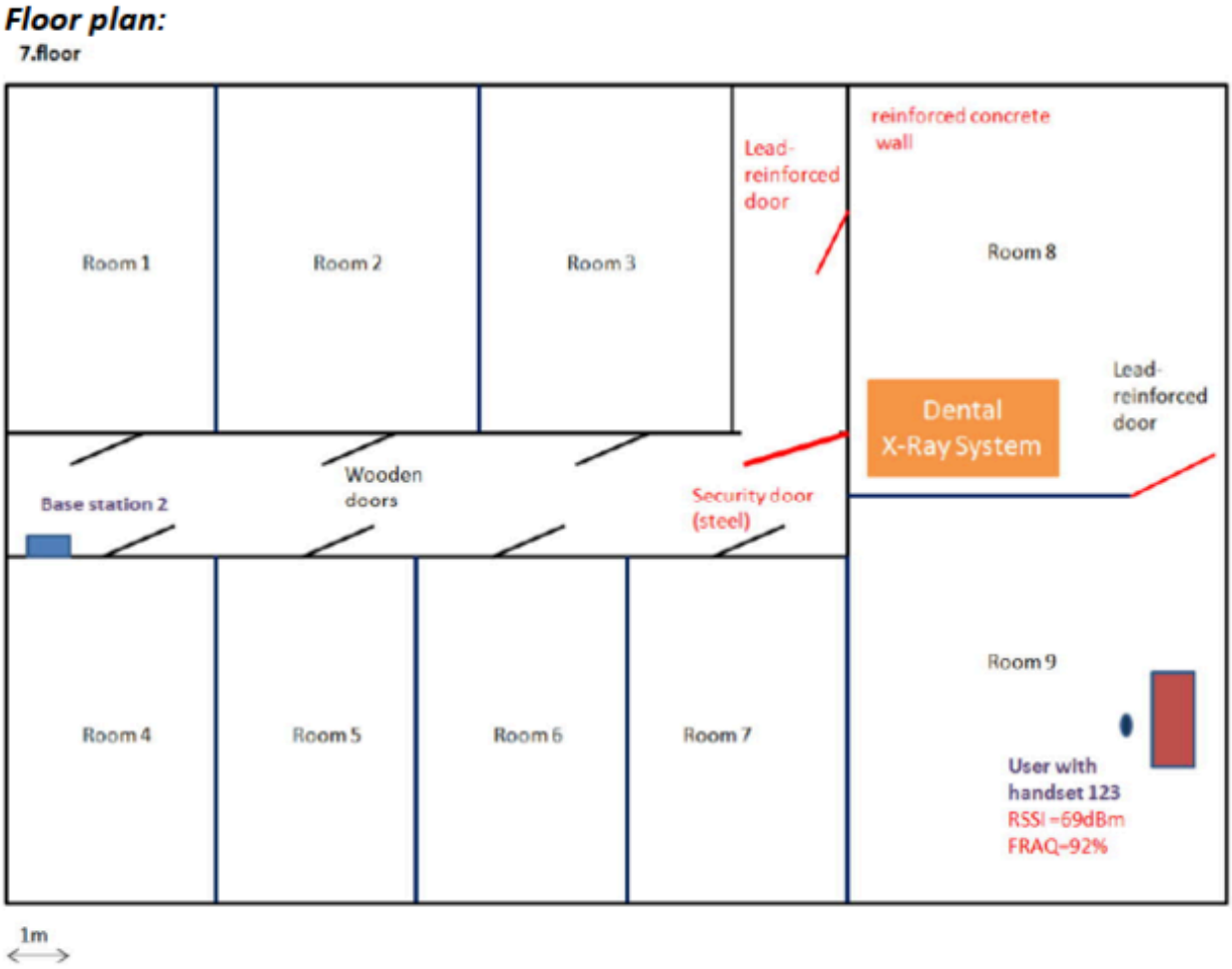
Attachments: trace.20151119-174500.log.gz

Or complete data set: 172.30.242.200-gw-2015-11-19-diagfiles.tgz

photo_location_bs2.jpg

BS-Static data: bssdata.zip

KDS of customer



6.14.3 Collecting the SLC-Trace

Please note the following important information:

1) The SLC trace transfer is needed when we have SLC16N (X5) or SLCN (X8) or SLMUC (X8). When we have integrated DECT, e.g. SLU8, SLU8N or SLUC8, the traces are written directly to system log, there is no need for trace transfer, so no need for SLC16N component activation.

2) Remember that FP_LW-SLC16N trace component is different from other components: the SLC traces are recorded in the card always and they stop recording when the FP_LW-SLC16N component is enabled (this prevents the existing trace information to be overwritten) and transfer from the card to the system takes place. In other words, when you check the below parameter you stop the traces on the cards and start the transfer from the cards to the central system log. When this transfer is finished, the FP_LW-SLC16N trace component must be disabled (uncheck). This action stops the transfer from the SLC cards to the central system and starts the tracing on the SLC cards for future usage.

3) Please note that the memory on the SLC cards is limited to 4MB. For this reason, please enable theFP_LW-SLC16N component as soon as possible after the problem occurred. Depending on the traffic(the load) which is on the switch, the transfer must be started from a few minutes to a few hours,otherwise the traces are overwritten.

It is imperative to download the SLCN traces immediately after error occurrence. The reason is the SLCN trace buffer is very small and on systems with substantial traffic only about 15 minutes of history can be captured.

If you want to make several scenarios, it is preferable to collect the SLCN traces after each, to avoid traces to be overwritten.

6.14.3.1 Collecting traces from the SLC boards in OSBiz Systems

Prerequisites

Login: Expert Mode

Trace in SLC is always running in SLC, but to get the trace information (which is in the boards) into system trace (central system) the trace must be uploaded from SLC to system trace. This will be done in the following way

Step by Step

1) Start upload from SLC to System trace buffer

a) Under **Expert Mode** > **Maintenance** > **Traces** > **Trace Components** > **FP_LW_SLC16N** enter the following:

Trace level: 1

Trace on: Check mark

b) Press the **Apply** button.
After this, a small window might appear, depending on the browser. Now the trace is being uploaded from SLC to system trace buffer. This might take some time (approx. 20 min or more, depending on the amount of SLC-boards in the system).

When all data has been uploaded then an entry in the “Eventlog” under “messages” file will be made.

c) Go to **Expert Mode** > **Maintenance** > **Events** > **Event Log** and click on **Load**.
With this action, the event log file will be downloaded.

d) Go inside the archive and look on the file `messages` located under the folder `log`.

e) In this file, search for the text `finished`.

You should see a text like `SLC trace transfer finished`. This means that the SLC transfer was successful.

2) To start again the SLC traces, for future usage, go back to **Expert Mode** > **Maintenance** > **Traces** > **Trace Components** > **FP_LW_SLC16N** and enter the following:

Option	Description
Trace Level	0
Trace on	Uncheck mark

Press the **Apply** button.

3) Get the Diagnosis-Files.

   Specify a given time interval or get all data to cover the period since the problem occurred until the time when the SLC trace transfer finished.

   a) To get the Diagnosis file, go to **Service Center** > **Diagnostics** > **Trace** and click on **Diagnostics Logs**.
   b) Choose a period which will include the time when the problem occurred and the time when the SLC transfer finished.

   Be careful of the next possible mistake. Let's suppose that the error occurred at 10:02. The SLC transfer started at 10:57, the transfer finished at 11:16. We must collect at least the period from 10:00 till 11:15. Please note that the interval is from 15 to 15 minutes. 11:15 means that the interval beginning with 11:15 (till 11:29:59) is included. Mistake: if it is collected only the interval from 10:00 till 10:15 (which indeed includes the time when the problem occurred) is not enough because the events from the SLC boards from 10:00 till 10:15 have been transferred to the central syslog after the transfer started (at: 10:57) and finished (at 11:16). Even so, it is not sure that the SLC traces are OK, are not overwritten. The collection of these traces was stopped at 10:57.

6.14.3.2 Collecting SLC traces in a nutshell

Step by Step

1) Disable FP_LW-SLC16N trace component to allow tracing in the SLC cards.
2) Enable CMI trace profile.
3) Do the tests and finish them (in case of a sporadic problem, wait until the problem occurs).
4) Enable FP_LW-SLC16N trace component that starts trace transfer (and stops SLC tracing).
5) Wait until the message **SLC trace transfer finished** appears
   That means that going in **Expert Mode** > **Maintenance** > **Events** > **Event Log** > **Load** a file like: `<ip-address>-gw-year-month-dayevent.tgz` will be downloaded. Inside there are 2 folders: `evtlog` and `log`. Open the file `messages` from the folder `log` and check if the text `SLC trace transfer finished` exists. If it is found it means that the SLC traces from the boards have been transferred. If this message is not found or it is an old message like this, then wait and check again after 5 minutes.
6) Deliver the traces

   a) Go to **Service Center** > **Diagnostics** > **Trace** and click on **Diagnostics Logs**.

      The downloaded file `oso_diagnostic.tgz` contains traces and events.
   b) Another possibility is to go to **Expert Mode** > **Maintenance** > **Traces** > **Trace Log** and select a period to include the time when the problem occurred and time when the transfer finished and then click on **Load**.

   The downloaded file is a file with the name: `oso_diagnostic.tgz`. Deliver also the last events log file you downloaded. (a file like `<ip-address>-gw-2017-month-day-event.tgz`). The first method (using **Service Center**) collects more data than the second and is preferable.

7) Disable FP_LW-SLC16N trace component to allow tracing in the cards for future use.

When the problem is 100% reproducible under certain conditions, ideally, to have only the traces from the desired scenarios and not unnecessary data from the past, if it is possible, do the following:

a) Disable FP_LW-SLC16N trace component to allow tracing in the SLC cards
b) Enable CMI trace profile
c) Enable FP_LW-SLC16N trace component that starts trace transfer and get previous unnecessary data.
d) Wait for “SLC trace transfer finished” message and clear all the data captured (trace-logs and events).
e) Disable FP_LW-SLC16N trace component.
f) Do the tests and finish them (or wait until the problem occurred)
g) Enable FP_LW-SLC16N trace component that starts trace transfer.
h) Wait for “SLC trace transfer finished” message
i) Collect and deliver the traces.
j) Disable FP_LW-SLC16N trace component to allow tracing in the cards for future use.

Traces following at least the 1st method are necessary; the 2nd method would be perfect.

6.14.3.3 Collecting traces from the SLMUC boards in OSBiz Systems

The trace mechanism for CMI is described below.

A new trace mechanism and a new trace component has been implemented: **FP_LW-SLMUC** for receiving traces from SLMUC cards.

Until now the trace data were stored in a cyclic 4MB buffer on the card and when it was necessary the trace buffer was transferred to the system. This often meant the trace data did not contain a reported call scenario due to the time frame being overwritten. With the new trace mechanism, the data are written in the system trace real time so long as the system trace is available.

To configure the new mechanism, the user can set the level of trace details (1, 3, 6 or 9):

- Level 1: captures only errors reported by the card
- Level 3: captures basic messages from Layer 2 and the OSBiz side in addition to Level 1
- Level 6: captures more detailed messages regarding Base Stations, Portable parts and cards
- Level 9: captures all messages

Activation: FP_LW-SLMUC set to 1, 3, 6 or 9, check the Trace ON Box and click **Send**.

Deactivation: FP_LW-SLMUC set to 0, uncheck the Trace ON Box and click **Send**.

NOTICE: Since the new mechanism increases the HDLC traffic of the system, the user should use the advanced level details with caution and only for the time that it is necessary. The big HDLC traffic by the traces causes delays to the calls and to the Dect menu. This is an indication to reduce the trace level detail. The new trace mechanism is currently available only for SLMUC cards.

SLCN and SLMUC Old Trace Mechanism - FP_LW-SLC16N component

The old trace mechanism is still available for SLMUC cards and is the only trace mechanism available for SLCN cards. With this mechanism, the latest 4MB of trace data stored in the cyclic buffer are transferred from the cards to the system after activating the transfer. The advantage of this mechanism is that the traces are always written into the trace buffer of the card without causing traffic to the system but only the last 4MB of trace are available.

Transfer Activation: FP_LW-SLC16N set to 1, check the Trace ON Box and click Send.

NOTICE: The traces are always written to the trace buffer except from the time that the transfer is ongoing. As soon as the transfer finishes, trace is stored in the buffer again.

To capture traces from X8 with SLMUC and SLCN cards proceed as follows:

Step by Step

1) Old trace mechanism - **FP_LW-SLC16N** component:

a) Activate CMI Profile.

This option must be always activated.

b) Continue by executing the scenario.

c) Transfer Activation: Trigger the transfer of the traces from the cards to the system

If the Trace ON box is checked, uncheck the box, click Send and then check the box and click Send in order to start the transfer.

d) Wait until the data from all cards are transferred to the system: check messages for “SLC Trace Transfer” message

e) Get the trace log.

2) New trace mechanism - **FP_LW-SLMUC** component:

a) Activate CMI Profile.

This option must be always activated.

b) Activation: Activate the trace mechanism

c) Continue by executing the scenario.

d) Deactivation: Deactivate the trace mechanism.

This is recommended in order to avoid unnecessary HDLC traffic.

e) Get the trace log.

NOTICE: If the system has a combination of SLCN and SLMUC, then the new trace mechanism will be activated only

at SLMUC. The SLCN cards will continue storing the trace in the local buffer.

6.15 License issues

Trace Profile

- Basic
- Voice_Fax_connection
- License_problem
- Validate that under WBM:

  Expert Mode > **Maintenance** > **Traces** > **License Component** > **CLA**, the Trace Level is set to **ALL**.

INFO: Licensing logs have a relatively brief history and information could be rotated when tracing intensively. It is advised to collect logs as close as possible to the time stamp of a reported issue so as not to loose vital license diagnostics.

Additional data

- original .lic file
- Screen shots of License Manager and Home screen where applicable.

6.16 System startup issues after software activation / software update

Trace Profile

- Basic
- Voice_Fax_connection
- Core Logs (if generated)

NOTICE: Please contact your support team

6.17 UC Smart issues

Trace Profile

- Basic
- Voice_Fax_connection
- UC_Smart
- Smart_VM
- CSTA_application

Additional data

- List of all involved components with software versions including client PC details for OS 32/64bit and MS Office versions/service packs
- Get client PC and OS details from local PC: **Start** > **execute** > **dxdiag**

- UC Smart Client Logs from local PC
- Screen shot from UC Smart application including date and time

Please ensure that during trace download the following flag is set, **Application Protocols** (add also **CSTA_application** traces).

6.18 MyPortal / MyPortal for Outlook / MyAgent / MyAttendant / MyReports

Trace Profile

- Basic
- Voice_Fax_connection
- CSTA_application (only for CC and myAgent scenarios)

Additional data

List of all involved components with software versions including client PC details for OS 32/64bit and MS Office versions/service packs.

UC Suite Client Logs from local PC.

Screen shot from UC Suite application including date and time. The time of occurrence is vital.

UC Suite diagnostics (that include UC Suite Diagnosis Only Backupset) are required for resolving myReports issues. If a problem is related to the reports content (data shown in the report files), please include screenshots or video captures of the reports in question (entire screen always preferred), or entire report files.

NOTICE: When capturing a client's screenshot e.g. from myAgent, please provide the whole screen. The time at the bottom right of the screenshot is important for the incident analysis.

Windows Eventlog complete saved as (*.evtx)

Please ensure that during trace download the following flags are set: **UC Suite-Protocols**, **Application Protocols**.

Reference also sections on Process Dump and UC Suite troubleshooting

Since OpenScape Business V2 R2 UC Suite Logging is enhanced. With this change most of the errors can be analysed with default traces.

The enhanced UC Traces should be only activated if GVS / development requests it. Please deactivate them directly after finishing the trace scenario.

6.19 UC Suite Clients Crash or Freeze – Process Dump

Procdump (https://docs.microsoft.com/en-us/sysinternals/downloads/procdump) gives us a snapshot of what an application is doing at any time. Procdump should be used for OLI/myAgent/FaxPrinterDriver when the application either crashes or freezes/becomes unresponsive.

Step by Step

1) Extract the contents of `procdump.rar` to any folder on your PC.
2) Using CMD, navigate to that folder.
3) Depending on the type of error being investigated, type one of the following commands:
   a) When the application is frozen:
      - For Outlook: `procdump.exe -ma outlook.exe`
      - For myAgent: `procdump.exe -ma myagent.exe`
   b) When the application crashes:

      Type the following before the application crashes (or before you start the application)
      - For Outlook: `procdump.exe -ma -w -e outlook.exe`
      - For myAgent: `procdump.exe -ma -w -e myagent.exe`
4) Provide the `DMP` file in the folder where you extracted it, along with the client log files and Windows machine's `EventLogs`
5) Install DebugDiag from the following link: https://www.microsoft.com/en-us/download/details.aspx?id=103453
6) Once installed, right click on the `DMP` file and select **DebugDiag Analysis**.

   After the analysis is completed, save the generated data and attach it to the ticket.

6.20 Troubleshooting UC Suite issues

- When UC Suite crashes are experienced (system, CSP, etc.):

  Set the flag **Core Logs** prior to collecting/downloading system traces.
- For problems with UC Suite **Fax printer Driver**:

  Collect and provide Fax Printer Driver logs over client machine's path: `C:\ProgramData/CommunicationsClients/CC-Logs/OSBizUser[e.g.406]\FaxPrinterDriver`
- For UC Clients **Auto Update** issues:

  Collect contents of the following paths from the client machine:
  - `C:\ProgramData/CommunicationsClients/AutoUpdate` - Contains traces for the migration process from V2R6 to V2R7 clients
  - `C:\ProgramData/CommunicationsClients/CC-Logs/AutoUpdate` - Contains traces from auto update background service

In case of AutoUpdate related issues, please include the above paths contents.

Auto attendant / Schedules

For issues related to auto attendant / schedules no system-specific traces are needed. From UC Suite, "oso_diagnostic" is required including UC Suite traces.

6.20.1 myPortal@Work (UC Smart, UC Suite) client issues

You need to provide the following traces

Step by Step

1) System traces with Trace Profiles:

- Basic
- VoiceFaxConnection
- SIP-Interconnection-Subscriber-ITSP

and additionally enable the following Trace Components:

- ERH_H323_REG level 3
- HFAM level 6
- MSTU level 9
- MSTU_RTPPROXY level 9
- NSA level 6
- TC level 3
- SPP level 6
- MSH level 6
- LLC_CALL level 3
- IPNC level 6
- MPH level 6

2) RTPProxy Trace or Media Server Trace.

NOTICE:

The RTPProxy Trace service is only available on OSBiz X systems with:

- V2 mainboards
- V3 mainboards up to OpenScape Business V3R2 FR1

Upon Start RtpProxy Trace payload for all active myportal@work VoiP calls will be dropped.

The Media Server Trace service is only available on:

- OSBiz S systems
- OSBiz X systems with V3 mainboards.

---

3) TCPDump (system side), depending on the nature of the issue, also wireshark from client side.

4) From the client machine where myPortal@work is installed and under **Settings** > **Debug settings**, collect the client's logs after problematic scenario has been reproduced.

5) Where applicable and necessary to demonstrate a defect, capture screen shots of the UI or a video.

6) From the System side, make sure that **Application Protocols** and **UC Suite Protocols** are selected when system diagnostics are collected since LAS logs are vital for investigation.

7) State Timestamps of the actions/scenario and users' parameters involved to identify inside logs.

6.21 Application Launcher issues

- Traces for Client App. Launcher:

  Local Disk > **Users** > **<User>** > **AppData** > **Roaming** > **Tray_Tool** > **trace.atr**
- Traces for Server App. Launcher:

  From the System side, make sure that **Application Protocols** is selected when system diagnostics are collected.

Remarks

App Launcher trace file can get easily corrupted as it is "dynamically" copied. The result will be to get empty decoded view of the trace by using the special Development tool for examining App Launcher logs.

Corruptions can happen usually when an engineer copies the traces but the Application Launcher application is still running in the background or if it is terminated not gracefully e.g. via Windows Task Manager.

After a critical error or after a specific time period, Application Launcher updates the trace file, but if during the update it is terminated or someone copies this file then the trace file could get corrupted or the copied file might be incomplete.

In order to avoid this, which makes the investigation harder and lengthens processing time, you are advised trying to gracefully terminate the app by right-clicking its icon at the task bar to allow for proper update of its contents.

If corruption has already taken place and in order to avoid maintaining it, please completely delete the log file while the app is not running and then start up App Launcher to have it properly regenerated.

6.22 Skype for Business

Trace Profile

- Basic
- Voice_Fax_connection
- SIP_Interconnection_Subscriber_ITSP
- TCP dump/Wireshark

Trace components

FP_CP-Port-User: level 9

FP_DH-SIP: level 9 (only for OpenScape Business X variant)

In case of registration issue with ITSP/lines please activate following profile in addition:

- SIP_Registration

6.23 Connected CSTA Applications

Trace Profile

- Basic

- CSTA_application

Please ensure that during trace download the following flag is set: **Application Protocols**.

6.24 TAPI Service Provider

- Please activate the following flags first on the TAPI PC and restart the Telephony-Service before reproducing the issue

  Control Panel > **Phone and Modem** > **Advanced** > **OpenScape Business TAPI** > **Configure** > **Advanced**

  Debug-trace options: on with verbose level

  Write trace to file when Debug-trace is turned on
- Depending on the TAPI operation mode choose the following traces on the OSBiz system
  - **OSBiz TAPI CSTA**

    UC Suite-Protocols

    Application Protocols (add also **CSTA_application** traces)
  - **OSBiz TAPI UC Smart**

    Application Protocols (add also **CSTA_application** traces)
- Over the client machine end, please include Windows Event Viewer Logs.

6.25 Accounting Manager issues

To activate, set Registry key:

```
HKEY_CURRENT_USER\Software\Siemens\Accounting Tool
\Accounting Tool TraceToFile, REG_DWORD, value 1
```

The generated trace file can be found under:

```
%LOCALAPPDATA%\VirtualStore\Program Files (x86)\Accounting
Manager\Trace.log
```

- Depending on the CDR output format, consult also the relevant CDR troubleshooting section for the respective CDR diagnosis data over system side.
- Include screen shots of the Accounting Manager configuration and particularly any active Filters.
- Indicate that OSBiz Central Call Charge Recording flag **Activate Call Charge Recording** is set and also indicate the configuration under **Expert Mode** > **Telephony Server** > **Basic Settings** > **Call Charges**

NOTICE: In particular situations it could be required that prior to fetching CDRs from within Accounting Manager, GVS will have to first remotely connect and collect from the PBX via ssh the generated `gez.txt` file to analyze CDR record formation. This file gets deleted when Accounting Manager retrieves the CDRs.

6.26 Issue involving OpenScape Contact Center

For OSBiz scenarios where OSCC is involved and in order to avoid multiple requests, along with OSBiz Diagnostics with "Application Protocols"[1] set, please collect the following OSCC diagnostics:

- OSCC design db
- OSCC telephony server trace (full level)
- OSCC call director server trace (full level)
- OSCC routing server trace (INFO level)
- CMS trace (full level)
- OSCC error log
- Windows Event Logs (OSCC)
- `/var/log/messages+warn` (CMS)

6.27 ODS/ODBC issues

- Name, exact version, 32bit/64bit variant of the 3rd Party Datasource used by a customer.
- An indication from within the 3rd Party datasource, of the column **Data Types** used.
- Size/records of the datasource and its location (i.e. integrated to the ODBC Bridge server or remotely located on a separate server).
- Firewall/ports allowed over ODBC Bridge and Datasource servers.
- A validation of UniqueIDs not containing null or duplicate values.
- A rough estimate of end user size pulling LDAP searches.
- An indication of any special characters used in both column headers and data contents. This should consider also “regular” characters but on data deviating typical syntax, e.g. tel.# `+30{210}xxxxxx` instead of `+30(210)xxxxxx`
- If ODBC Bridge remote access is not possible, along with ODBC Bridge configuration and logs, please provide also System DSN configuration of the associated ODBC driver configuration.
- Where found valuable, a wireshark of the communication in between ODS and ODBC Bridge Server and ODBC to Datasource Server.
- Validate if the following ODBC functions are indeed supported by the Database Management System (DBMS) and the corresponding ODBC driver used: `SQLAllocHandle`, `SQLBindCol`, `SQLConnect`, `SQLDisconnect`, `SQLDriverConnect`, `SQLExecDirect`, `SQLFetch`, `SQLFreeHandle`, `SQLFreeStmt`, `SQLGetDiagRec`, `SQLGetInfo`, `SQLSetConnectAttr`, `SQLSetEnvAttr`, `SQLGetEnvAttr`, `SQLGetFunctions`, `SQLGetStmtAttr`, `SQLNumResultCols`, `SQLGetTypeInfo`, `SQLColAttribute`, `SQLGetData`, `SQLTables`.

6.28 DLI issues

- If a DLI issue is reproducible, please set the trace component **DLI_WORKPOINT** to level 3 and perform the use case anew. Once the

[1] Enable **CSTA_application** prior to executing the scenario.

scenario completes, collect the logs and reduce trace component back to default level.

- For the matching timestamps, Phone diagnostics of a sample failing device is also required for the investigation of DLI issues.

6.29 OpenScape Business and Unify Phone interconnection issues

In case of OpenScape Business and Unify Phone interconnection issues enable and provide the following trace components:

- PCC level 9
- API_CTI level 9
- SIP_SA level 9

NOTICE: For issues regarding payload problems follow the relevant directions as already mentioned in chapter General payload issues or interworking scenarios on page 12.

---

7 Diagnosis on VoiceMail issues

Identify initially what type of VM is used (SmartVM, UC Suite VM)

1) OSBiz X

- **a)** Application mode is UC Smart > Voicemail capabilities are provided by SmartVM feature (ISDN ports).
- **b)** Application mode is UC Suite > Voicemail capabilities are provided by UC Suite.

2) OSBiz S

- **a)** Application mode is UC Smart > Voicemail capabilities are provided by SmartVM feature (MEB trunks).
- **b)** Application mode is UC Suite > Voicemail capabilities are provided by UC Suite.

If problems appear during recording a message in the VM, ensure that the recording scenario is included in traces and also activate a TCP dump.

If problems appear during playback of a message from the VM, ensure that both recording and playback scenarios are included in traces, and also activate a TCP dump.

When ITSP and/or HFA subscribers are involved, Wireshark traces are also required.

When UC Suite VM is used, please ensure that during trace download the **UC Suite Protocols** flag is set.

8 Kernel Crash Data service

Kernel Crash Remote Data Collection

System restart because of POWER DOWN or WATCH DOG or KERNEL OOPS.

NOTICE: Most cases are related with Linux OS kernel crash. Most cases also require extra trace logs (USB serial console log).

The system is now able to collect remotely kernel crash data in a diagnostics data file, by activating this service via the **Admin Portal**.

The process includes the following steps:

- Activate **Kernel crash data** service via the Admin Portal.
- Wait for the next system kernel crash.
- Download **Diagnosis Logs** via the Admin Portal.
- Deactivate the service.

NOTICE: The Kernel crash data service is only available on OSBiz X systems with V3 mainboards: OCCLA, OCCMA(R), OCCB(R).

NOTICE: The Kernel crash data service requires a system restart for activation and deactivation. The system retains the status after a system restart.

NOTICE: The Kernel crash data service requires a free space of 200MB on storage disk. Only SATA SSD disks are supported (NVMe SSD when available). It is recommended to delete traces before service activation in case that extra free space is needed.

9 Media Server Diagnosis

Media Server Remote Data Collection

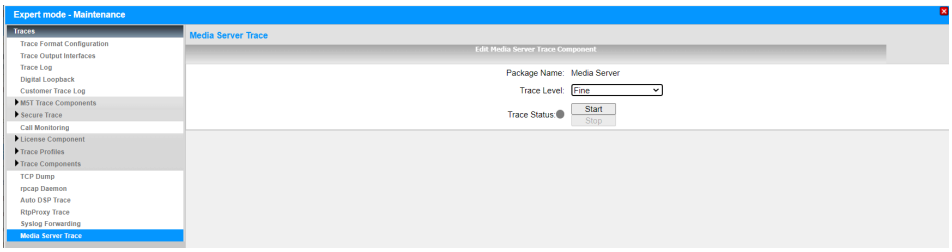
The system is able to collect remotely media server data in a diagnostics data file, by activating this service via the **Admin Portal**.

The process includes the following steps:

- Select the **Trace Level** via the Admin Portal.

  NOTICE: The most frequently used trace level is **Fine**.

- Activate **Media Server Trace** service via the Admin Portal.
- Reproduce the problematic scenario.
- Download **Diagnosis Logs** via the Admin Portal.
- Deactivate the service.



NOTICE: The Media Server Trace service is only available on:

- OSBiz S systems
- OSBiz X systems with V3 mainboards: OCCLA, OCCMA/B(R), OCCSB

10 Remote Access RSP.servicelink

Why RSP.servicelink

RSP.servicelink is the preferred connectivity method for all products of the actual Unify portfolio offering easy to install, easy to use secure broadband remote access.

Customers benefits with RSP.servicelink

- Highest security
- Secure outgoing connection set up
- Broadband connection
- One connectivity for all actual products
- SSL-VPN
- Easy setup
- Cost efficiency
- Suited for monitoring
- Future proof platform