Partner Guidelines

<for opening tickets with Unify >

Version: <3>

Date: <5 July, 2018>

Table of Contents

List of Changes

Version	Date	Changes	Author
2.1	6.04.2017		
3	5.07.2018	OSB chapter updated SBC chapter updated CMI chapter added AC WIN, DS Win BLF Win Chapter updated	Paul Brinzei, Andreea Arteni

1. REQUIRED INFORMATION

1.1. Problem Description

Please ensure you provide a complete description of the technical problem including:

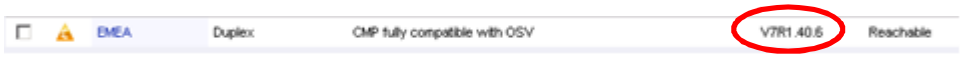
- Detailed description of the error scenario: (call handling details, steps, errors, any other relevant information)
- Involved parties with corresponding E.164 numbers or user ID's
- Exact timestamp of the described error scenario/reproduced scenario (to be in line with trace data set that needs to be provided)
- Is the error always reproducible at the customer site?
- Is the error in combination with application use? (Which one?)
- Is this a new installation site?
- Does this error also occur at any of your other customers?
- Has a hardware-defect been eliminated as the issue?
- Was IP-infrastructure (e.g. performance, IP address block) eliminated as the cause?
- Was misuse and misconfiguration eliminated as cause?
- Error frequency and known trigger (e.g. how often, when)
- Are there abnormal hints (e.g. high load, time stamps)?
- Can the error be solved temporarily (e.g. restart, workaround)?
- Are all deployment requirements fulfilled and environmental conditions sufficient (temperature, humidity, grounding, EMC protection)?
- If applicable:
    - Virtualization settings have been double checked with OpenScape Virtualization Guide?
    - Problem reproducible with default CDB?
    - Has there been communication with a Unify specialist from Level 2/3 already?
        - Add contact details if so
    - Did the error appear after a migration (i.e. H3k->OSBiz migration scenario) or software update?

1.2. Architecture Involved: details according to product family: SMB, OS4000, OSV

Please provide details of:

- Product, software version details, which kind of UC solution in use
- Hardware-Architecture (e.g. system type, virtualization, networking)
- Client-Server architecture (WIN / MAC / Linux) version numbers
- Licensing (local, networking, virtual, ALI)
- Connected endpoints (SIP / HFA / TDM / Mobile)
- Connected plus products / other non Unify endpoints / solutions
- Connected trunks (ITSP / ISDN / SIP) / system networked
- Hardware-revisions (e.g. firmware, board revisions, endpoint revisions)
- The software versions of the involved devices

Here is an example of the software version details from the OSV and UC platforms:



or

1.3. Actions Taken by the Partner

Please ensure you provide a complete description of the troubleshooting actions you have already performed and the results of your initial analysis.

NOTE: This is very important to bring efficiency to the incident process. When you provide a complete troubleshooting history Unify can continue where you left off and avoid duplicating work already completed.

2. Basic Traces

Please note: For scenarios involving multiple systems or components of a system (i.e. client or endpoints connected to a PBX) traces are required from the each system component involved in the scenario.

2.1. OpenScape Business

Trace profiles in OpenScape Business are available in WBM section Service Center Diagnostics – Trace. All OpenScape Business systems have the Basic Trace Profile activated by default.

Additional (optional) trace profiles have an online description to help identify and activate the proper trace profiles for special areas affected. In most of cases, activating the corresponding trace profiles is already sufficient for further investigation by Unify development.

Expert Hint: As t**race files** can grow to a significant amount depending on selected profiles and system traffic it is recommended to select trace download **for corresponding time slot** when the reported error has previously occurred. Please mind that those timeslots can be chosen for **Trace Log** and **UC Suite Protocols** independently.

Overview and usage hints of available Trace Profiles:

- **Basic** – Simple trace profile that allows a basic analysis of system activities; **enabled per default (factory setting)**.

Optional Trace Profiles (**to be activated during corresponding trace session only!**)

- **Actors_Sensors_Door-Opener – I**ssues with the STRB peripheral card, e.g. actors, sensors or a door opener which is connected to an analog port.
- **Calls_with_Analog_Subscriber_Trunks** – Shall be combined with the voice_fax_connection profile for detailed analysis of issues with analog phones or analog trunks.
- **Calls_with_ISDN_Subscriber_Trunks –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with ISDN (S0) phones or ISDN (PRI/T1) trunks.
- **Calls_with_System_Device_HFA –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with HFA IP devices, e.g. registration, wrong display messages, wrong LED signals, user cannot take or answer call, call not ringing, no ringback tone.
- **Calls_with_System_Device_Upn –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with UP0E devices, e.g. wrong display messages, wrong LED signals, user cannot take or answer call, call not ringing, no ringback tone.
- **CDR_Charging_data –** Incorrect or missing charge data.
- **CMI –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with integrated CMI, e.g. handover, registration, lost connections.
- **CSTA_application –** Malfunctions of CSTA controlled features in the system, e.g. lost connections to external applications or wrong functionality. Application traces have to be collected additionally.
- **Display_problems –** The displayed texts are incorrect, missing or appear after a delay.

This applies to all device types with a display.

- **Feature_Service_activation –** Issues with feature/service (de-)activation via service code or menu option.
- **Gateway_Stream_detailed –** Detailed analysis of issues with missing payload in calls between IP and TDM, e.g. SIP trunk to UP0E phone or TDM trunk to IP phone. High influence on the system performance.
- **Gateway_Stream_overview –** Issues with missing payload in calls between IP and TDM, e.g. SIP trunk to UP0E phone or TDM trunk to IP phone. Overview only, but low influence on the system performance.
- **IP_Interfaces –** Issues with system IP interfaces:, i.e. WAN, LAN or Admin.
- **License_problem –** Issues with licensing, e.g. with license configuration or evaluation.
- **Network_Call_Routing_LCR –** Issues with live monitoring between nodes, LCR dial rules or unreachable destinations.
- **Peripheral_cards –** Issues with the initialization or start-up of peripheral cards.
- **RAS_or_Internal_access –** Shall be combined with the IP_Interfaces profile for detailed analysis of issues with remote administration (RAS) or internet access.
- **Resources_MOH_Conferencing –** Issues with music on hold or conferencing.
- **SIP_Interconnection_Subscriber_ITSP –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with SIP phones, access points, ITSP interfaces or SIP interconnections, e.g. calls to or from ITSP/SIP are not signalled at phones, DTMF or fax cannot be sent or received via ITSP/SIP interconnections.
- **SIP_Registration** – ITSP / SIP-nodes / SIP-phones / SIP-access points cannot register or lose registration.
- **Smart_VM –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with Smart Voicemail.
- **UC_Smart –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with UC Smart.
- **Voice_Fax_connection –** Issues with voice or fax connections, e.g. missing or distorted connections, wrong LED signals, interrupted calls or faxes, user cannot take or answer call, call not ringing at phone, no ringback tone. This trace profile is enabled by default (factory settings). It may be combined with interface specific profiles depending on the involved device types.
- **VPN –** Issues with VPN connections, e.g. connection disrupted, unable to import or generate SSL certificate (.crt), certificate revocation list (.crl), peer certificate (.pkcs12) for VPN, unable to import or generate SPE certificate.
- **Web_based_Assistant_Expert_Mode –** Issues with the expert mode of Web based Assistant, e.g. data not stored after input or data lost. High influence on system performance.
- **Xpression_Compact –** Shall be combined with the voice_fax_connection profile for detailed analysis of issues with Xpressions Compact.

The Button **Diagnosis Logs** on Service Center – Diagnostics – Trace WBM page leads to Trace-logs download options. Most common Logfiles and Protocols for trace download are already pre-selected here by default:

Trace Log, Event Log, Admin log, Licence Protocols, Customer Trace, Framework Protocol, Diagnosis Log, System Diagnosis Protocols and PPP Log.

The 3 protocols listed below are optional (typically they are large in size), and therefore **need to be selected manually** in cases where the corresponding areas are affected:

- **UC Suite Protocols** (necessary for all UC Suite Problems; Hint: Booster Server needs separate download)
- **Application Protocols** (necessary for Middleware Problems)
- **CoreLog Protocol** (necessary e.g. for unexpected System-Restarts)

Please also keep in mind: For all issues regarding Client-Applications (myPortal etc.) the Client-logs (CC logs which have to be activated in advance) from affected user (PC's) will also need to be provided.

Please make sure the CC logs are active by following these steps Expert Mode - Applications – UC Suite – Server – Logging, make sure that options are set (Enable log upload for uploading logs in system traces, Enable client logging to generate logs)

For OpenScape Business X variants (embedded platforms): Please provide a KDS (incl. login credentials) taken by Manager E to give a brief overview about customer's general scenario and configuration.

For OpenScape Business server variants: Please provide a **Diagnosis** Data Backup (incl. login credentials) to give a brief overview about customer's general scenario and configuration.

2.1.1. HiPath 3000

As this product is no longer supported please follow the guideline on how to migrate from HiPath 3000 to OpenScape Business V2:

HiPath 3000 V7, V8 and V9 System can be migrated directly to OpenScape Business V2. A direct migration requires:

- An active HiPath 3000 CDB.
- Manager E V10 R2.12.0 or higher
- Upgrade license V9 (L30250-U622-B684. This is independent from the HiPath 3000 version!)
- Connection from administration PC to Central License Server (CLS)

After the successful technical migration the central license server provides for HiPath 3000 V7 systems 70% for HiPath 3000 V8 systems 80% of active TDM subscribers as OpenScape Business TDM user licenses. If

HiPath 3000 V9 systems are migrated, 100% of the active TDM subscribers are provided as OpenScape Business TDM user licenses.

The already existing **indirect** migration from HiPath 3000 V7 / V8 to OpenScape Business V2 is still available.

In case of indirect migration, CDB of HiPath 3000 V7,V8 systems must be converted to HiPath 3000 V9, then uploaded into a HiPath 3000 system that has been upgraded to V9 software including 'Hardware and Overwrite" afterwards it can be finally migrated to OpenScape Business.

The converted CDB is uploaded to the new OpenScape Business system with active flags for "Overwrite & Hardware". Afterwards the license dialog has to be executed within OpenScape

Business administration and an appropriate license file for the new OpenScape Business System has to be generated on the Central License Server and has to be imported into OpenScape Business. Details are described within chapter 25 of the administration manual.

The following restrictions have to be considered for successful licensing:

• Registration information must be equal to either Company-ID or the full Company information like - Company Name, address, etc. Otherwise license migration will fail.

• The generated user_info.xml can only be created once during a migration process. If file content is faulty (not equal as described above) the migration must be repeated with a new (or newly created) SDHC card.

For a full description please check the Adminstrator documentation chapter 25

Migration from OpenScape Office HX V3 to OpenScape Business UC Booster Server V2

The migration of an OpenScape Office V3 HX to OpenScape Business Booster Server V2 requires an interim stage to OpenScape Business Booster Server V1R2.2.0 as a direct migration to OpenScape Business Booster Server V2 is not supported.
With OpenScape Business V1 R2.2.0 a conversion script was provided allowing migration of an OpenScape Office HX backup to OpenScape Business UC Booster Server. After migration to V1.R2.2 an upgrade to OpenScape Business V2 can be performed. A detailed step by step guideline is available within chapter 25 of the administration documentation.
Note:
The following UC configuration data and user data are not transferred and must be reconfigured in the UC Booster Server:

- Web services (e.g., XMPP, Web Collaboration, Mobility)
- Open Directory Service
- OpenStage Gate View

Initial start-up of the OpenScape Booster Card

Precondition:
OpenScape Business with OpenScape Booster Card is connected to a Gigabit network.

Hint:
In some cases, depending on the customer network it is possible that the OpenScape Booster Card is not able to connect to OCCx, or loses the connection to the OCCx during operation, even though it has a working LAN link.

Affected software: smaller or equal OSBiz_v1_R2.0.0_033

Workaround:
The easiest way to work around this problem is to temporary use a 10/100 MBit mini switch to connect OCCx and OCAB to the customer's network. No configuration change is necessary in this case.

An alternative way is to configure the OCAB LAN2 port to 100FDX and to connect OCCx

LAN3 port with OCAB LAN1 port directly by using a LAN cord.

As soon as SW OSBiz V1 R2.1.0_279 or higher is available and loaded to the system the workaround must be removed.

Solution:
A software solution will be available with Version OSBiz V1_R2.1.0_279 and higher.

2.1.2. IVM

- HiPath 3000 Trace (see above) IVM trace
- Call Monitoring at the first port of the IVM for reproducible errors
- Other traces may be required after consultation with the Partner Service Desk!

2.1.3. EVM

H3K:

- KDS (incs PW.)
- Default Trace + DW-UPN Level 9 + DH-EVM Level 9 + VMM Level 9
- Eventlock
- Stack
- Detailed description of the error (Please describe the error in details so a third party would be able to understand it.)
  1. Date
  2. Time
  3. Number (caller and call recipient)
  4. Display messages
  5. Type of call (consultation, group, conference, etc.)
  6. Frequency (5x per day, 1x a week, etc.)
- Other trace requirements after consultation with partners support

2.1.4. OSO MX/LX/HX

For this product please see OpenScape Business on section 2.1

Attention: naming for OSO Trace profiles is different from OSBiz and Manager E. Hint: OSBiz embedded is not supported in OSO.

2.1.5. ODC-PE with SIP Provider

If using the ODC-PE configured as **SIP** Provider, please take the following traces as requested:

NOTE: It's important to start all traces/logs BEFORE starting to use ODC-PE.

- ODC-PE **BSTrace** file;
- **MSI** trace file;
- **Wireshark** trace / log file; ➔ this trace is needed if there is a problem with payload/calls.

- When the error occurs, take note what **TIME** it is (format **hour:minutes**);
- Take note of the LOGIN and PROFILE used during the error;
- Add the backup file with the configuration files;
- Sometimes the problem is due to PC processor too high, so send the:
    - Windows type used: Xp/Vista/7- (SP?)
    - Amount of RAM memory;
    - Amount of RAM memory FREE (during ODC-PE use);
- A step-by-step guide on how to reproduce the error
  Example: PartyA_N8900 callsPartyB_N8901; after x minutes / seconds, the call drops, etc.
- Printscreen of error (if it's difficult to explain the details).

ODC-PE with HFA Provider

If using the ODC-PE configured as HFA Provider, please take the following traces as requested:

PS: It's important to start all traces/logs BEFORE starting to use ODC-PE.

- ODC-PE **BSTrace** file;
- **SCI** trace file;
- SoftOla trace file;
- **Wireshark** trace / log file; ➔ this trace is needed if there is a problem with payload/calls.
- When the error occurs, take note what **TIME** it is (format hour:minutes);
- Take note of the LOGIN and PROFILE used during the error;
- Add the backup file with the configuration files;
- Sometimes the problem is due to PC processor too high, so send the:
    - Windows type used: Xp/Vista/7- (SP?);
    - Amount (%) of CPU used during the problem;
    - Amount of RAM memory;
    - Amount of RAM memory FREE (during ODC-PE use);
- A step-by-step guide on how to reproduce the error
  Example: PartyA_N8900 callsPartyB_N8901; after x minutes / seconds, the call drops, etc.
- Printscreen of error (if it's difficult to explain the details).

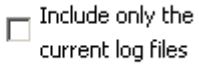
2.2. OpenScape 4000

Mandatory Information:

- Complete regen file
- :PAS: C-FBTHIST
- STA-LOGBK:"<relevant time>";
- DIS-APS;
- DIS-PATCH:SYS;
- DIS-DIMSU;
- DIS-SIGNL:SYSTEM;
- All files from :PAS:HIM/BS/*

1. System restarts:

- Autotrace files from :PAS:ACTF/AT/*
- From V6 if all Portal/Platform Logs, ensure that following is unchecked:



Note: Activate trace from point 2 for next occurrence.

2. Generic trace for 4k problems: path problems, features, etc.:
   - Accurate scenario description: calling, called, time stamp, actions, behaviour
   - 4K trace:

     EX-TRACS:BP;
     copy,hd-tab,8,allstd,y;
     ON,HD,:DIAG:ERROR,500-10,Y,Y; /* ACTIVATION TO HARD DISK, send all files
     End

     Note: display,trcconf; in amo tracs can be used to configure the most apropriate trace for a specific scenario, but number 8 can be used for most of the cases.

3. Additional for IP issues:
   - GW restart:
     All available LOGS (WBM -> Maintenance -> Actions -> Manual Actions -> All Logs)

   - Sniffer and GW traces made for each board with appropriate trace profile using either Assistant IPTrace, Xtracer or Wireshark.

     Note: IPTrace & RPCAP sniffer traces are not sufficient for payload issues and a real sniffer trace must be used e.g. mirror port.

     Profile examples (trk=trunk):
     Profile 1.1.3(detail) SIP Trk. Payload problems
     Profile 1.1.2(detail) SIP Trk. General problems
     Profile 3.2(detail) IPDA Payload problem

NOTE: ***If you are not sure about the flags needed for a specific complex issue please call the Expert Assistant Hotline for further support.***

Please be aware that Unify may then recommend more specific traces and stop conditions based on first analysis.

When a Hard disk is supplied and the ROOT password is different than the standard if it cannot be included as an attachment within gsi-flow for security reasons a contact person must be provided to supply the password.

2.2.1. System Manager and NDSA Problems

2.2.1.1. First time installation and upgrade failure

If the System Manager Server installation can't be started please check whether the following prerequisites are met:

- A functional network interfaces card (NIC) is mandatory and it must be connected to the network.
- The System Manger server must be a member server of a domain (or it can also be the domain controller).
- The user who performs the installation must have domain administrator rights.

If the installation starts but fails at a certain point try rebooting the server. If the problem still occurs provide:

- the <Windows folder>\ SysWOW64\Inst_History_log.txt,
- the c:\Program Files (x86)\Common Files\InstallShield\Engine\6\Intel 32\IKernel_log.txt,
- and a screenshot of the error message

All files mentioned above must be collected while the error message is on the screen (before closing it with OK).

2.2.1.2. Database backup / restore (or merge) failure

If either the backup or restore operation fails

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- and the latest available database backup must be sent to development

2.2.1.3. Database access problems

If the database can't be edited properly via the Systemmanager Admin application please restart it. If the problem still occurs provide:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- a complete database backup,
- a description of the actions performed before the problem occurred,
- and a screenshot of the error message

2.2.1.4. Issues with system configuration

In case of any problems occurring during configuration in the Systemmanager Admin application first try restarting it. If it doesn't help

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- a complete database backup,
- detailed description of the performed configuration
- and a screenshot of any error message (if available) should be attached

2.2.1.5. Issues with turret connection and assignment

For problems with the communication between the system manager and the turrets please provide the following:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- TurretIp.log from the turret(s),
- and 2 Wireshark traces, 1 captured on the System Manager Server and 1 on the turret

2.2.1.6. Issues with MLC connection and assignment

For problems with the communication between the system manager and the MLC server(s)

please provide the following:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- the /var/mlc/mlccp.log,
- the /var/mlc/SMpriorityList.cfg,
- and a Wireshark trace captured on the MLC Server

2.2.1.7. Task scheduling problems

To use scheduled jobs (e.g. to synchronize the ETD) you have to copy the files

On 32 bit systems:

- capi20.dll
- capi2032.dll
- capi20nt.dll from the directory Tools\CAPI to %SystemRoot%\system32
  - And create new registry entry:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Trading E\Systemmanager JobServer]
    "ServerWithoutISDN"="yes"

    or execute ServerWithoutISDN.reg (from CD: Tools\CAPI)

On 64 bit systems:

- capi20.dll
- capi2032.dll
- capi20nt.dll from the directory Tools\CAPI to %SystemRoot%\SysWOW64
  - And create new registry entry:
    [HKEY_LOCAL_MACHINE\Wow6432Node\Siemens\Trading E\Systemmanager JobServer]
    "ServerWithoutISDN"="yes"

    or execute ServerWithoutISDNx64.reg (from CD: Tools\CAPI)

If the scheduled jobs are not executed automatically restart the OpenScape Xpert Job Server service.

- If the problem still occurs please attach all .txt and .dmp files under C:\Program Files (x 86)\Trading_E\Program folder to the ticket.

2.2.1.8. Fault management (SNMP) problems

First of all double check if the CAPFM SNMP client is installed and configured on the system manager server and if Fault Management is enabled in the Systemmanager Admin. If the problem still occurs provide:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- and the c:\Program Files (x86)\Siemens\HiPath CAP\FM\capfmtrace.log

2.2.1.9. Contact Interface problems

Describe the exact hardware configuration, the type and version of the contact interface device and the connection type (local or central).

The files need to be attached to contact interface related tickets (all can be found under C:\Program Files (x86)\Siemens\HiPath Trading CI):

- ConfigData.xml,

- CIService_log.txt,
- LogsForDeveloper.XmlLog,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder from the affected turret,
- Please attach a Starcam trace as well (tracing the turret which intends to use the contact interface device)

2.2.1.10. Licensing problems

If you face any licensing problems, first check if the licenses are valid and are assigned properly in the License Manager. If everything looks good in the License Manager try restarting the OpenScape Xpert License Server service and wait for 5 minutes.

If the problem can't be solved by restarting the service:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- and the whole C:\Program Files\Trading_E\Tb\RBStat folder from the turret must be provided

2.2.1.11. System Manager Admin can't be started

Restart OpenScape Xpert Config Server service. If the problem still occurs send:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder,
- and a screenshot of the error message to GVS

2.2.1.12. Crash of System Manager Admin

If the Systemmanager Admin client crashes attach:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder

2.2.1.13. NDSA backup / restore / disconnect issues

In most cases the NDSA backup / restore issues can be solved by restarting the appropriate services.

If the problem still persists:

- all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder must be provided from both System Managers

2.2.1.14. NDSA failover issues

In case of NDSA failover issues (in case the failover isn't performed within 5-6 minutes) first of all check if the backup SM is reachable from the MLC(s) and Turrets.

- If the primary system manager fails and the turrets are not able to connect the backup system manager:
  - all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder from both System Managers,
  - and the TurretIp_log.txt from a turret is needed

- If the primary system manager fails and the MLC's are not able to connect to the backup system manager:
  - all .txt and .dmp files under the C:\Program Files (x86)\Trading_E\Program folder from both System Managers,
  - and the mlccp.log files from the MLCs are needed

2.2.2. MLC and Voice Recording Problems

2.2.2.1. First time installation and upgrade failure

If the first time installation fails make sure that all prerequisite debian packets are installed (ntp, openssh server,openssh-client, psmisc, pdnsd, libpam-cracklib, sudo) and the MLC server is connected to the LAN

If the problem still occurs provide

- the /var/log/dpgk.log,
- and the whole /var/mlc folder (if exists)

If the manual upgrade fails provide:

- the /var/log/dpgk.log,
- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- and all /var/mlc/mlccp.log<date_time>.txt.gz (e.g.: mlccp.log.2013.09.14__13.54.45.txt.gz) files covering the timeframe of the error

If the automatic upgrade from the system manager (via IIS) fails, first check whether the IIS service is up and running and if it is configured properly (try if you can reach the system manager's shared folders from the MLC server). To verify the IIS service configuration try manually download the mlc package with the wget command (wget -v http://<SM _server_IP>/Mlc_SW/<mlc_package>).

If the MLC package Is reachable and the error still persist provide the following files:

- /var/log/dpgk.log,
- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- and all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error

2.2.2.2. MLC doesn't show up in the System Manager Admin client

If the MLC has been successfully installed but it doesn't appear in the System Manager Admin:

- Check whether the MLC is connected to the LAN and it can communicate with the System Manager Server (both ways)
- Check the /var/mlc/SMpriorityList.cfg file. It should properly contain the SM server's hostname and IP address: 0;19;ipsmgvs01.trading.isec.hu;192.168.11.70
  - The hostname is written to the SMpriorityList.cfg file during the first successful connection. Therefore this information won't be available prior the first successful assignment in the System Manager.

If the problem still occurs provide:

- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/SMpriorityList.cfg,
- the /var/mlc/MLC_Info.txt,
- and a Wireshark trace captured on the MLC server

2.2.2.3. Problems with registering lines on the PBX

If the lines are not registering on the PBX check the network connection of the MLC server and make sure the “SIP Outbound Proxy” field in the MLC Properties is empty unless there is a SIP Outbound Proxy in use.

The following files must be attached to the ticket:

- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/MLC_Info.txt,
- the /etc/resolv.conf,
- the /etc/pdnsd.conf,
- the /etc/default/pdnsd file,
- and a Wireshark trace captured on the MLC server

2.2.2.4. Lines greyed out

If the lines are greyed out try to restart the MLC process and collect the following:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz (e.g.: mixer.log.2013.09.14__13.57.32.txt.gz) files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- and a Wireshark trace captured on the MLC server (start capturing before restarting the MLC process)

2.2.2.5. Crash of the MLC

In case the MLC process crashes (all lines greyed out, red flag in the System Manager Admin) restart the MLC process and provide:

- the /var/mlc/crash<date_time>.tar.gz (e.g.: crash.2013.09.16__16.00.01.tar.gz),
- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- the /var/mlc/mixer.log,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- and all /var/mlc/core* files

2.2.2.6. General call related problems (not possible to establish calls, calls are getting disconnected, basic call features are not working, etc.)

When calls are failing or certain features are not working or not working properly development needs the following information and files:

- a very detailed description of the feature that is used and the way it is used,
- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,

- the /var/mlc/performancemonitor_log.txt,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder from the affected turret,
- and a Wireshark trace captured on the MLC server

2.2.2.7. General call display problems (all turrets are affected)

If something is not displayed properly on all turrets' lines, call queues or speech units please provide:

- the information expected to be displayed (how is it sent by the PBX)
- what is displayed instead (attach a screenshot)
- the /var/mlc/ MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- a Wireshark trace captured on the MLC server,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder from the affected turret,
- and the TurretIP.log from an affected turret

2.2.2.8. General voice quality and speech path problems (all turrets are affected)

In case of system wide distortion, echo, one way audio, speech delays, gaps in the payload the development requires:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- a Wireshark trace captured on the MLC server (before capturing disable the RTP encryption between the MLC and the turrets),
- the recording of the call from the voice recorder,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder from the affected turret,
- and the TurretQaxy.ini from an affected turret

2.2.2.9. DTMF problems

Development needs the following files in order to analyze DTMF problems:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- a Wireshark trace captured on the MLC server,
- and the whole C:\Program Files\Trading_E\Tb\RBStat folder from the turret the DTMF tones were sent from

2.2.2.10. DTMF audio feedback problems

If there are problems with the DTMF audio feedback, please collect the following for

development:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- and a Wireshark trace captured on the MLC server (before capturing disable the RTP encryption between the MLC and the turrets)

2.2.2.11. Voice recording problems

If voice recording is configured, but the voice recorder doesn't record any of the calls or the recording quality is not adequate please collect the following:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- a Wireshark trace captured on the MLC server,
- and a database backup

If the recording works, but the information of the call (e.g. numbers, direction, agent name) is missing or is not correct the problem should be on the Master Tradeboard. Send the following files to development:

- a database backup,
- the TurretIp.log from the Master Tradeboard,
- and a Starcam trace (connected to the Master Tradeboard)

2.2.2.12. Recording warn tone issues

For problems with the recording warn tone (no tone played, problem with the volume or quality) attach the following files to the ticket:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- the SmAdmin_log.txt,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder from the affected turret,
- a Wireshark trace captured on the MLC server,
- and a database backup

2.2.2.13. Performance issues

If the MLC regularly switches overload protection mode on provide the following:

- the /var/mlc/MLC_Info.txt,
- the /var/mlc/mlccp.log,
- all /var/mlc/mlccp.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mixer.log,
- all /var/mlc/mixer.log<date_time>.txt.gz files covering the timeframe of the error,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt,
- a Wireshark trace captured on the MLC server,
- copy of the output of the following Linux commands:
  - cat /proc/cpuinfo,
  - pstree –pah,
  - top –h,
- and the following information:
  - is the MLC server virtualized, or native?
  - is the Hyperthreading CPU feature enabled in BIOS (on native servers)?

2.3. OpenScape Xpert Client Problems

2.3.1.1. First time installation and upgrade failure

If the first time installation fails make sure the Windows PC is a member of the Domain and the user performing the installation has local administrator rights. It is also mandatory that the client PC is connected to the LAN.

If the problem still occurs provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder

If the upgrade fails provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder

2.3.1.2. OS Xpert Client doesn't show up in System Manager Admin

In case the OS Xpert Client application has been successfully installed but it doesn't appear in the System Manager Admin:

- Check whether the Turret PC is connected to the LAN and it can communicate with the System Manager Server (both ways)
- Check if the System Manager name is correctly entered in the Registry under the HKEY_LOCAL_MACHINE/SOFTWARE/Siemens/Trading E/TB/ServerName key
- If not it can be corrected by initiating a "Change/Remove" process in "Add Remove Programs" in Control Panel and selecting "Modify"

If the problem still occurs provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- and a Wireshark trace captured on the Turret PC

2.3.1.3. Configuration edit problems

If the configuration can't be edited on the OpenScape Xpert client collect the following:

- screenshot of any error message appears,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- and a complete database backup

2.3.1.4. OpenScape Xpert Client crash, or freeze

If the OS Xpert Client application closes unexpectedly provide the following:

- screenshot of the error message that appeared when the client crashed,
- and the whole C:\Program Files\Trading_E\Tb\RBStat folder

2.3.1.5. Blue screen problem (BSOD) on OpenStage Xpert 6010p

If the OpenStage Xpert device has a blue screen OS failure the following must be provided:

- a photo of the message on the blue screen,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- the operating system dump file (%SystemRoot%\Memory.dmp),
- and the operating system event logs

2.3.1.6. Lines are greyed out (not system wide - only on a certain turret)

When the lines on a certain turret are greyed out provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- a Wireshark trace captured either on the MLC or on the Turret PC,
- the /var/mlc/mlccp.log,
- the /var/mlc/mixer.log,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt from the MLC server

2.3.1.7. Audio and speech device problems (not all turrets affected)

Before reproducing the problem please make sure the Qaxy Statistics Collector is enabled in C:\Program Files\Trading_E\Tb\TurretQaxy.ini: [QSC] ACTIVE=1

After reproduction it should be switched off: [QSC] ACTIVE=0

- If there's a problem with the overall quality of the speech / tones provide the following:
  - the whole C:\Program Files\Trading_E\Tb\RBStat folder
  - the C:\Program Files\Trading_E\Tb\TurretQaxy.ini file,
  - detailed description of the used speech devices,
  - some screenshots of the UVCView tool showing the firmware version of all USB devices of the OpenStage Xpert 6010p or the USB Analog Adapter,
  - and a Wireshark trace captured either on the MLC or on the Turret PC, but before capturing please disable SRTP encoding in the System Manager
- If there's no sound on a certain handset/speaker or on the whole device send the following:
  - the whole C:\Program Files\Trading_E\Tb\RBStat folder,
  - the C:\Program Files\Trading_E\Tb\TurretQaxy.ini file,
  - detailed description of the used speech devices,
  - and some screenshots of the UVCView tool showing the firmware version of all USB devices of the OpenStage Xpert 6010p or the USB Analog Adapter
- If there is a problem with the speech device assignment:
  - the whole C:\Program Files\Trading_E\Tb\RBStat folder,
  - the C:\Program Files\Trading_E\Tb\TurretQaxy.ini file,

- and a detailed description of the used speech devices are needed

2.3.1.8. Echo problems

If there's a noticeable echo in the handset/speaker of the client please do the following:

- Shut down the Turret.
- Set the AEC-CONFIGURATION of the used device to ACTIVE:2
- Start the Turret.
- Ensure that the available hard disc space is at least 4 MBytes for every minute of recorded echo canceller activity.
- Reproduce the echo problem. Input and output sample streams will be written into files named Rin_, Sin_, Serr_, Sout_ with a suffix for the echo canceller instance.
- Shut down the Turret. The latest echo canceller coefficients will be written into files named Cout_ with suffix.
- Set the AEC-CONFIGURATION of the used device to ACTIVE:1
- Supply the generated files as trace data for analysis together with a description of the test scenario.
- The Turret can be restarted

2.3.1.9. Problems with telephony features (consultation, transfer, call forward, etc.)

If there's a problems with certain telephony features collect the following:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- the /var/mlc/mlccp.log,
- the /var/mlc/mixer.log,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt from the MLC server,
- and a Wireshark trace captured on the MLC server

2.3.1.10. Line conference issues

If the line conference feature doesn't work properly provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- the /var/mlc/mlccp.log,
- the /var/mlc/mixer.log,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt from the MLC server,
- and a Wireshark traces captured on all involved MLC servers

2.3.1.11. Speech Monitoring (SPM) problems

If there's no sound or the sound quality is not adequate on the SPM channel please collect the following:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- the C:\Program Files\Trading_E\Tb\TurretQaxy.ini file,
- a detailed description of the used speaker(s)
- the /var/mlc/mlccp.log,
- the /var/mlc/mixer.log,
- the /var/mlc/mlc.audit.log_<date>,
- the /var/mlc/performancemonitor_log.txt from the MLC server,
- and a Wireshark trace captured either on the MLC or on the Turret PC, but before

capturing please disable SRTP encoding in the System Manager

If the SPM channel assignment fails provide:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- and a complete database backup

2.3.1.12. Busy indicator issues

If the busy indicator doesn't work properly collect:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- and the SmConfigServer_log.txt from the System Manager Server

2.3.1.13. CTI interface problems

In case of problems with the OpenScape Xpert client's CTI interface provide the following:

- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- a Starcam trace (tracing the turret which intend to use the contact interface device),
- and a complete database backup

2.3.1.14. Contact Interface problems

Describe the exact hardware configuration. The type and version of the contact interface device and the connection type (local or central).

The files need to be attached to contact interface related tickets (all can be found under C:\Program Files\Siemens\HiPath Trading CI):

- ConfigData.xml,
- CIService_log.txt,
- LogsForDeveloper.XmlLog,
- the whole C:\Program Files\Trading_E\Tb\RBStat folder,
- and please attach a Starcam trace as well (tracing the turret which intend to use the contact interface device)

2.3.1.15. Memory leak problem

If the TurretIp.exe or the TurretQaxy.exe processes are having memory leak issues (continuous increase of memory usage) please install the Debugging Tools for Windows and prepare it for making UMDH traces. (Please contact GVS for the mycache.zip, the TurretIp.pdb and the Debugging Tools for Windows).

- Copy mycache.zip and extract it to a local folder: mycache,
- put the TurretIp.pdb to the c:\MySymbols folder.
- Install the Debugging Tools for Windows.
- Open Debugging tools/Gflags, and on the graphical interface choose the Image File tab. Type the process name, including the file name extension (for example, TurretIp.exe). Press the TAB key, select Create user mode stack trace database, and then click Apply.
- Right click on My Computer, select Properties and open the Environment Variables on the Advanced tab. Create a new system environment variable with the name OANOCACHE and the value 1.
- Before using UMDH, you must have access to the proper symbols for your application. You should copy all the .pdb files to a local folder (for example c:\MySymbols), and after that create a new system environment variable called

_NT_SYMBOL_PATH
    - The value should be something like this: c:\MySymbols;srv*c:\mycache*http://msdl.microsoft.com/download/symbols (c:\mycache is a valid cache folder to use as your downstream store for using the public Microsoft symbol store for your Windows symbols)
- Add the location of umdh.exe to the PATH system environment variable. (usually c:\ C:\Program Files\Debugging Tools for Windows (x86))

After installing the Debugging Tools for Windows and preparing the system for UMDH tracing the following actions need to be done in order to capture traces:

- Run the application in which you think there are memory leaks.
- Open task manager and search for the PID (Process ID) of the running application (Important: Every time you restart the application, the PID will be changed)
- open a command prompt and type the following command when you would like to create a snapshot of the memory usage of the running application:
    - umdh -p:1111 -f:c:\UMDH\log_01.log (1111 is the PID, log_01.log is the target log file)
- After ONE DAY! you should create another log file of the current memory usage (log_02.log)
- When both log files are available send them to GVS.
- Please send the C:\Program Files\Trading_E\Tb\RBStat folder as well.

2.3.1.16. User interface and display problems

In case of problems with the OpenScape Xpert turret's user interface please provide the following:

- screenshot of the user interface,
- and the whole C:\Program Files\Trading_E\Tb\RBStat folder

2.3.2. How to set up logging and capture traces

2.3.2.1. Debug level logging on system manager

The logger settings for each System Manager Server components are located under C:\Program Files (x86)\Trading_E\Program\

- DbRecover_logger_settings.lcp
- DbRepair_logger_settings.lcp
- DbUpgradeAll_logger_settings
- LicenseServer_logger_settings.lcp
- SmAdmin_logger_settings.lcp
- SmConfigServer_logger_settings.lcp
- SmDcomServer_logger_settings.lcp
- SmJobServer_logger_settings.lcp
- SmRestoreDb_logger_settings.lcp
- SmToolInitDB_logger_settings.lcp
- SmUpdateDb_logger_settings.lcp

To increase the log level of a certain component adapt the 2nd line of the related .lcp file:

- for info level logging: log4cplus.rootLogger=INFO, File

- for debug level logging: log4cplus.rootLogger=DEBUG, File

Setting the logs to DEBUG level dramatically increases the amount of data written to the log files. Please consider the available space on the hard disc.

In order to increase the maximum size of a log file modify the following value:

- a limit of 5MB per log file: log4cplus.appender.File.MaxFileSize=5MB
- a limit of 20MB per log file: log4cplus.appender.File.MaxFileSize=20MB

The amount of log files to maintain before overwriting the oldest one can be set like this:

- use only one file: log4cplus.appender.File.MaxBackupIndex=1
- use 5 files to store log date: log4cplus.appender.File.MaxBackupIndex=5

2.3.2.2. Debug level logging on the OpenScape Xpert Client

The logger settings for each OpenScape Xpert Client components are located under C:\Program Files\Trading_E\Tb\

- TurretIp_logger_settings.lcp
- TurretQaxy_logger_settings.lcp
- TurretStartup_logger_settings.lcp

To increase the log level of a certain component adapt the 2nd line of the related .lcp file:

- for info level logging: log4cplus.rootLogger=INFO, File
- for debug level logging: log4cplus.rootLogger=DEBUG, File

Setting the logs to DEBUG level dramatically increases the amount of data written to the log files. Please consider the available space on the hard disc.

In order to increase the maximum size of a log file modify the following value:

- a limit of 5MB per log file: log4cplus.appender.File.MaxFileSize=5MB
- a limit of 20MB per log file: log4cplus.appender.File.MaxFileSize=20MB

The amount of log files to maintain before overwriting the oldest one can be set like this:

- use only one file: log4cplus.appender.File.MaxBackupIndex=1
- use 5 files to store log date: log4cplus.appender.File.MaxBackupIndex=5

2.3.2.3. Logging and log file handling on the MLC server

- The MLC is set to debug level by default. No need to modify it.
- When sending MLC traces to GVS please make sure that the time of the failure is covered by the log files. All mlccp.log, mixer.log files are automatically compressed after reaching 100Mbytes. These log files are stored in gzip files and are automatically deleted after 7 days. The compressed files are named according to the date and time they are containing logs from. This means every gzip file contains all logs from the time indicated by the file name till the time of the following gzip file.
  - the mlcccp.log files are compressed as: mlccp.log.2012.01.08__21.49.11.txt.gz
  - the mixer.log files are compressed as: mixer.log.2012.01.08__21.44.55.txt.gz
- If development is requesting the MLC logs with M5T tracing activated the following should be done in the /var/mlc/mlccp_logger_settings.lcp file:
  - Switch M5T logging on modify line "#log4cplus.logger.dpcy.M5T=DEBUG" to "log4cplus.logger.dpcy.M5T=DEBUG" (remove the # mark from the beginning),

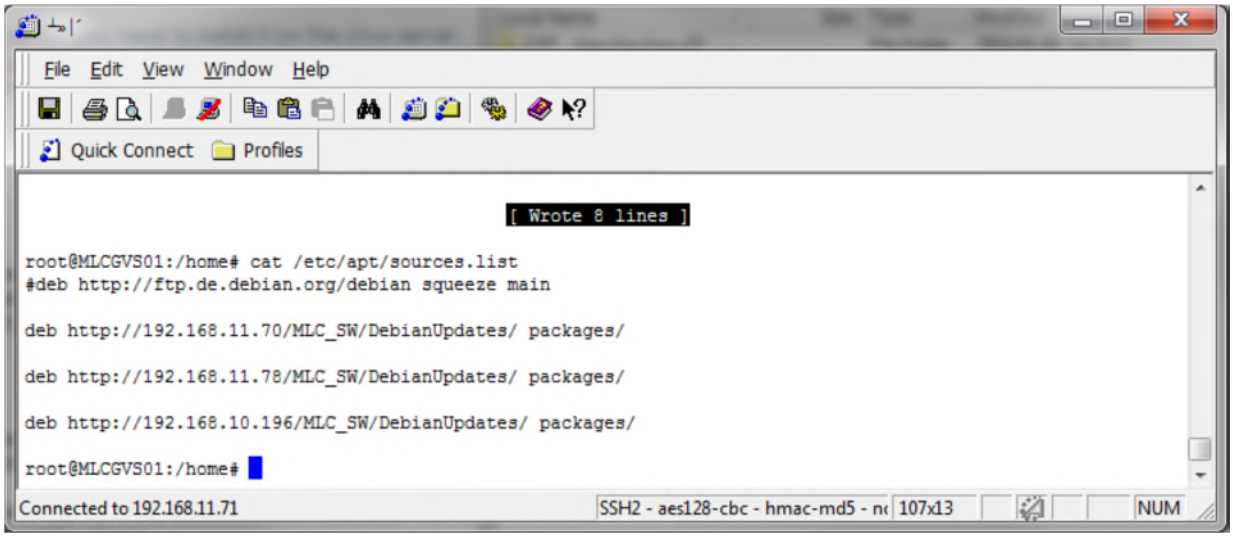
- Save changes to file "mlccp_logger_settings.lcp".
- To switch M5T logging off modify line "log4cplus.logger.dpcy.M5T=DEBUG" back to "#log4cplus.logger.dpcy.M5T=DEBUG" (add the # mark to the beginning).

2.3.2.4. Capturing network trace (tcpdump or tshark) on the MLC server

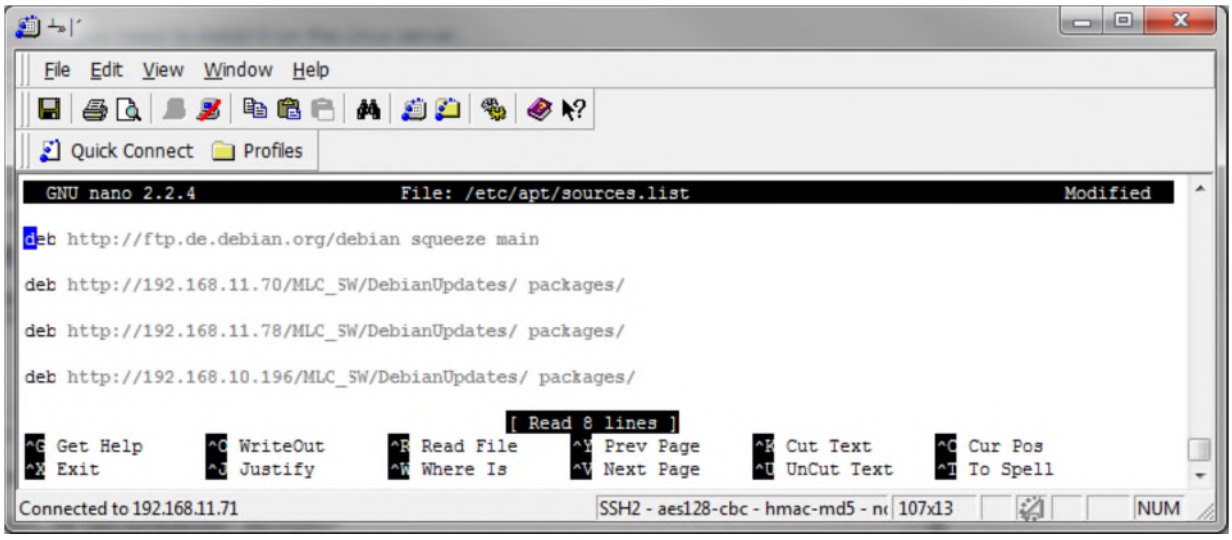
First, either tcpdump or tshark has to be installed on the MLC server. The following example shows how tcpdump can be installed and used.

The easiest way is to use Debian's sources with the apt-get command since it will install it with all necessary dependencies. This requires internet access on the MLC. If the MLC has access to the internet then please check whether one of Debian's FTP server is configured in the /etc/apt/sources.list file.

- cat /etc/apt/sources.list



- If it is commented out with a # like on the screenshot above you'll need to uncomment it. If there's no FTP listed in here you'll need to add it (for Germany: ftp.de.debian.org/debian).
  - The recommended text editor in Debian is Nano.
  - nano /etc/apt/sources.list



- After editing the file please press "Ctrl + x" to exit nano and then press "y" to save

the changes of the sources.list file.

- Now tcpdump can be installed with the apt-get install tcpdump command.

If no internet access is available on the MLC server then you'll need to download tcpdump and all depending packages.

- for debian V6: http://packages.debian.org/squeeze/tcpdump
- for debian V7: http://packages.debian.org/wheezy/tcpdump

These packages can be installed with the dpkg –i command (just like the MLC package) after transferring them to the MLC server.

Once installed you can capture all traffic on the MLC server with this command: tcpdump -n -i any –w /home/capture.pcap,

This will create a file, named capture.pcap under the home folder and write the traces into that file.

2.3.3. HiPath CAP/CSTA

2.3.3.1. Component Specific Tracing – HiPath CAP V3.0

1 Standard logging for SCC/P

The standard logging should be enabled. It should be adjusted for all

SCC (300,3000,4000,8000,DX,etc..)

SCCP

LogLevel settings

Please edit <installdir>\HiPathCTI\config\<Server Name>\telasserver/sccp_<SCC/P Id>\Telas.cfg !

The following entries and values should be set:

log.level = 5

debugLevel = 9

cstaLogEnabled = 1

The settings above increase the number of lines logged, the use of direct file logging is adviced. It can be set with

the following entries:

2 File logger for SCC/P

```
# File System Location
# ====================
# <volume>:...\HiPathCTI\distribution\config\SccP\Telas.cfg
# ========================================
# logging and tracing
# -----------------------------------
# level settings for all loggers
```

```
#------------------------
loggerHistoryLevel = 0
loggerFileLevel = 9
loggerCapLevel = 0
loggerBoxLevel = 0
# capLogger settings
#------------------------
capBlockmode = 1
# fileLogger settings
#------------------------
loggerFile = <installdir>\HiPathCTI\logs\<Server Name>\%s_logger.log
loggerFileMaxSize = 100000
loggerFileNum = 10
fileMode = continuous
#fileMode = StopOnError
#fileMode = DumpOnError
#fileMode = SystemOnError
# history logger settings
#------------------------
historySystem = copy a b
historyTrigger = triggerstring
# history logger trigger settings
#------------------------
#triggerMode = continuous
triggerMode = DumpOnTrigger
#triggerMode = StartOnTrigger
#triggerMode = StopOnTrigger
#triggerMode = SystemOnTrigger
#triggerMode = CrashOnTrigger
```

In the loggerFile setting the <installdir> and <Server Name> parts should be replaced with the actual data.

loggerFileNum specifies the number of logfiles created, the loggerFileMaxSize specifies the length of one logfile.

3 Standard logging for CA4000/SAT/SPI

For CA4000 please edit

<installdir>\HiPathCTI\config\<Server Name>\ca4000_<ca4000 Id>\ca4000.cfg

log.level = 5

For SAT please edit

<installdir>\HiPathCTI\config\<Server Name>\sat\sat_svc\SatServer.cfg

LOG_LEVEL = 5

For SPI please edit:

<installDir>\HiPathCTI\config\<Server Name>\spi\Telas.cfg

log.level = 5

debugLevel = 9

traceLevel = 5

4 Standard logging for XMPLS

Please edit <installdir>\HiPathCTI\config\<Server Name>\ XMLPhoneSvc_<XMLPS Id>\Telas.cfg !

The following entries and values should be set:

log.level = 5

debugLevel = 9

Note: These modifications require the restart of the corresponding call control modul(s) in Diagnostic Agent.

2.5 Configuring longer logfiles

In several case when trace has been saved, it does not contain the logs, when the issue occurred (logs has been run

out). For more and longer CAP logs please edit

<installdir>\HiPathCTI\config\common\global.cfg

log.level = 5

log.maxLines = 500000

log.maxFiles = 20

<installdir>\HiPathCTI\config\<Server Name>\admin\log\LogServer.cfg

Here are the entries which has to be modified (for all affected SCC/P):

log.maxLines.<SCCP Id>_Error = 500000 (size of the log in lines)

log.maxFiles.<SCCP Id>_Error = 20 (number of log files)

log.maxLines.<SCC4000 Id>_Error = 500000

log.maxFiles.<SCC4000 Id>_Error = 20

E.g.:

log.maxLines.SCCP_Error = 500000

log.maxFiles.SCCP_Error = 20

log.maxLines.HP4000_Error = 500000

log.maxFiles.HP4000_Error = 20

6 Additional traces in case of HiPath4000 V6

In case of HiPath4000 V6 the logfiles of CA4000 can be collected from the integrated CSTA: pls see the

7 Crash situations

In case of crash of SCC, SCCP, SPI or XMPLS components it may be useful to have an additional trace file. It can be

activated the following way.

- Stop the regarding process in Diagnostic Agent on the "Processes" tab

- In the directory

<installdir>\HiPathCTI\config\<Server Name>\telasServer_<SCC, SCCP, SPI or XMPLS Id>

copy the following lines into S10service_ctrl.proc:

args: -l

args: 6

args: -f

args: <?x $INST ?>/logs/<SCC, SCCP, SPI or XMPLS Id>Trace.txt

The name of the txt could be for example:

args: <?x $INST ?>/logs/SCC4000Trace.txt

- Start SCC/P or XMLPS in Diagnostic Agent7.1 Crash situations in case of Windows 2008/Windows 7 or above

Additional note: If a process has not been crashed, just 'frozen' (it means that Diagnostic Agent shows with red status but in the Task Manager the regarding process is still running) then the dump file can be generated with the following method (it is working only on Windows operation systems):

Open the Task Manager, select the regarding process click right mouse-button and select the 'Create dump file' menu – it saves the dump file for the frozen process.

7.1 In case of Windows 2008/Windows7 the crashcatcher doesn't generate any dumpfiles when crash happens (cause: the used userdump.exe isn't supported on these operation systems)

For a workaround the dumpfiles can be generated with the following method:

For all configuration processes (SCC, SCCP or XMLPS) a new key should be created in the registry:

E.g. if an SCC4000 has been already configured in CAP, then into the registry it should be entered:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps\SccHiPath4000.exe]

"DumpFolder"= REG_EXPAND_SZ: <CAP installation path>\logs

"DumpCount"=dword:00000005

"DumpType"=dword:00000002

If done the process should be restarted.

More hints can be found in the URL:
http://blogs.msdn.com/b/dasane/archive/2010/02/18/taking-the-usermode-dumps-on-windows-2008-server-windows-7-where-debug-diagnostics-1-1-does-not-work-yet.aspx

8 Performance problems

It is possible there are performance problems if any of the following symptoms can be observed:

- there are delays in the message processing of CAP
- a CAP component uses 100% CPU for more than 1-2 seconds
- the memory usage of a component increases continuously (without end)

In this case further analysis requires performance logs. It takes longer and more CAP logs and performance monitor log files.

For more and longer CAP logs please see cap. 2.5

In order to have performance monitor logs please start performance monitor (it refers if CAP is running under

Windows)!

(perfmon.exe)

Choose „Counter Logs", then „New Log settings..." by right clicking.

Add a name and add counters to the measurement for every affected process (SCC/P):

- „Process" -> SCC/P -> %Processor time -> Add
- „Process" -> SCC/P -> Private Bytes -> Add

add the overall processor time, too:

- „Processor" -> Total -> %Processor time -> Add

Set the interval to 1 second.

Set the Log File to a „Text file (Comma delimited)" and set „End file names with: mmddhhmm"

Finally schedule the measurement to be started and stopped manually.

By right clicking on the name of the measurement it can be started and stopped.

The log file will be generated in the given directory.

9 Problems with SPI service

In case you experience problems with Service for Pbx Information component please adjust the following settings.

In case there are many devices configured on the specific Hipath4000 then the timeout should be adjusted to let

CAP management query all devices from the switch.

In <installDir>\Siemens\HiPathCTI\config\<Server name>\admin\mgmnt\admin.cfg

SysMgmtTimeout = 600000

If you experience further problems please activate SPI tracing.

XML-Trace for SPI Service

SPI.traceDir = <?x $INST_DIR ?>/logs

SPI.traceHeader = true

And additional modificate the following entries in the config file of SPI:

<installDir>\Siemens\HiPathCTI\config\hu3cb9fc\spi\Telas.cfg

log.level = 5

debugLevel = 9

traceLevel = 5

The additional SPI traces will be generated here:

<intsallDir>\Siemens\HiPathCTI\logs\SPITraceFile.txt

<intsallDir>\Siemens\HiPathCTI\logs\SPI_XML.trc

These modifications require a CAP service restart.

Remark to SPI (switch configuration)

SPI provides the canonical prefix information to the device numbers if only the Dialling Plan Data is configured in the HiPath4000.

See the following AMOs:

DISP-ZAND:ALLDATA;

REG-KNDEF:KNNR=<PNNO>;

where PNNO is the value of the PNNO parameter in the response of the AMO disp-zand: alldata.

If the following parameters in the last AMO response should have reasonable configured values: ISDNCC, ISDNAC, ISDNLC.

10 TAPI specific problems

For TCSP logging, the following settings have to be made in the registry, under

HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Tcsp:

Add new String Value, with name 'FileLog', and value 'C:\Tcsp.log' (or what is more convenient).

Increase the value of the tcspDebugLevel to 10 (decimal).

Restart the PC, so settings will take effect.

[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Tcsp]

"FileLog"="C:\\tcsp.log"

"tcspDebugLevel"=dword:0000000A

Additionally enhance the log level of the affected SCC and CA4000 as well!

After problem reproduction provide the TAPI log and the CAP sysdiag zip too.

11 Installation problems on Windows

Please provide the output of <sg.msi or setup.exe> /L*v <somepath>\install.log

12 Sniffer logging

The sniffer logging provides information about data flow between the switch and CAP. For these logging you need to install and configure the following:

First you need the Ethereal program – it can be downloaded from official site: http://www.ethereal.com

This document created by using version 0.10.14

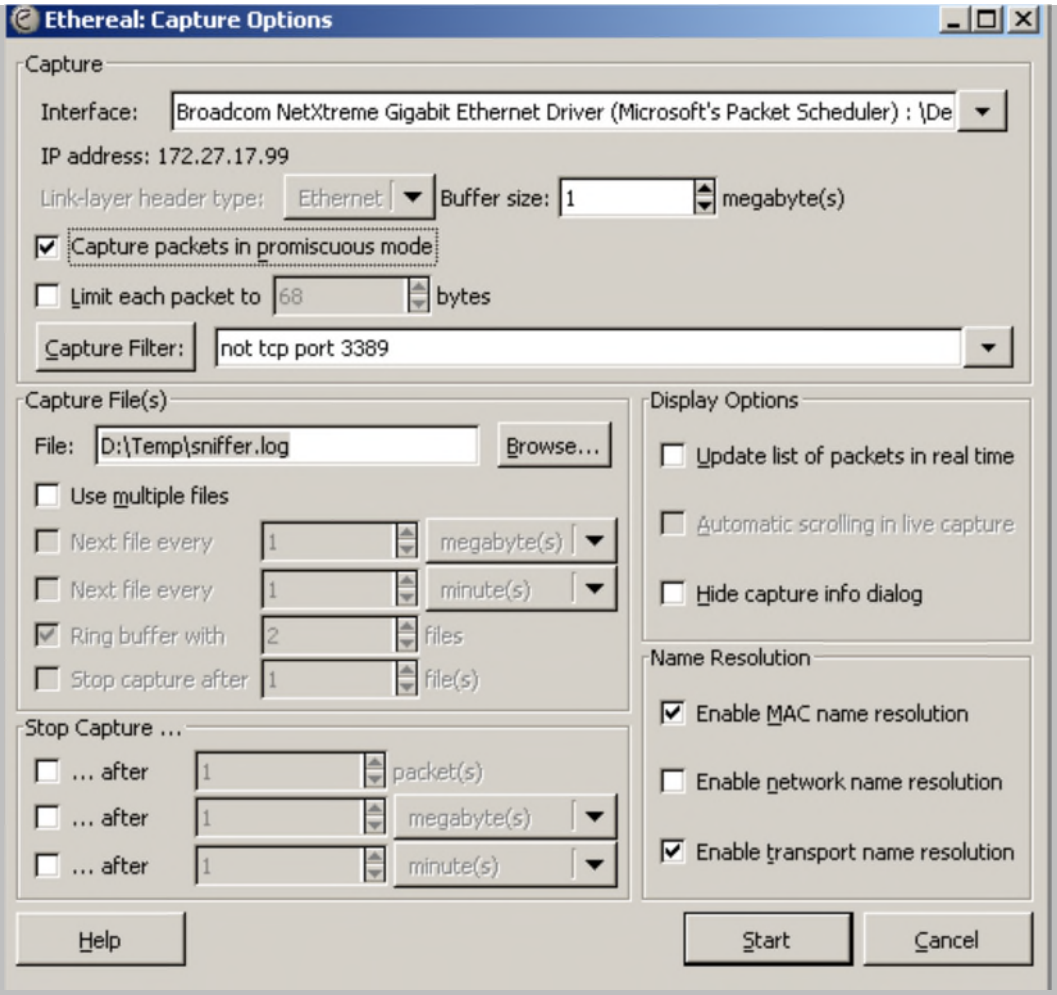
After it has been installed, start it. You should configure the following settings in the Capture/Options menu:

- Interface: select the appropriate network adapter (which is using by CAP)

- Change the buffer size regarding the scenario (if scenario is difficult then increase it to 10 MB)

- Enter the name and the location of the capture file (e.g. sniffer.log)

If all was done, click on the start button. Reproduce the error-scenario, stop the capture and save the logfile.



13 How to check version info?

How to check the version number of SCCP/SCC4000?

1. Choose "snapshot" on the SCCP/SCCC4000 in Diagnostic Agent on the "Processes" tab
2. Click on "status" and check the "Version" value

How to check the version number of CA4000?

1. Choose "snapshot" on the CA4000 in Diagnostic Agent on the "Processes" tab
2. Click on "status" and check the "ca4000_version" value

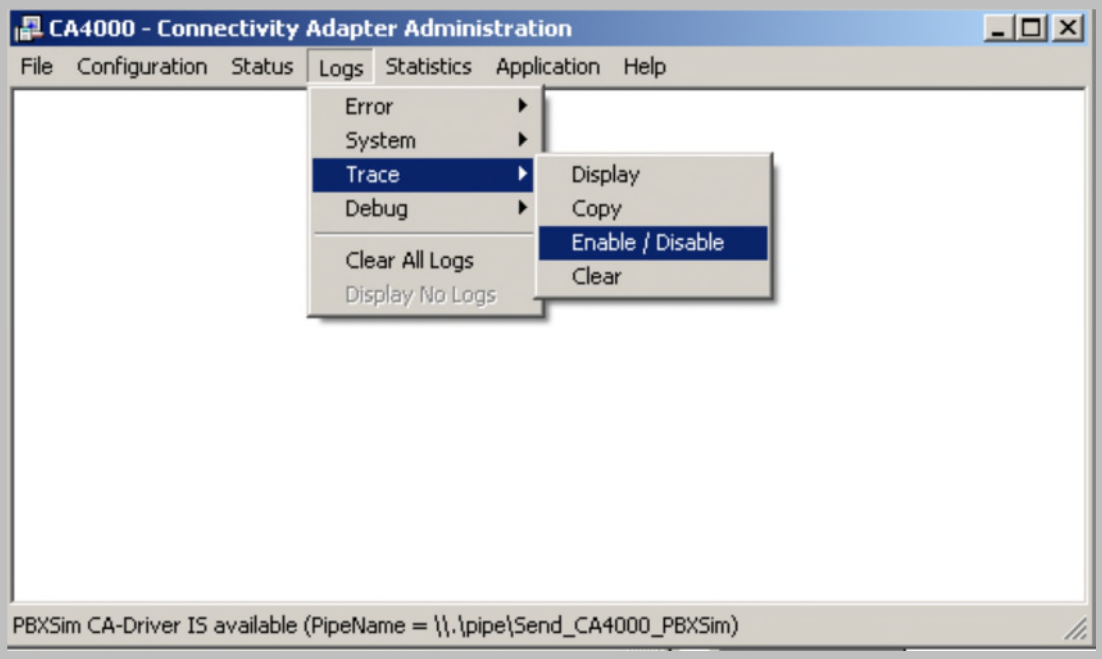
2.3.3.2. Component Specific Tracing – CAP Inside

1. Configure of Standard logging

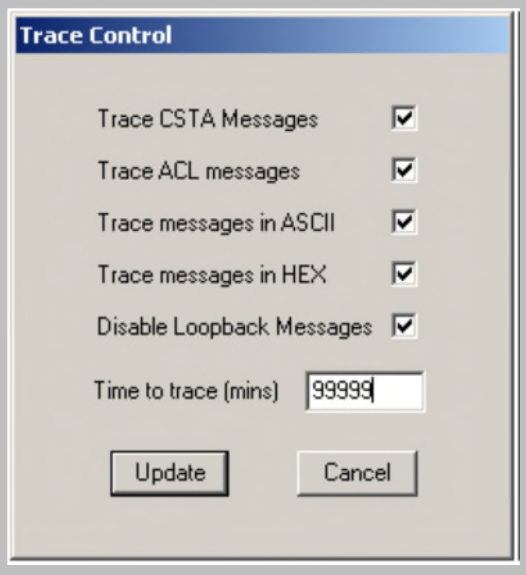
For the required CA4000 trace log, please make the following settings in CA4000 - Connectivity Adapter

Administration window in Logs -> Trace -> Enable / Disable menu

point:



point:



Check the following points:

- Trace CSTA Messages
- Trace ACL Messages
- Trace messages in ASCII
- Trace messages in HEX
- Disable Loopback Messages

Time to trace must be a non-zero value.

The CA4000 trace log file will contain the CSTA and ACL messages in ASCII and HEX form.

2. Collecting the traces

In case any error happens please always provide the following files:

From <installdir>\Logs\<Server Name>\CA4000_<PBX Id> directory:

- debug.log
- debug.bak (if available)
- error.log
- error.bak (if available)
- system.log
- system.bak (if available)
- trace.log
- trace.bak (if available)

From <installdir>\Logs\<Server Name>\CAServiceLog directory:

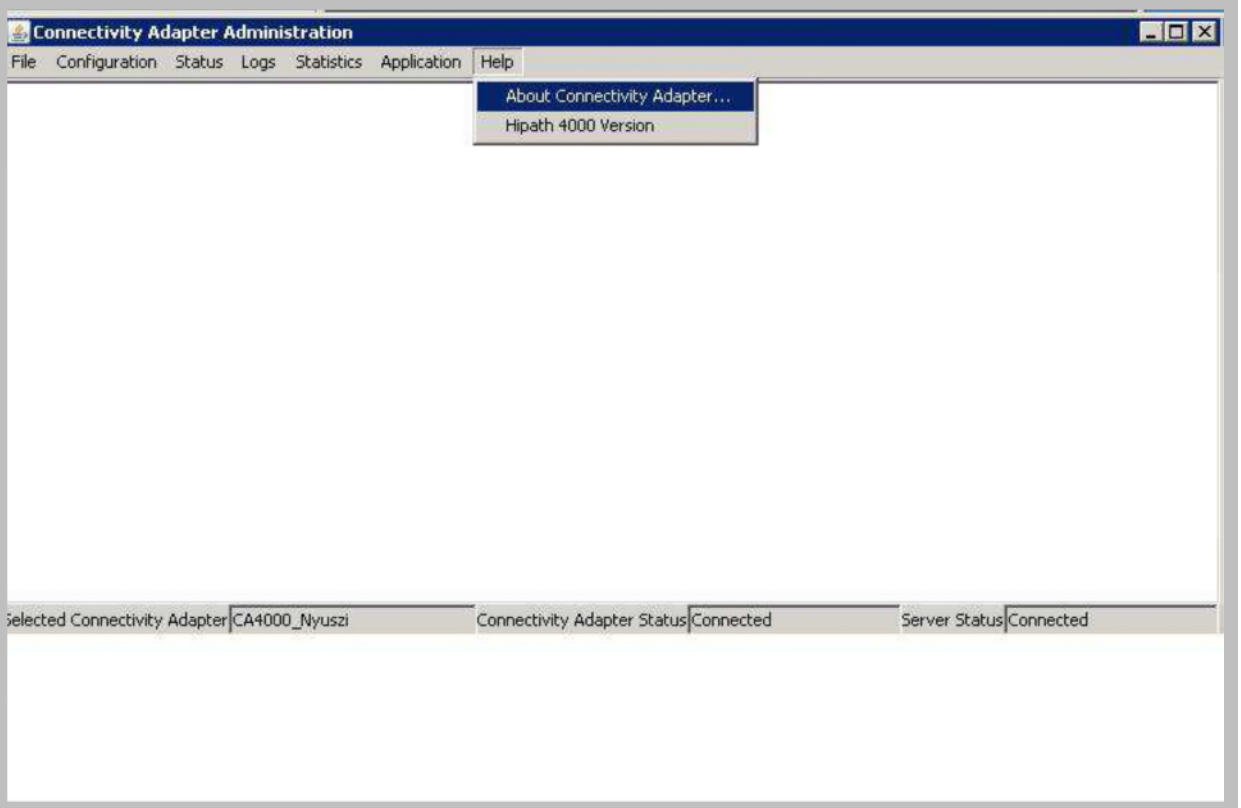
- zoom.log

From <installdir>\config\<Server Name>\CAServiceLog directory:

ca4000.cfg

3. How to check the version info?

Click on the “About Connectivity Adapter…” menupoint from the Help menu:

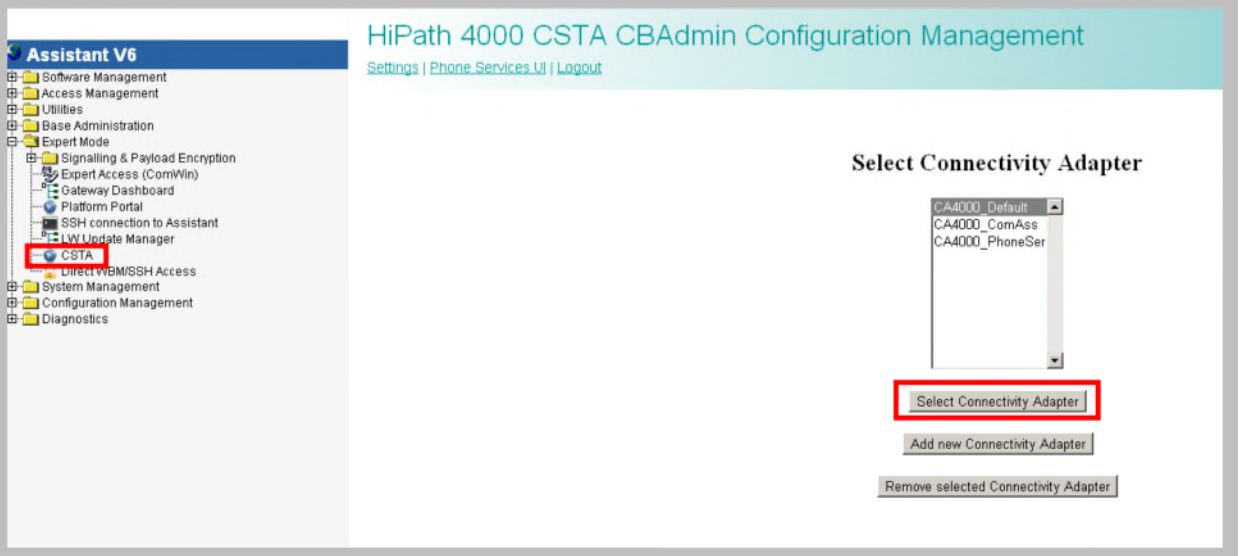


The versions of CB Admin, CB driver and CB starter will be shown.

2.3.3.3. Component Specific Tracing – HiPath 4000 CSTA

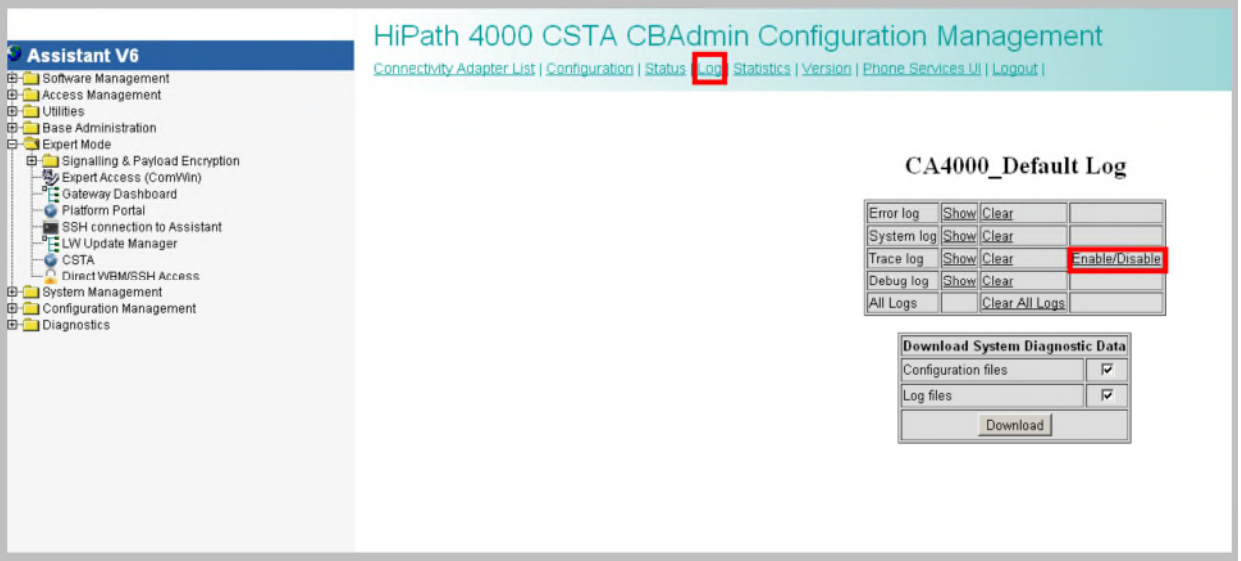
1 Activating the tracing

First select the Connectivity Adapter:

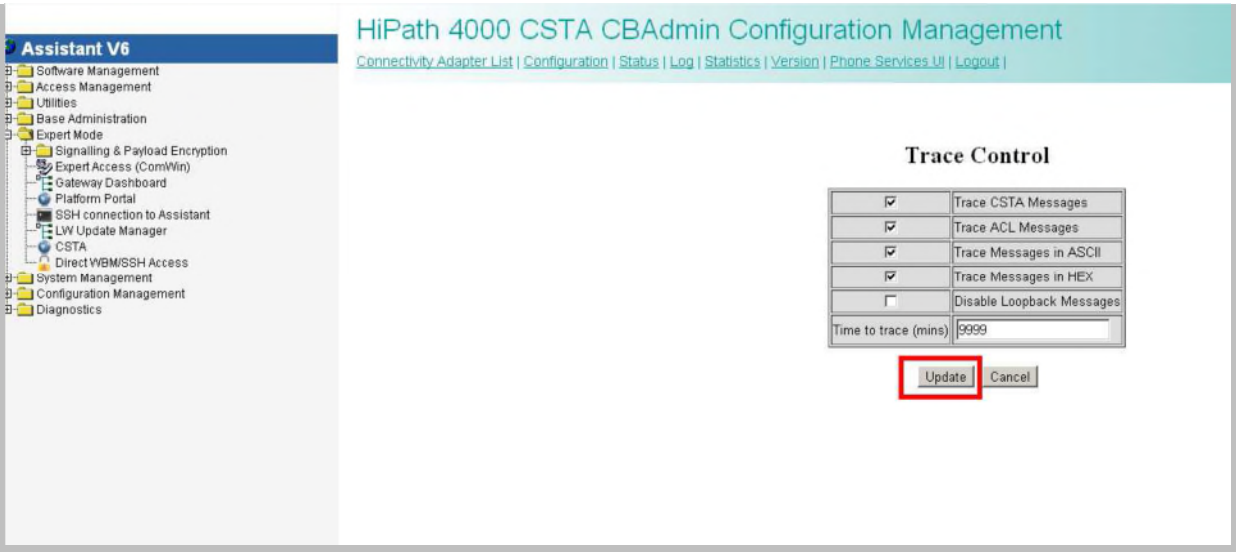


1.1 Before Version V7R2

Next select the Enable/Disable menupoint from the Logs menu:

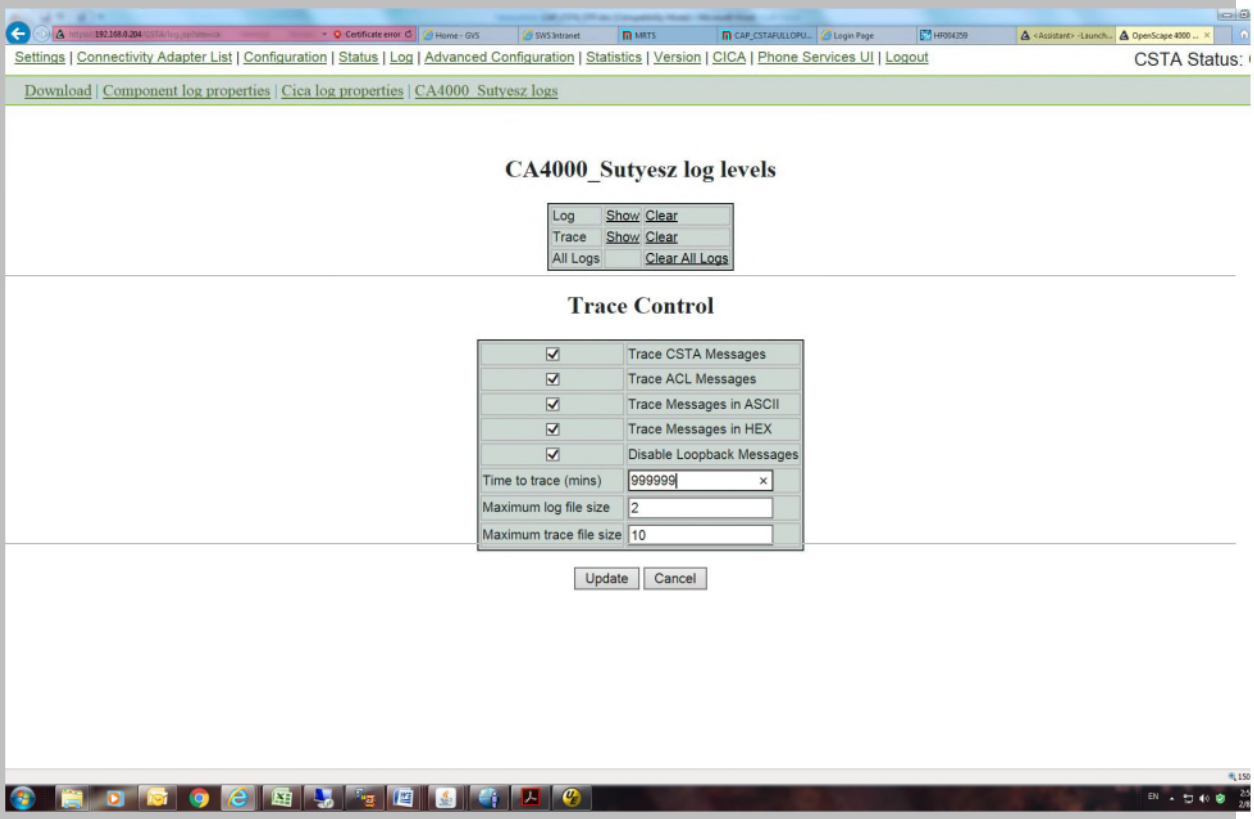


Last activate the checkboxes and set 999999 in the field “Time to trace (mins)”:



1.2 From version V7R2

Next set 999999 in the field “Time to trace (mins)” from the Logs/CA4000_<CA-name>_logs menu:



In the field “Maximum log file size” the size of the logfile can be added.

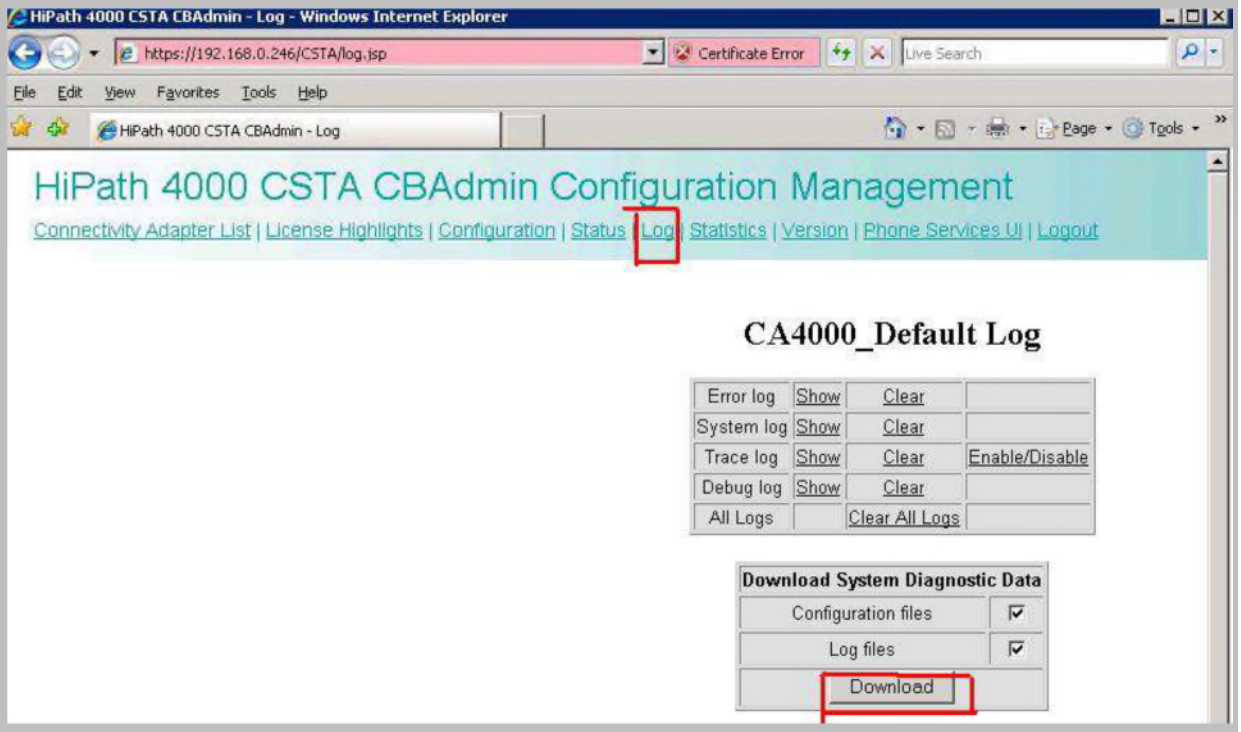
In the field “Maximum trace file size” the size of the tracefile can be added.

Please change these from default values only after consulted with GVS collegaues.

2. Collecting the traces

2.1 Before version V7R2

From the menu Log activate both the checkboxes “Configuration files” and “Log files” then click on the button Download



2.2 From version V7R2

From the menu Log/Download activate both the checkboxes “Configuration files” and “Log files” then click on the button Download

Note: if WBM is not working, then trace can be collected via the following method:

From the CSTA VM the log and config directory should be first compressed via the following command:

linux:/opt/siemens/CSTA/Logs # tar cjvf csta_log_config.tar.bz2 /opt/siemens/CSTA/Logs/ /opt/siemens/CSTA/config/

Then this compressed file should be copied via sftp or scp.

3. Standalone version

The integrated CSTA can be accessed via Assistant Expert mode/CSTA (see 1. picture in cap. 4.1)

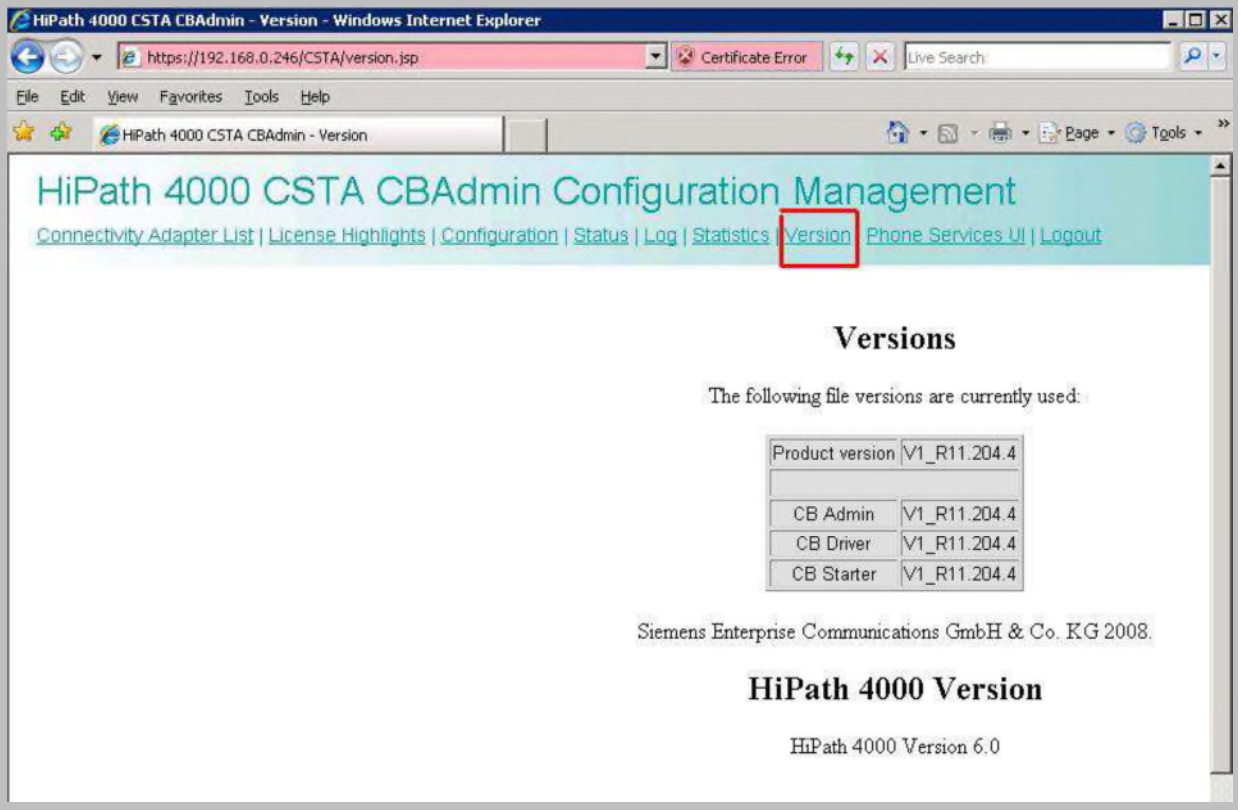
The standalone version (both windows and linux) can be accessed via the following URL:

http://<servername>:8080/CBAdmin

When it is done, then the functionality is the same like the integrated CSTA.

4. How to check the version info?

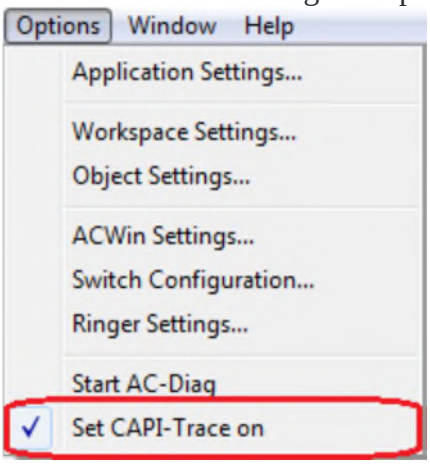
Click on the Version menu:



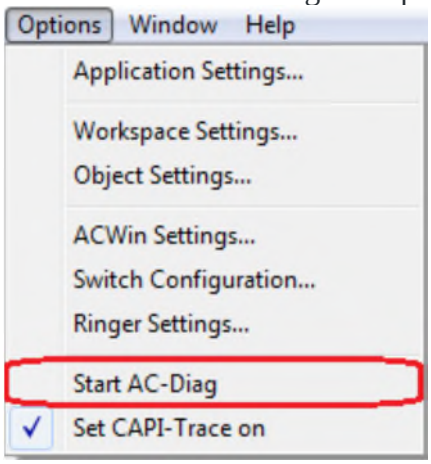
2.3.4. AC-WIN

2.3.4.1. Turning logs on

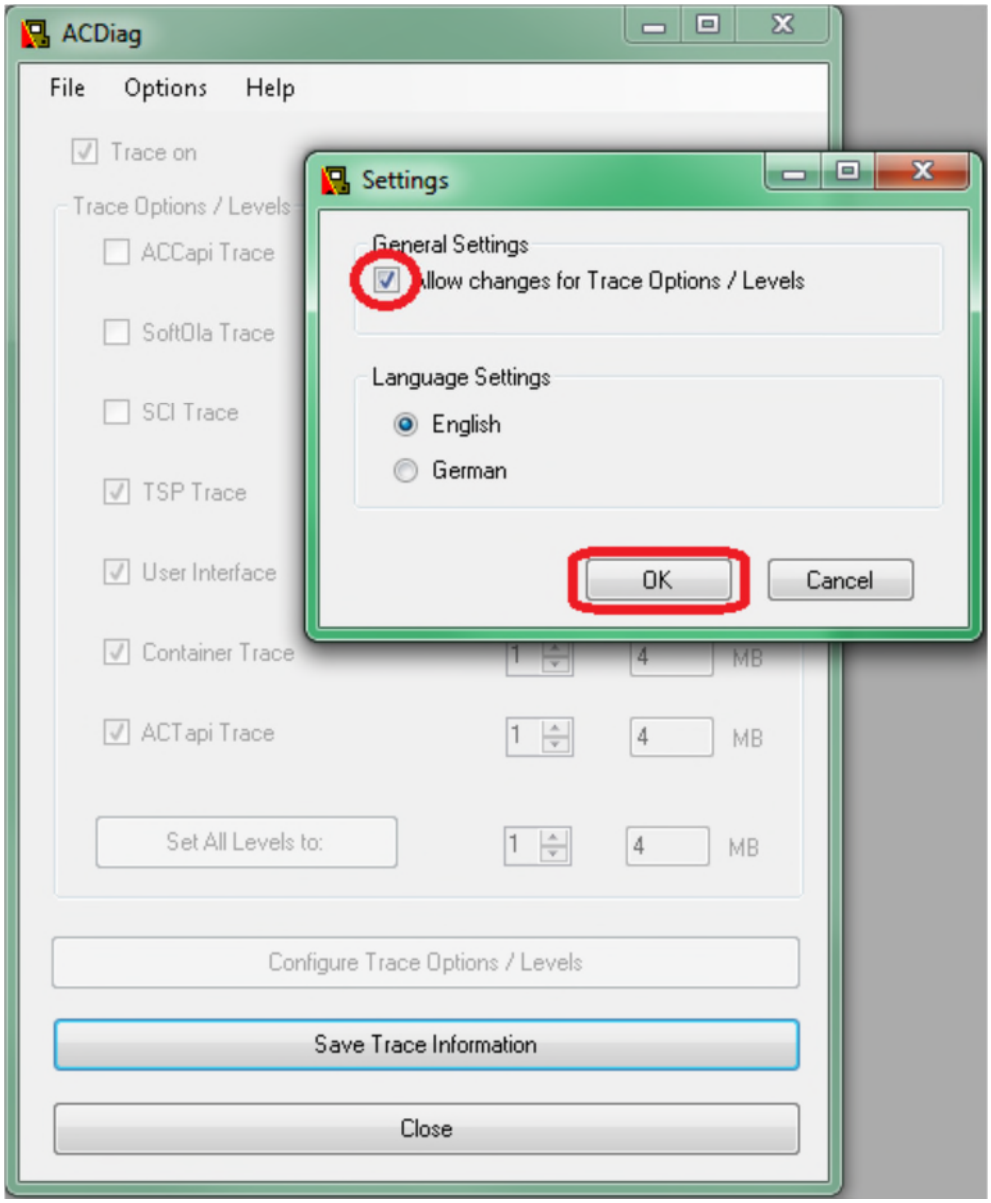
- ACCapi trace:
  - In AC-Win IP window go to Options and select Set CAP-Trace on.

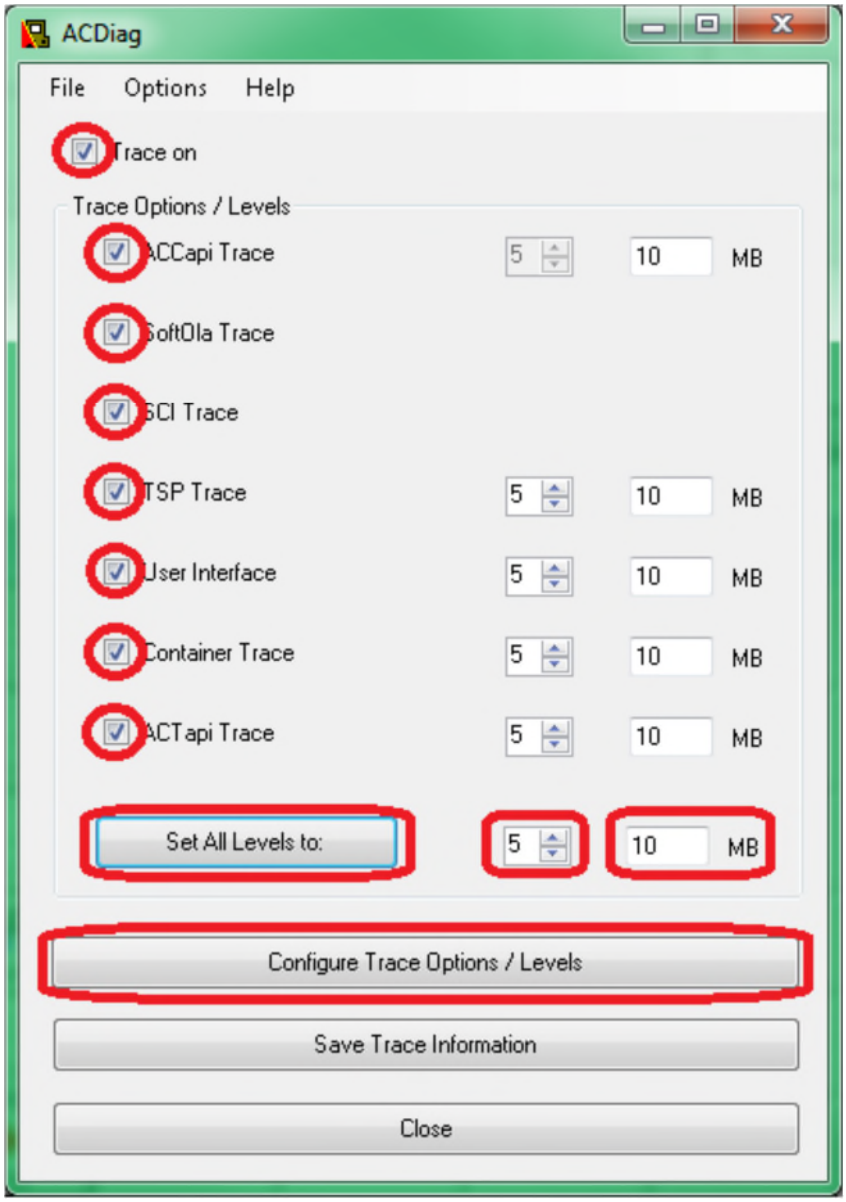


- ACDiag.exe:
  1. In AC-Win IP window go to Options and select Start AC-Diag.

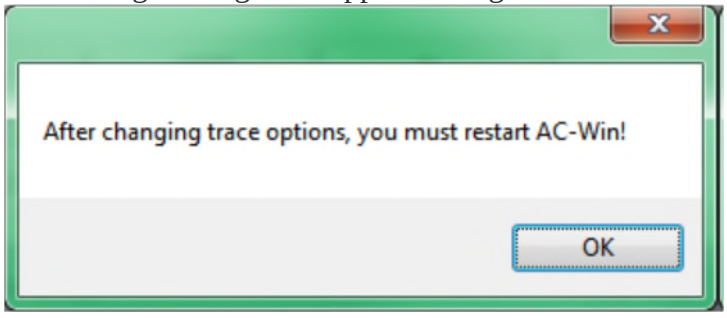


  2. The ACDiag window will open.
  3. Go to Options / Settings and check the box for Allow changes for Trace Options / Level.


ACDiag
File
Options
Help
Trace on
Trace Options / Levels
ACCapi Trace
SoftOla Trace
SCI Trace
TSP Trace
User Interface
Container Trace
ACTapi Trace
Set All Levels to:
MB
Configure Trace Options / Levels
Save Trace Information
Close
Settings
General Settings
Allow changes for Trace Options / Levels
Language Settings
English
German
OK
Cancel

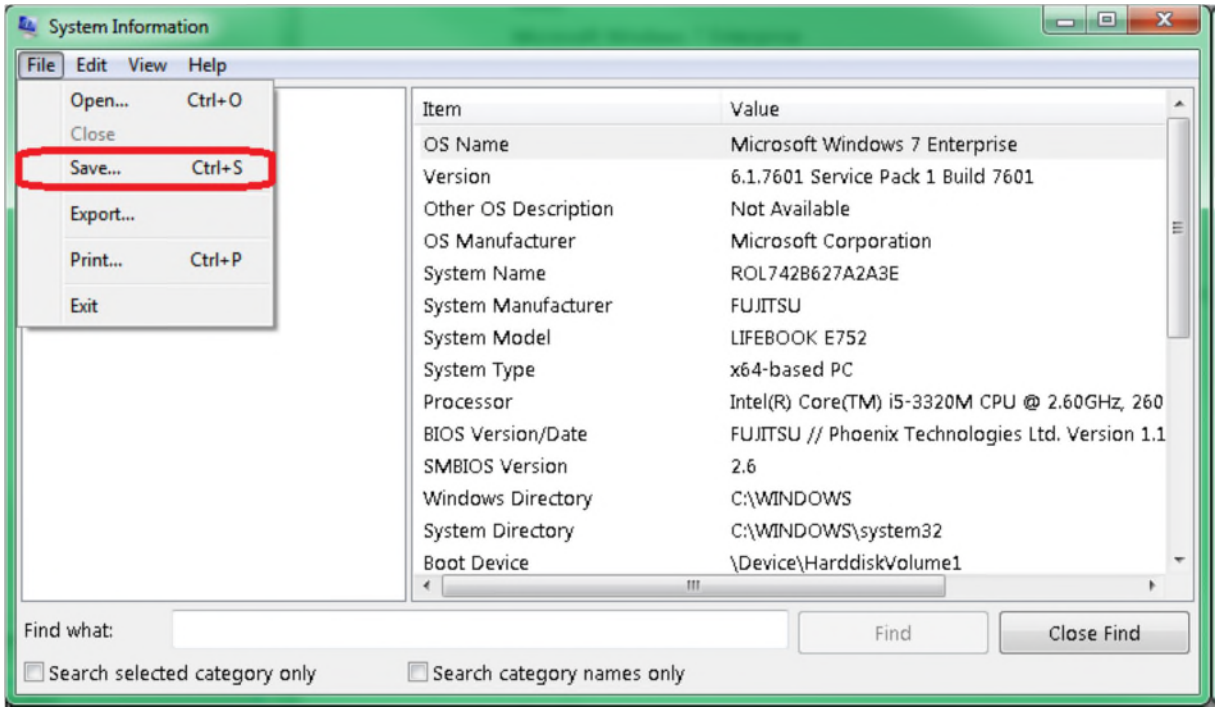


4. Press OK
5. Select all checkboxes and Set All Levels to 5 with 10 MB file size (as in the picture above).
6. Press Configure Trace Options / Levels. This will save the settings.
7. An alerting message will appear telling that AC-Win must be restarted.

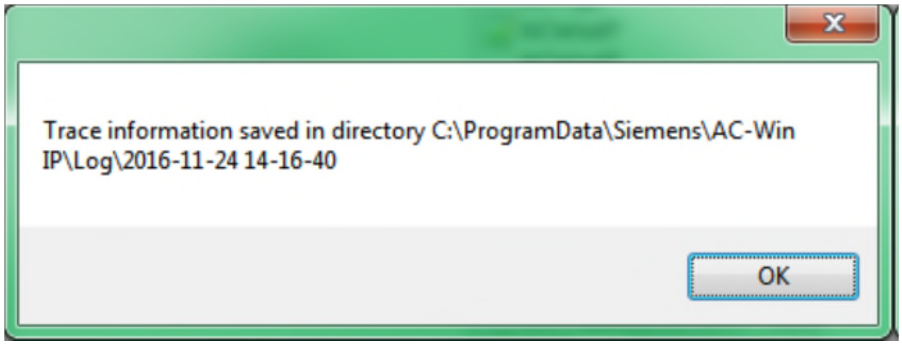


8. Press OK

9. Click on Save trace Information, System Information window will pop-up. Save this as an .nfo file.



10. A message window will tell you that all the Trace information was saved into a folder named to the current date.

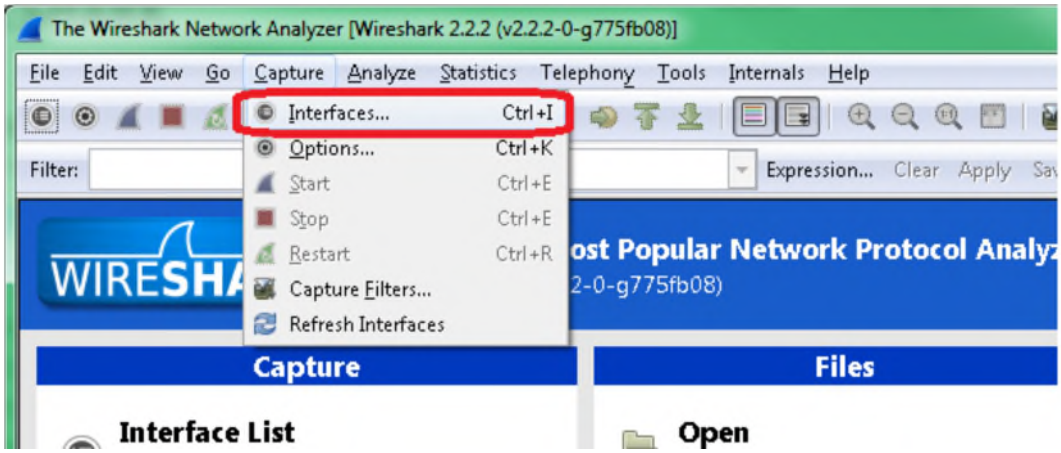


11. Close all AC-Win windows and restart AC-Win application.

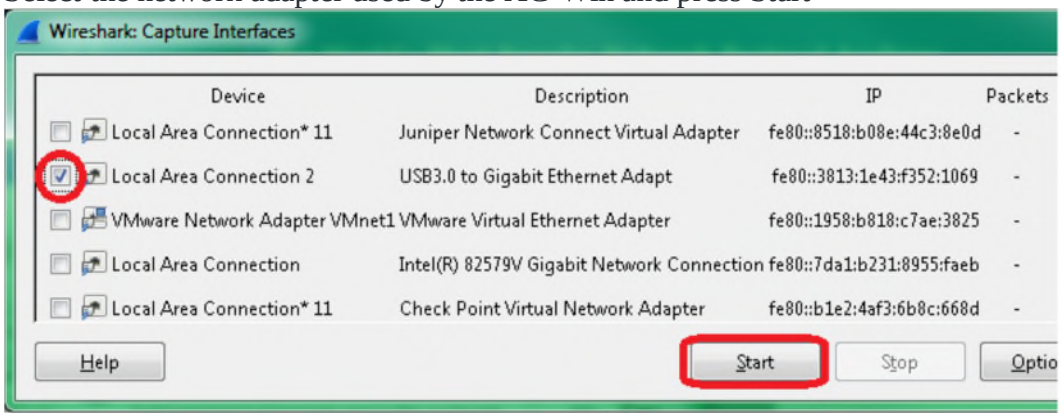
- WireShark-Trace

Please note the IP of the source and target device.

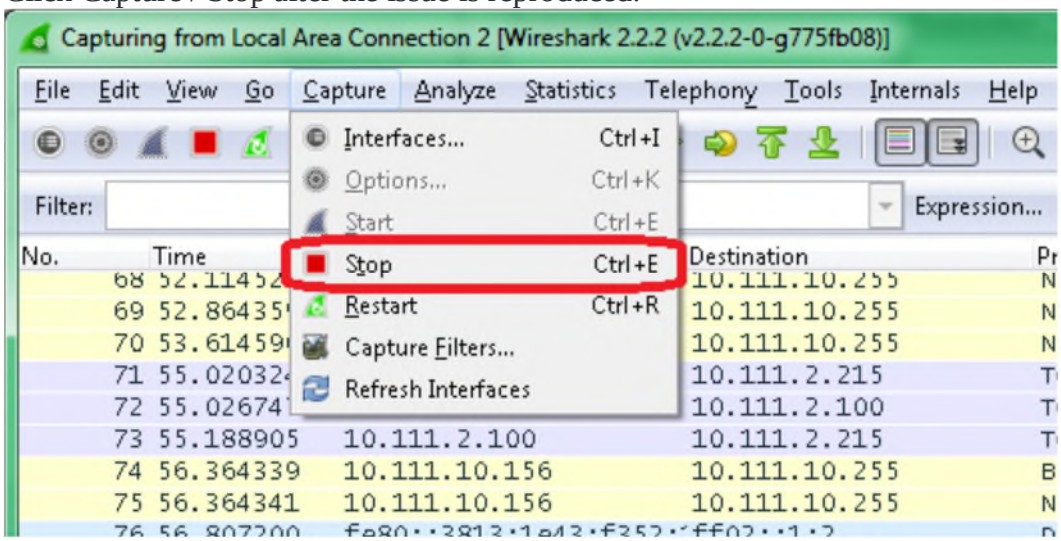
1. Run Wireshark;
2. Click Capture -> Interfaces... and click the Start button corresponding to the network adapter you are using for your network connection:



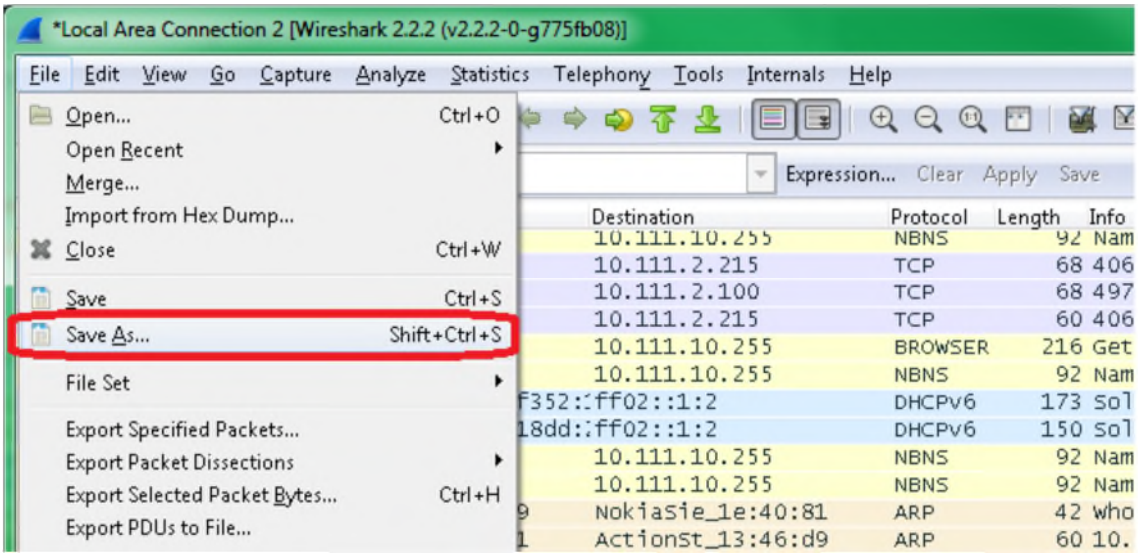
3. Select the network adapter used by the AC-Win and press Start



4. Reproduce the issue without closing the Wireshark application:
5. Click Capture / Stop after the issue is reproduced:



6. Save the captured data by clicking File -> Save as:



- Headset

  Which headset are you using?

2.3.4.2. Collecting logs

- Make a docx or pdf file with a detailed error description.
- Do screenshots as many you can to describe the issue.
- Specify the time when the error occurred.

In Windows 7, 8 and 10, the logs are located in a hidden directory:

C:\ProgramData\Siemens\AC-Win IP\Log

Or in “Users” directory:

C:\Users\All Users\Siemens\AC-Win IP\Log

It is recommended to stop the AC-Win application and delete the log files before reproducing the issue.

ZIP these files together with the Wireshark trace and send it to us.

In the zip file should be included:

- ACCapi_DDMMYYYY_HHMMSS.log
- ACContIP.log
- ACTapi.log
- ACWinIP.log
- EventLog.txt
- InstalledProducts.txt
- SCITraceYYYYMMDDHHMMSS.log
- SiemensAll.reg
- SoftOlaYYYYMMDDHHMMSS.TRC

- if the application is crashing and you can't find this trace, then it probably will be in C:\temp

- Up0e.log

- Whireshark-trace.pcap

- Scenario.docx or Scenario.pdf

2.3.4.3. AC-Win doesn't start (licensing problem and others)

Start ACDiag.exe manually

If application cannot start, then run ACDiag.exe manually from AC-Win installation directory and do the settings like de-scribed in the **Turning logs on** section

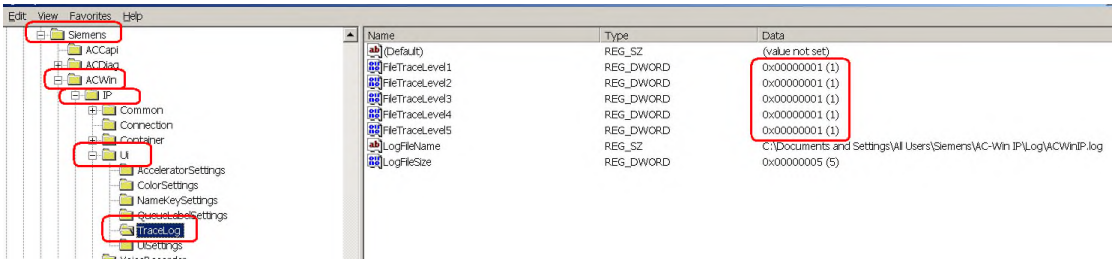
Set logs manually

If ACDiag.exe cannot be started, then you can set the logs manually in the registry.

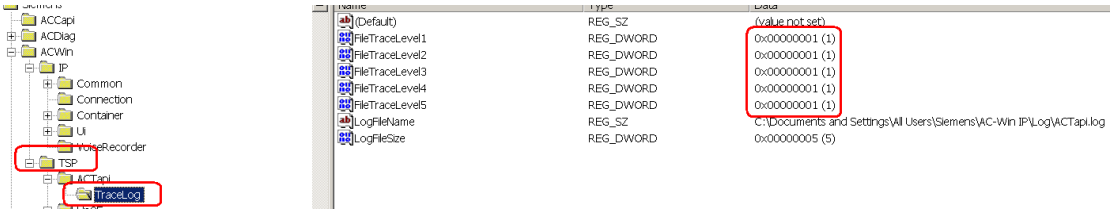
Type **regedit** in the windows **Start** menu, then navigate to the following paths and do the settings:

Go to HKEY_LOCAL_MACHINE \ SOFTWARE (\ Wow6432Node) \ Siemens:

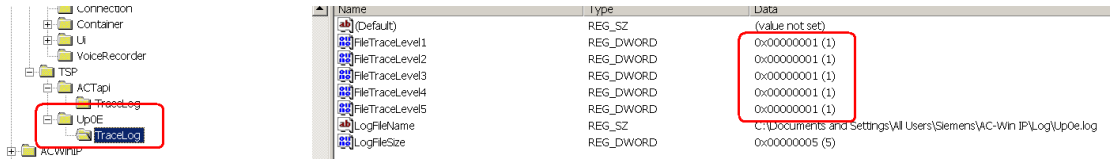
- for UI trace



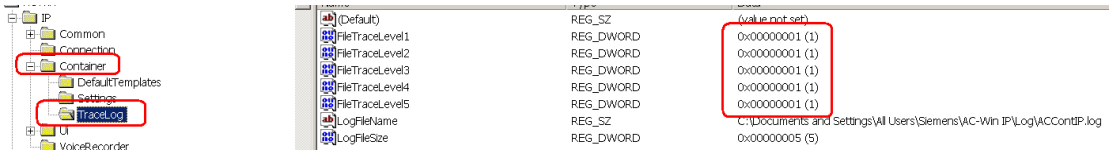
- for TSP trace



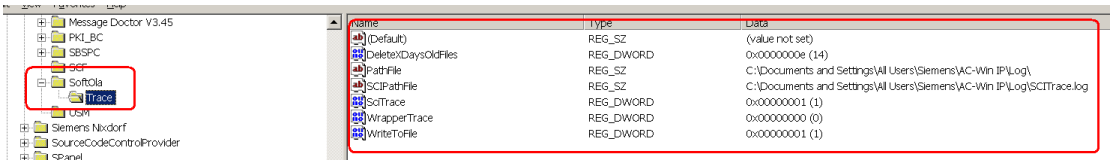
- for Up0E



- for Container



- for SoftOla



2.3.5. DS-Win

2.3.5.1. Collecting logs

- Make a docx or pdf file with a detailed error description.
- Do screenshots as many you can to describe the issue.
- Specify the time when the error occurred.

In Windows 7, 8 and 10, the logs are located in a hidden directory:

C:\ProgramData\Siemens\DS-Win V4\Log

Or in “Users” directory:

C:\Users\All Users\Siemens\ DS-Win V4\Log

It is recommended to stop the DS-Win application and delete the log files before reproducing the issue.

ZIP these files and send it to us.

In the zip file should be included:

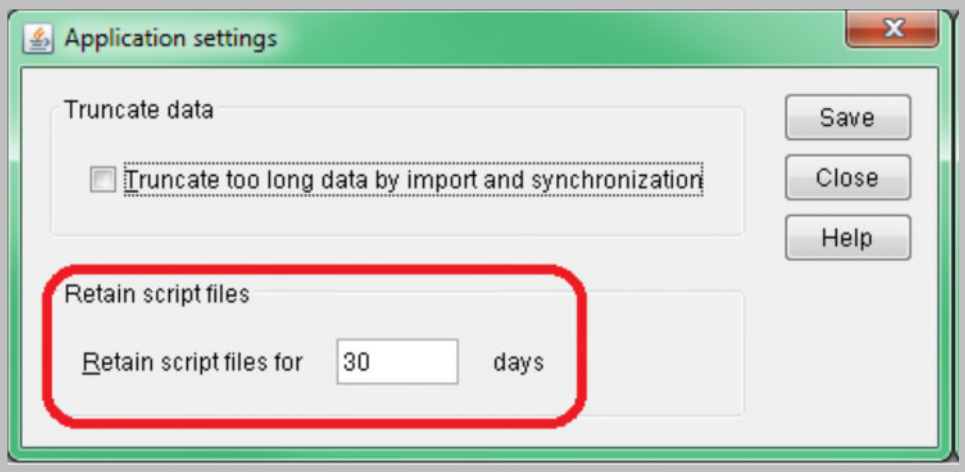
- admin.log
- Designer.log
- DSWW4.log
- hibernate.log
- iReport.log
- mcsync.log
- migration.log
- Scenario.docx or Scenario.pdf

2.3.5.2. Problems

- If your problem is related to **Database Migration** we will need the DS-Win V4 database and

all the scripts from the database installation directory (example for PostgreSQL: C:\PSQL\9.5\scripts).

Important! – *If the folder is empty then make sure that in DS-Win Admin the "retain script files" parameter is set with a proper value (Options->Application Settings).*



- If your problem is related to **Database Import** we will need the data file you used for import (**txt** or **csv**) and a short description of the import specification. If you modified the standard database, we will also need the modified version.

- If your problem is related to **Synchronization** we will need the following files:

  - *DSWin2.rsp and DSWin2_I.dat* (The path for these files can be defined in the synchronization specifica-tion, but the default folder is *C:\ProgramData\Siemens\DS-Win V4*)

- If you are not using the standard **GUI** and your problem is related to this, we will need your GUI.**xml** file from *C:\ProgramData\Siemens\DS-Win V4\Data\Forms* folder and the DataSources.xml and DbTables.xml files from *C:\ProgramData\Siemens\DS-Win V4\Data\DBDesc* folder. Also we will need *C:\Program Files (x86)\Siemens\DS-Win V4\Config\Win_View_config.xml*

- In case of **printing** problems we will need the template files from C:\ProgramData\Siemens\DS-Win V4\Templates.

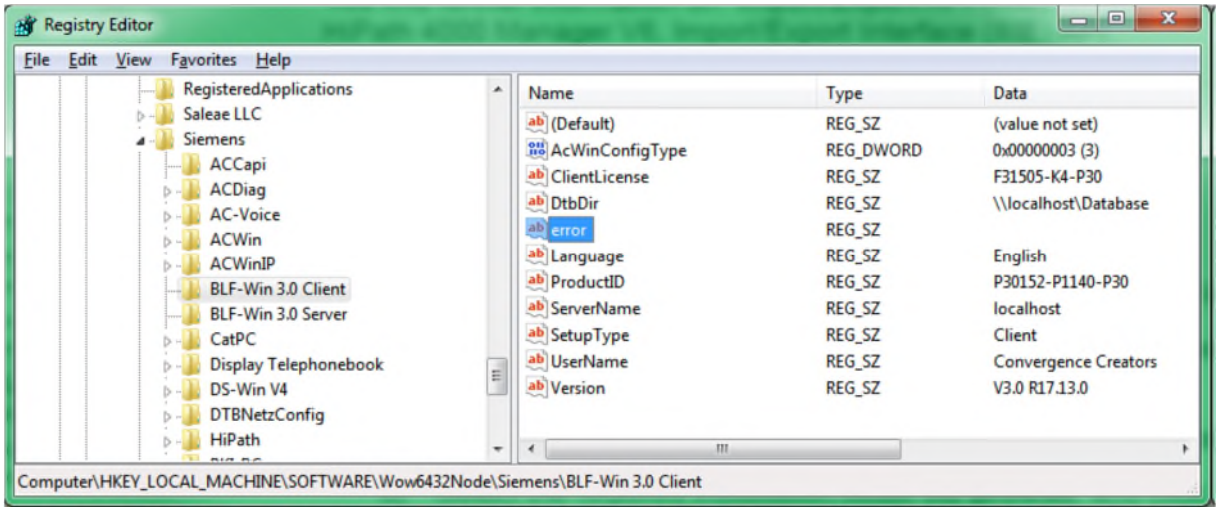
2.3.6. BLF-WIN

2.3.6.1. Turning Blf Logging On

1. Type **regedit** in the windows **Start** menu, then navigate to the following paths and do the settings:

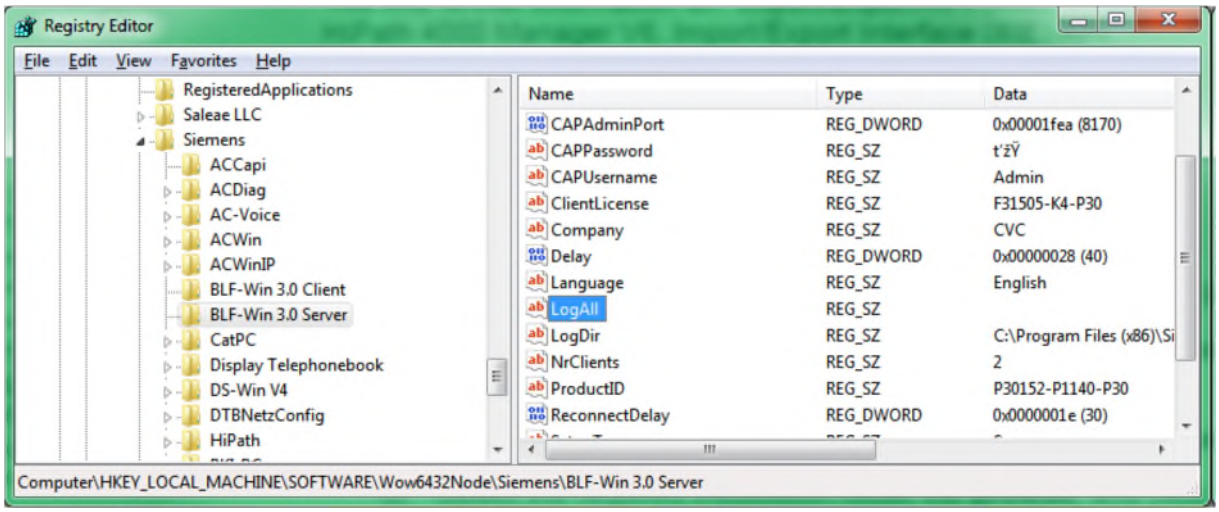
2. Go to HKEY_LOCAL_MACHINE \ SOFTWARE (\ Wow6432Node) \ Siemens \ BLF-Win 3.0 Client

3. Create a 'New String Value' with name **error** with no value.



4. Go to HKEY_LOCAL_MACHINE \ SOFTWARE (\ Wow6432Node) \ Siemens \ BLF-Win 3.0 Server

5. Create a 'New String Value' with name **LogAll** with no value.



2.3.6.2. Turning Cap Logging On

1. On the PC where the CAP is installed, go to the installation directory (default: *C:\Program Files (x86)\Unify\OpenScapeCTI*) and then edit the \config\common\global.cfg file.

log.level = 5
log.maxLines = 100000
log.maxFiles = 10

2. Go to \config\<PC name>\CA4000_<SCC_name> folder and edit the CA4000.cfg file.

enter **log.level=5**

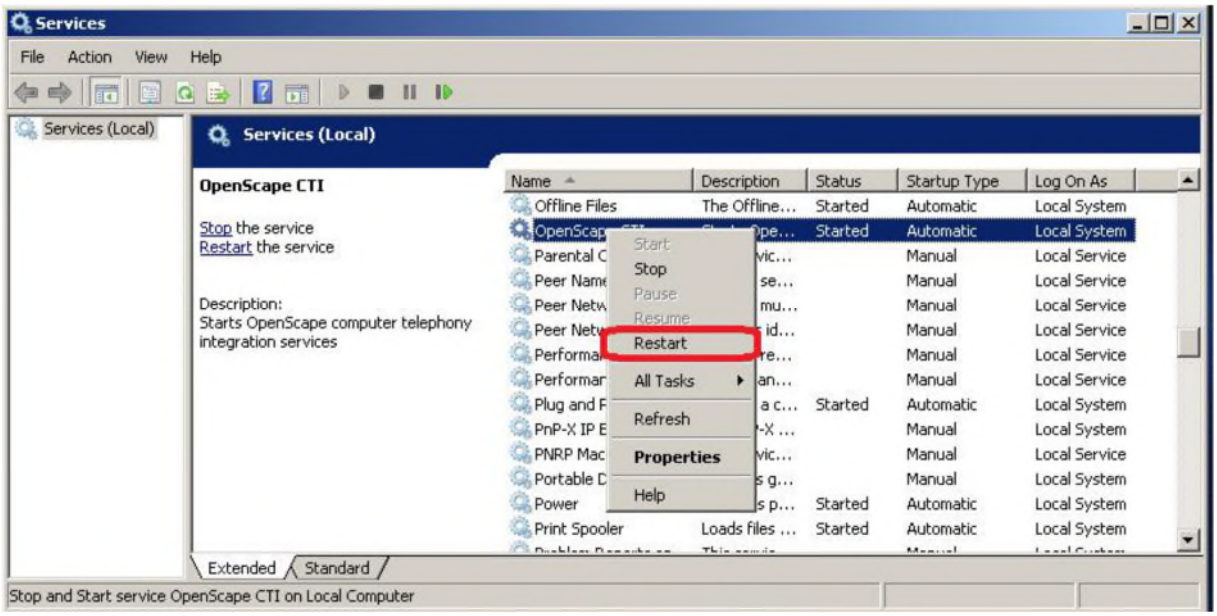
3. Go to \config\<PC name>\telasServer_<SCC_name> folder and edit the Telas.cfg file.

log.level=5
cstaLogEnabled=1
debugLevel=9

4. Go to \config\<PC name>\sccp_<SCCP_name> folder and edit the Telas.cfg file.

log.level=5
cstaLogEnabled=1
debugLevel=9

5. Restart CAP service:



2.3.6.3. Collecting BLF logs

- Make a **docx** or **pdf** file with a detailed error description.
- Do screenshots as many you can to describe the issue.
- Specify the time when the error occurred.

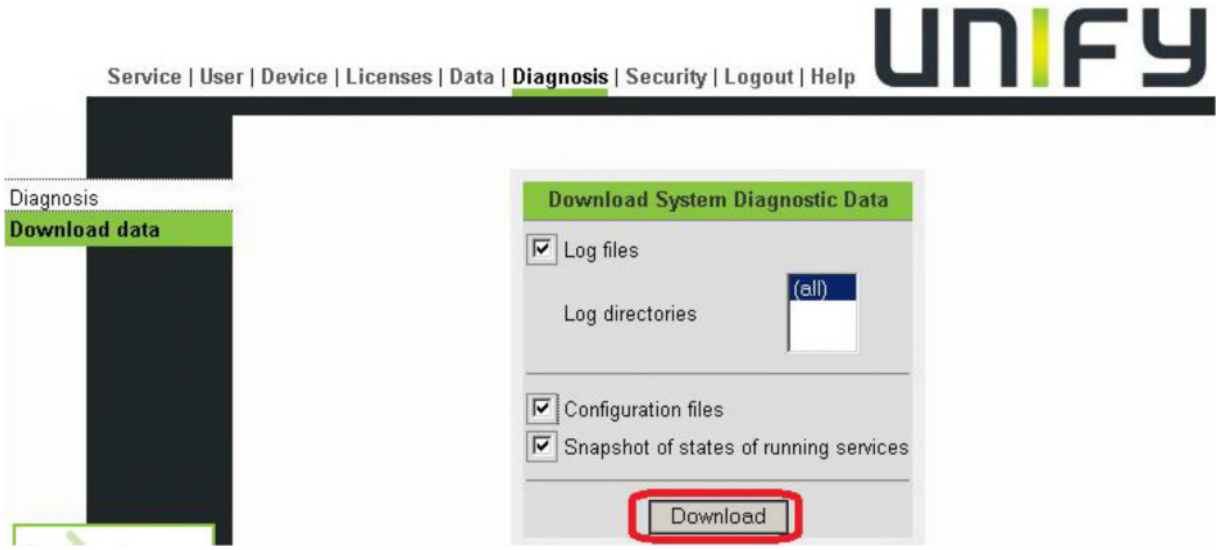
In Windows 7, 8 and 10, the logs are located in the following directories:

C:\Program Files (x86)\Siemens\Blf-Win 3.0\Client
C:\Program Files (x86)\Siemens\Blf-Win 3.0\Server\Logs

It is recommended to stop the BLF application and delete the log files before reproducing the issue.

2.3.6.4. Collecting CAP logs

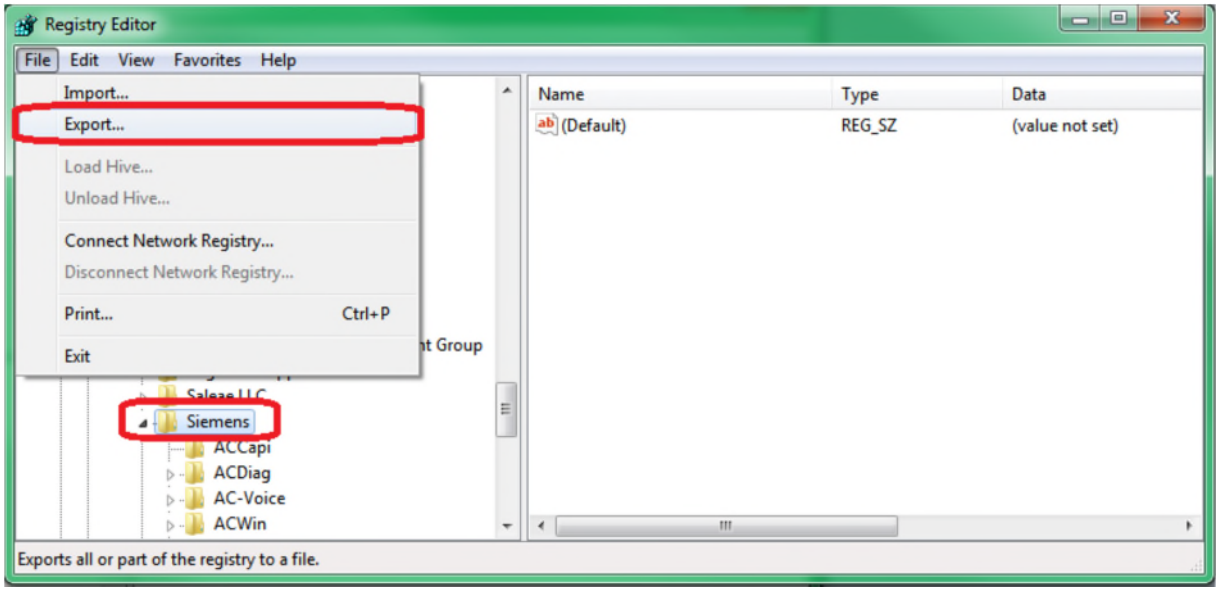
1. Open CAP Management interface and go to the “Diagnosis” tab.
2. Select all checkboxes and click Download, then save the sysdiag.zip.



2.3.6.5. Archiving the logs

Further information is necessary about the System where the BLF is running.

1. Export the registry keys from **regedit.exe** from the windows **Start** menu by selecting the Siemens Key from the hierarchy and then File / Export. Export as <PC name>_reg.reg.



2. Make a regen of the PBXes used with BLF. This will result a regen.samtxt file.
3. Export a list of patches with AMO Command: DISP-PATCH:grp,*; in a file named “patches.txt”

ZIP the BLF and CAP log files together and send it to us.

In the zip file should be included:

- Error.log, Update.log, System.log (from BLF Server)
- YYYY.Month.DD.HH.MM.SS.log (from BLF Client)
- Sysdiag.zip (from CAP)
- <PC name>_reg.reg (from registry)
- regen.samtxt
- Patches.txt
- Scenario.docx or Scenario.pdf

NOTE: *If there are more then one clients please send "<date_time_Stamp>.log" foreach client that you want to take in consideration when analyzing logs.*

Extra Info: *After you send the logs to us, it is a good idea to stop the logging for CAP and BLF (by deleting the logs you send to us from your computer, deleting the registry Error and LogAll that you added with regedit and write in CAP config-uration files the default values).*

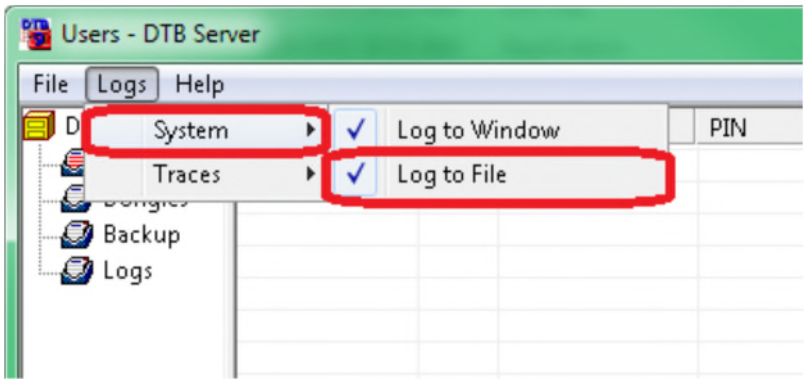
2.3.7. DTB for Windows

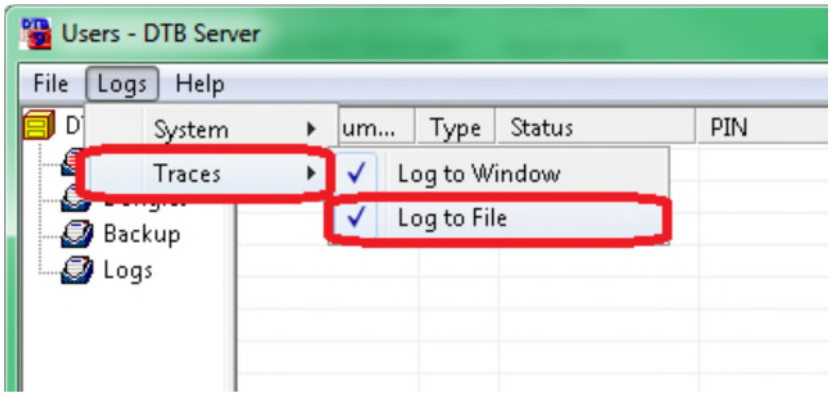
2.3.7.1. Turning logs on

1. Stop DTB Master then edit C:\DTB\DTBNetzConfig\dtbmaster.ini

   logfile=on

2. In DTB Server **Logs / System / Log to File** and **Logs / Traces / Log to File**





2.3.7.2. Obtaining CAP logs

1. On the PC where the CAP is installed, go to the installation directory (default: *C:\Program Files (x86)\Unify\OpenScapeCTI*) and then edit the \config\common\global.cfg file.

    log.level = 5
    log.maxLines = 100000
    log.maxFiles = 10

2. Go to \config\<PC name>\CA4000_<SCC_name> folder and edit the CA4000.cfg file.

    enter **log.level=5**

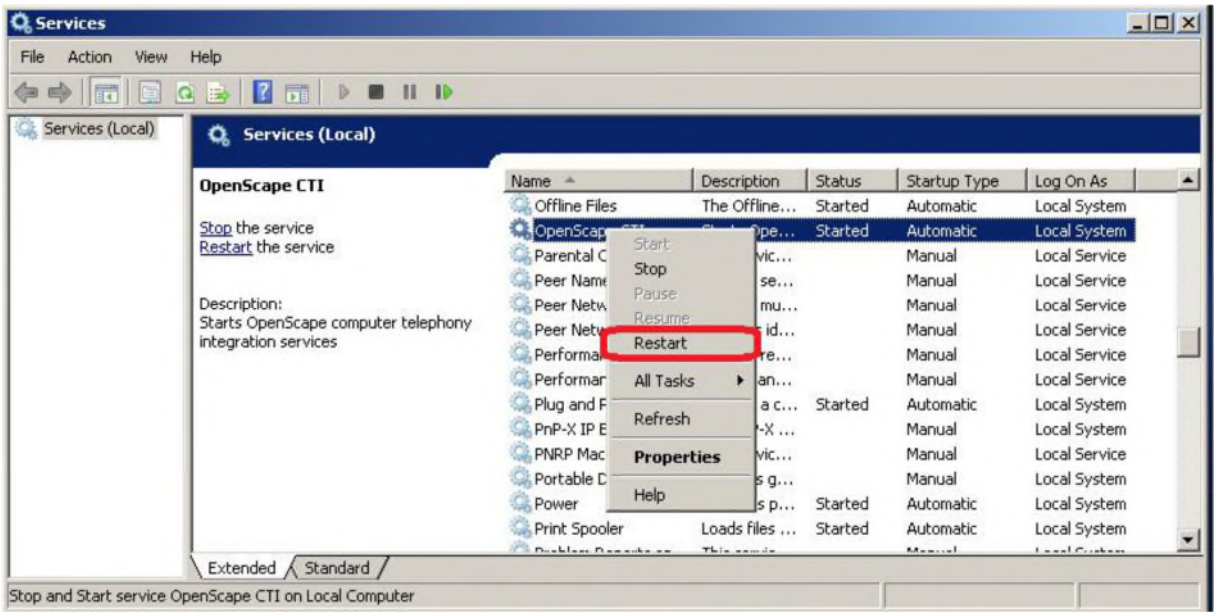
3. Go to \config\<PC name>\telasServer_<SCC_name> folder and edit the Telas.cfg file.

    log.level=5
    cstaLogEnabled=1
    debugLevel=9

4. Go to \config\<PC name>\sccp_<SCCP_name> folder and edit the Telas.cfg file.

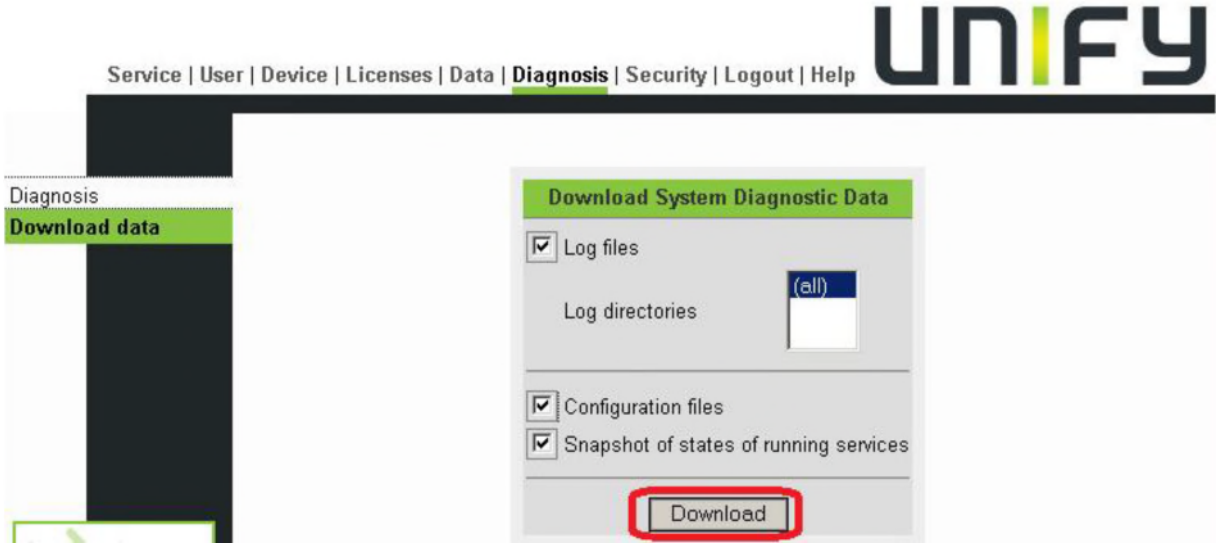
    log.level=5
    cstaLogEnabled=1
    debugLevel=9

5. Restart CAP service:



6. Open CAP Management interface and go to the “Diagnosis” tab.

7. Select all checkboxes and click Download, then save the sysdiag.zip.



2.3.7.3. Collecting logs

- Make a **docx** or **pdf** file with a detailed error description.
- Do screenshots as many you can to describe the issue.
- Specify the time when the error occurred.

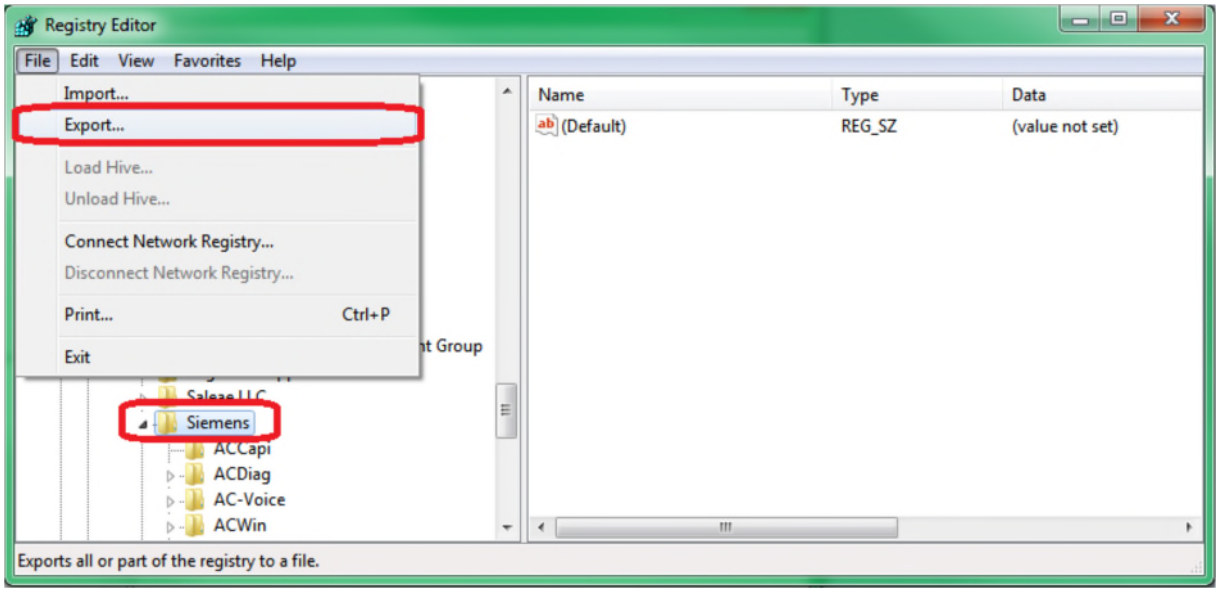
In Windows 7, 8 and 10, the DTB logs are located in the following directories:

C:\DTB\Display Telephonebook\DTBServerLog.txt
C:\DTB\DTBNetzConfig\DTB.log

It is recommended to stop the DTB application and delete the log files before reproducing the issue.

Further information is necessary about the System where the DTB is running.

- Export the registry keys from **regedit.exe** from the windows **Start** menu by selecting the Siemens Key from the hierarchy and then File / Export. Export as <PC name>_reg.reg.



ZIP these files and send it to us.

In the zip file should be included:

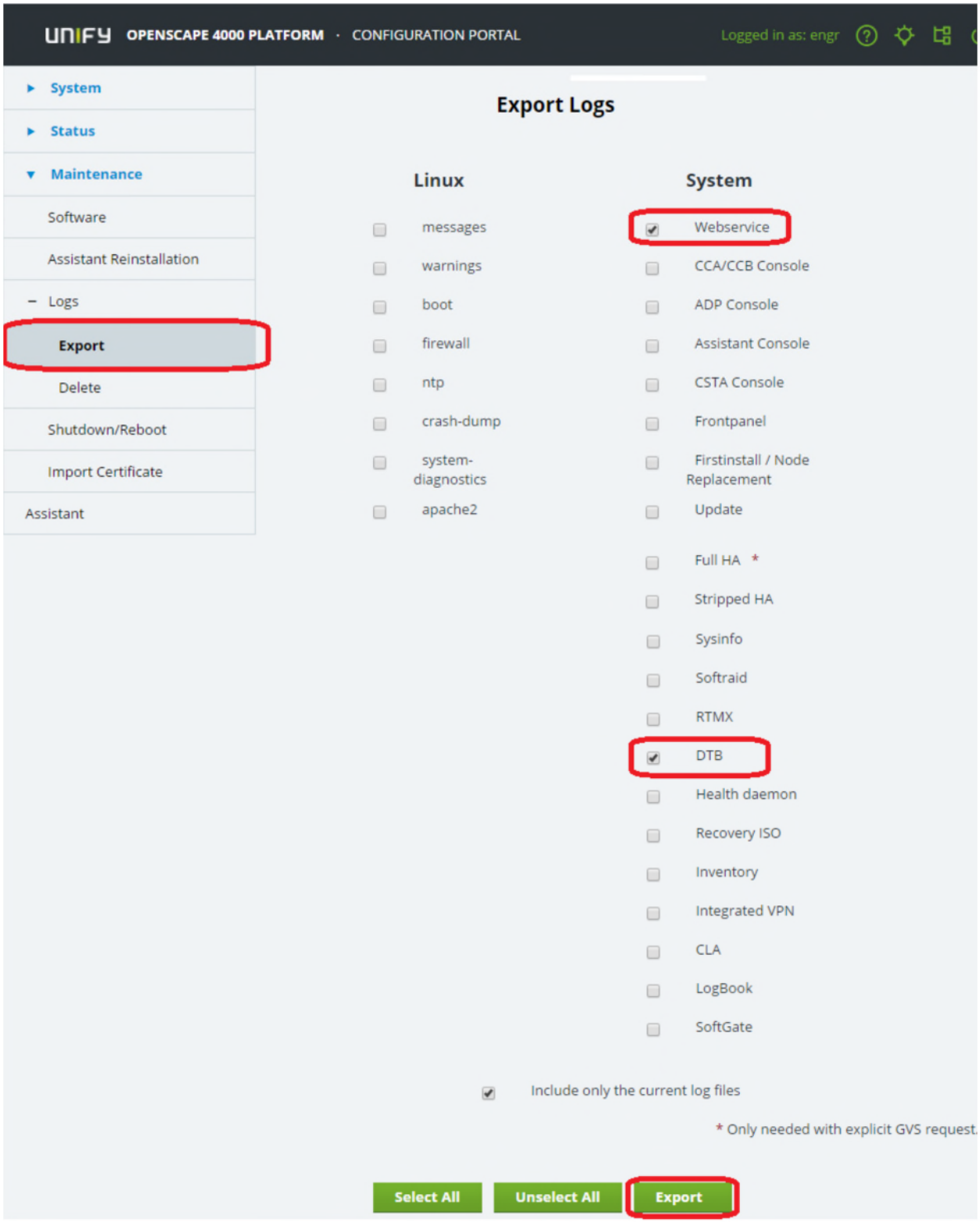
- all files from C:\DTB\Display Telephonebook
- all files from C:\DTB\DTBNetzConfig
- Sysdiag.zip (from CAP)
- <PC name>_reg.reg (from registry)
- Scenario.docx or Scenario.pdf

2.3.8. Integrated DTB

2.3.8.1. Collecting logs

- Make a **docx** or **pdf** file with a detailed error description.
- Do screenshots as many you can to describe the issue.
- Specify the time when the error occurred.

On the OS4k portal go to **Maintanance / Logs / Export**, make sure that the *DTB* and *Webservice* checkbox is selected, then press Export:



ZIP these files and send it to us.

In the zip file should be included:

- <hostname>-logs-current-<Portal IP address>-YYYY.MM.DD.zip (log files)
- Scenario.docx or Scenario.pdf

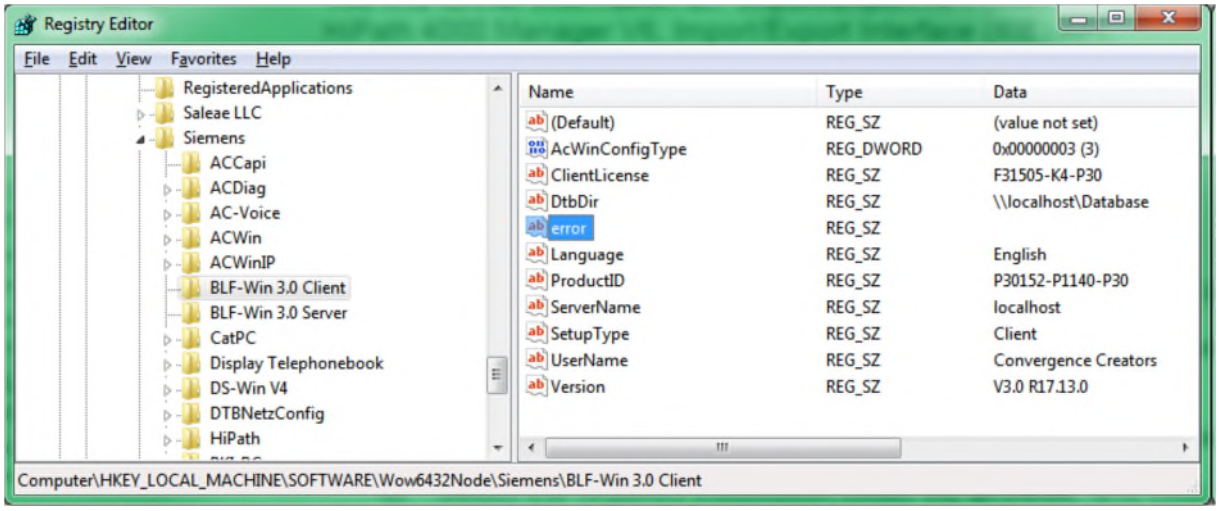
2.3.9. Integrated BLF

2.3.9.1. Turning BLF Client logs on

1. Type **regedit** in the windows **Start** menu, then navigate to the following paths and do the settings:

2. Go to HKEY_LOCAL_MACHINE \ SOFTWARE (\ Wow6432Node) \ Siemens \ BLF-Win 3.0 Client

3. Create a 'New String Value' with name **error** with no value.



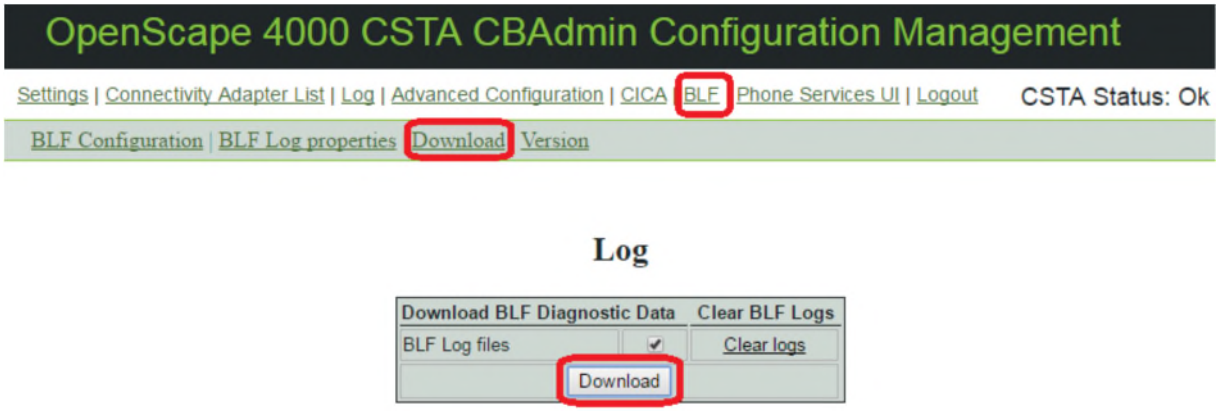
In Windows 7, 8 and 10, the logs are located in the following directory:

C:\Program Files (x86)\Siemens\Blf-Win 3.0\Client

It is recommended to stop the BLF application and delete the log files before reproducing the issue.

2.3.9.2. Collecting BLF Server logs

On the OS4k CSTA go to **BLF / Downloads**, make sure that the *BLF Log files* checkbox is selected, then press Down-load:



- Make a **docx** or **pdf** file with a detailed error description.
- Do screenshots as many you can to describe the issue.

- Specify the time when the error occurred.

ZIP these files and send it to us.

In the zip file should be included:

- BLFSysdiag-<Portal IP address>-YYYY.MM.DD-HHMMSS.zip (log files from BLF Server)

- YYYY.Month.DD.HH.MM.SS.log (from BLF Client)

- Scenario.docx or Scenario.pdf

2.3.10. OpenScape Voice Server Problems

- General problems:
- All Incidents regarding OSV problems should have RTT traces from the Trace Manager if available with 24_7 enabled.
- For Pstacks you should collect following:
  - RtpDumpLog
  - Files in /software/rtpcore
- Problems in conjunction with OSCC connectivity:
  - RTT trace capturing SIP, UCE and CSTA facilities
- OSV Alarms:
  - If alarm occurs and an analysis is needed, please take the following trace out of business hours:
  - *As user root, run:*
    # /unisphere/srx3000/srx/bin/RapidStat –c –b (both nodes, out of business hours)
  - *Provide the file generated in /log*
  - *Provide screenshot of the alarm*

How to Activate RTT on an OSV if no Tracemanager is Available

It is possible to activate RTT to local hard disk (HDD) of the OSV. As the /software volume normally has many GB of free memory available it is even possible to have traces for the last 10 - 20 hours available (depending on the traffic and active trace flags).

1. Check if the RTT is currently not running:
   - startCli (6 -1 - (7)6 - 2 - 5)
   - check if there are new files created under /software/RTT/:
     `ls -ltrh /software/RTT/HipathContTrace*`
2. Delete old trace files from /software/RTT/:
   `rm /software/RTT/HipathContTrace*`
3. Check how many disk space is available in /software/:
   `df -h`
   example: 174G 8.2G 157G 5% /software
4. Check the follwoing RTP parameters via startCli:
   - Srx/PrttReader/ContTraceFileSize (default 20971520 - ~20 MB each uncompressed RTT file)

- Srx/PrttReader/ContTraceNumberFiles (default 500 - Can be set to 1000 if enough space is available on the hard disk.)
- Srx/PrttReader/ContTraceCompressFiles (default 1 - if set to 1 the RTT files are compressed (gzip) wich is very effective and reduces the size with approx factor 0.1 (20MB -> 2 MB))
- Srx/PrttReader/ContTraceDirectory (default /software/RTT - There is now reason to change this, as /software has many space assigned and the folder monitored by the system. If the folder is getting to big, alarms are reported.)

5. start the continuous tracing via startCli:

```
Application-level Management..................6
     Softswitch Management.........................1
     (OSV <= V6:  Trace Management.............................7)
     OSV >= V7:  Trace Management..............................6
     Continuous Trace Management...................2
     Continuous Trace Management (methods):
               Activate Continuous Tracing...................1
               Deactivate Continuous Tracing.................2
               Start Continuous Trace File Export............3
               Stop Continuous Trace File Export.............4
               Display Continuous Trace Data.................5
               Return..............................99
               Selection (default: 5): 1
               Enter Filter Name <To display all valid Filter Names enter '?' (max
length: 31)>: ?
               --- All Filter Names ---
                    24_7_extern
                    24_7
                    24_7_min
               Enter Filter Name <To display all valid Filter Names enter '?' (max
length: 31)>: 24_7
               Enter Trace Duration <min: 0 max: 1440> (default: 0): 0
               Select Node <0=both,1=Node1,2=Node2 (min: 0 max: 2)> (default: 0): 0

               Do you want to execute this action? <y/n> (default: yes):
     Continuous Trace with filter name 24_7 was activated successfully on node 1.
     Continuous Trace with filter name 24_7 was activated successfully on node 2.
```

Deactivate the continuous tracing:

1. Stop it via startCli (6 -1 - (7)6 - 2 - 4)
2. Delete the files from /software/RTT:

```
rm /software/RTT/HipathContTrace*
```

2.3.11. Gateway Issues Connected to OSV

For any gateway issue please collect in parallel OSV RTT traces as described in section 2.3.10 OpenScape Voice Server Problems and also from the respective gateway:

- Mediatrix gateway problems:
  - Syslog from the Mediatrix with following facilities set on DEBUG level.
    - Call Routing (CROUT)

- Integrated Services Digital Network (ISDN)
- SIP Endpoint (SipEp)

- RG8700 problems:
  - Start the RTT tool for the RG8700 and select SIP, Q.931 and CATs (20,173,181,182).
  - Provide the created .cap file and caton file.
  - Start rapidstat (and provide /logfiles) if possible
  - Log files of the rg Under the dir. /ad0/data/logfiles
  - Log files from RG directory under /ad0/data/debug

  - For scenarios with PRI failure
    - Output of the command show /pri/<pri name >
      Output of the command show /pri/<pri name > counter
      Output of the command show /pri/<pri name > channel

  - For scenarios with RG rebooting
    - Log file from RTTC tool enabled the caton traces 20 173 181 182

- RG8300 (HP4K) problems: see related details in section OpenScape 4000 2.2

2.3.12. OpenScape Branch Issues

For issues related to OpenScape Branch please provide the following according to scenario:

- Network trace (ethereal)
- Logs (Sip Server, B2BUA and ISDN {if applicable})
  - Activate the corresponding logging configuration after consulting your technician or contact person of Unify. Depending on your scenario different loggings are necessary;
  - Use INFO level; activate DEBUG level only if asked by GVS;
  - Ensure that Log settings are reverted to default after the execution of the scenario.
- Rapidstat Level 5 (Collect **after** doing the call scenario and out on low traffic hours)

If an OSV is part of the scenario you also need to provide traces as described in point **OpenScape Voice Server Problems**

2.3.13. OpenScape SBC issues

For issues related to OpenScape SBC please provide the following according to scenario:

- Network trace (ethereal)
- Please see the logging section from OpenScape Branch Issues mentioned above.
  Logs (Sip Server, B2BUA, RtpProxy {for RTP issues} and SSM {if applicable}) in Debug, IN LOW TRAFFIC HOURS
  Ensure that Log settings are reverted to default after the execution of the scenario.
- Rapidstat Level 5 (Collect **after** doing the call scenario and out on low traffic hours)
- If the issue is related with OpenScape SBC Licenses and Centralised Licensing Model is used then symphonia logs are needed (with OpenScape Branch Assistant for V6,

V7R1 or with OpenScape SBC Assistant for V7R2 and upwards, in debug log level)

If an OSV is also part of the scenario you need to provide also traces as described in point **OpenScape Voice Server Problems**

2.3.14. Common Management Portal (former OpenScape Voice Assistant) Issues

For issues with Voice Assistant you need to be aware when making changes that the OSV is also involved.

- Enable SOAP RTT traces on OSV
- Run “tcpdump -w osv_cmp.pcap -i any tcp and port 8767 -s 19999” on UC backend, and reproduce the scenario
- Then collect output file (osv_cmp.pcap),and files symphonia.log, tomcat.log, usage.log, usage_tomcat.log from log folder of UC Backend server
- Collect also RTT traces from trace manager and deactivate SOAP traces.

2.3.15. DLS Issues

- Used DLS SW version and variant (DLS-Standalone – Linux/Windows, DLS-TAP or DLSOpenScape-onboard). Include your DLS node configuration along with DB configuration (for MultiNode).
- Which function was used / has been called
- Screenshot(s)
- Indicate the time of the actions performed for the various steps (in minutes).
- Activity and Error Log: Enable logging level as appropriate for the problem and generate protocol data for the timeframe where the problem occurred (HTML-page). Activity and Error Log is described in the DLS administrator manual, chapter 6.
- DLS Trace: send trace files as generated with Trace Mode and Level that fits best to the problem. See chapter 6.5.1 for more information on DLS Trace.
- File wrapper.log from <install path>\Tomcat5\logs where on OnBoard DLS, those messages are logged in the tomcat_stdout.log file.

2.3.16. OpenScape UC Issues

- For Basic issues please provide following:
  - Symphonia.log from the time of the scenario and collect.sh (low traffic hours) should be always provided. (If you need support on collect.sh settings please get in touch with Unify)

- Additional traces according to scenario:
  - For call scenarios (failed call, wrong display wrong call behavior), please provide RTT trace from OpenScape Voice on the facilities SIP,UCE,CSTA.

- UC Platform issues (crashes, restarts etc..), provide collect.sh from all UC servers of the deployment starting at least 1 day before the crash took place including any heapdump under "/var/siemens/common/log/dumps/".
- Desktop Client issue – tracemonitor log from the client. To create it run BSTrcMon.exe, situated in C:\Program Files\Enterprise\OpenScape Desktop Client\Tracemonitor, reproduce the scenario and after right clicking on the BST tool chose where to save the trace file.
- Web Client issues and E/A CockPit issues – add the logs located under /var/siemens/common/log/webclient/.
  - In the web browser, in the dial digits field type :trace=on in order to start traces on the browser side.

- Fusion for Outlook
  - Open OpenScapeClientDiagnosis tool (%INSTALL_FOLDER%/Openscape for Outlook/tools) and enable "Write to file", "MSI Trace" options, and UC extended logging to DEBUG
  - Restart client and reproduce scenario
  - In OpenScapeClientDiagnosis tool, click on "Collect Diagnosis Data" and provide the output file
  - Then restore OpenScapeClientDiagnosis to original settings.

- Desktop Integration Tool
  - Stop DIT.
  - Open file C:\Documents and Settings\<USERNAME>\Application Data\Siemens\OSCwebDI.cfg and add the line "DEBUG=1", when not present.
  - Start DIT again
  - Right click on shortcut icon of DIT and select debug
  - Click in the new opened window the button LOG: DEBUG
  - Close the window
  - Reproduce the problem

2.3.17. Telephone Devices Problems

For initial phone problems analysis you need to provide Diagnostic Data Collector output and traces with following basic activated flags:

- SIP Messages – Debug
- SIP Signalling- Debug
- SIP Call Control – Debug
- CSTA Service – Debug
- Communications – Debug
- Call View - Debug

NOTE: ***If you are not sure about the flags needed for a specific complex issue please call the Expert Assistant Hotline for further support.***

2.3.18. OSMO (OpenScape Mobile) Issues

For OSMO issues OSV traces are needed. You need to ensure that CSTA tracing is enabled!

Also set OSMO client traces (Settings\Advances\Logging) on Max level.

Below you can find the traces needed. If you are not sure about the log4j enablement please call Expert Assistant Hotline for further support.

Scenarios that involve UC features

- *UC server: symphonia logs with log4j_bcom active*
- *For multi-node installations: activate logging in the BE (backend) and FE (frontend) nodes*
- *For scenarios that involve the media server (typical case: conferencing): activate logging in the media server node*
- *Facade server: logs under /usr/local/tomcat6/logs*

If the scenario involves login failures in mixed mode (user has UC and OSMO configured):

- OSV SOAP traces
  Activate SOAP traces with /unisphere/srx3000/srx/rtt_trace_scripts/soapServer_all

2.3.19. CMI (Cordless Multicell Integration) – Diagnostics requirements

Call related problems

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

1. The detailed, actual problem description including the following info:
   1.1. Who has called whom including:
      1.1.1. Phone numbers
      1.1.2. Display Names
      1.1.3. Terminal-types
      1.1.4. Software version of the terminals
      1.1.5. Info about external or internal call (Dect/Dect Dect/internal Dect/external)
   1.2. Description about the call progress (who has initiated the call, a call back, etc.)
   1.3. If a call was disconnected unexpected the:
      1.3.1. Info about the display content of the DECT handset in the problem case like:
         1.3.1.1. can be seen immediately after a disconnection of the call directly the idle display
         1.3.1.2. can be seen immediately after a disconnection of the call a flashing

display

1.3.1.3. can be seen immediately after a disconnection of the call a text like "has hang-up"

1.3.2. Info if the Hang-up tone can be heard after an unexpected disconnection

1.4. If the connection has a bad quality, please describe the dysfunction 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])

1.5. Point of time when the problem occurred.

1.6. Is the problem reproducible?

1.7. If possible a photo from the display content or a video from the total problem sequence.

1.8. Info about the position of the DECT user at the site plan

1.9. Info if the DECT user has moved during the call

1.10. For internal users info about configured call distribution features like Teams, MULAP, Call Pickup, etc.

2. The statistical distribution of the problem:

2.1. How often does the problem on a day?

2.2. What is the relationship between good and bad DECT calls?

2.3. Is there a relationship between DECT problems and a dedicated location, e.g. a staircase?

2.4. Is there a relationship between DECT problems and a determinate base station?

3. The current site plan (position plan) of the base stations including information about special environmental 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 it, that the distance of the base stations is larger than 50 cm to any metal surfaces.

Please document this with a photo.

4. A current network deployment plan including the following info as **picture**:

4.1. IP addresses of all related components

4.2. Info about VPN

4.3. Info about the used PBX´s including used software versions and interconnections if more as one PBX is used (e.g. OSV/OSB or two linked OSBiz)

4.4. Info about BSIP deployment (small, medium, large) and used software version

4.5. Info about problem related SIP phones

4.6. Info about used switches

4.7. Info, if a UC solution (e.g. Web Client, MyPortal, etc. is involved)

5. Please log in at the BSIP web based management as "UnifyAdmin" and provide the following data:

5.1. BSIP backup (Administration > Backup Config)

5.2. the BSIP log data (Debugging > Download Logfiles)

5.3. BSIP coredump (Debugging > Download Corefiles)

5.4. And screenshots of

5.4.1. WBM Status > Base Status (absolute)

5.4.2. WBM Status > Base Mibs (absolute, previous)

5.4.3. WBM Status > Base RSSI (-85 dB) of all base stations (absolute)

5.4.4. WBM Status > Base 1588 (absolute)

5.4.5. WBM Status > User Mibs (absolute, previous)

6. The radio coverage at the location where the problem occurs (FRAQ and RSSI values concerning chapter 7-1 of the BSIP Service Documentation).

7. A Wireshark trace recorded at a mirror port of the IWU of the BSIP is required.

If the problem is reproducible please deliver only a short Wireshark trace, which covers the problem.

If the failure is not reproducible and a long-time recording is needed, please record multiple files with a size of 100MB.

You can write Wireshark compatible files with the following command line tools:

For Linux as example:

```
tcpdump -i eth0 -s 1500 -C 100 -W 50 -w hcip.pcap
```

where –C 100 stands for the file size in MB, –W 50 for 50 files and eth0 specifies the interface.

For Windows and Linux is tshark available as part of the Wireshark installation:

```
tshark -i 3 -b filesize:102400 -b files:50 -s 65535 -w c:\tmp\hcip.pcap
```

where –i 3 specifies the interface. With tshark –D can you get an overview about the available interfaces. The file size is specified in KB.

8. In dependency of the used PBX please attach also the internal diagnosis data from the PBX related *on the timing at which the error occurred*
9. PSR files if PSR required (E.g. the use of non supported switches).

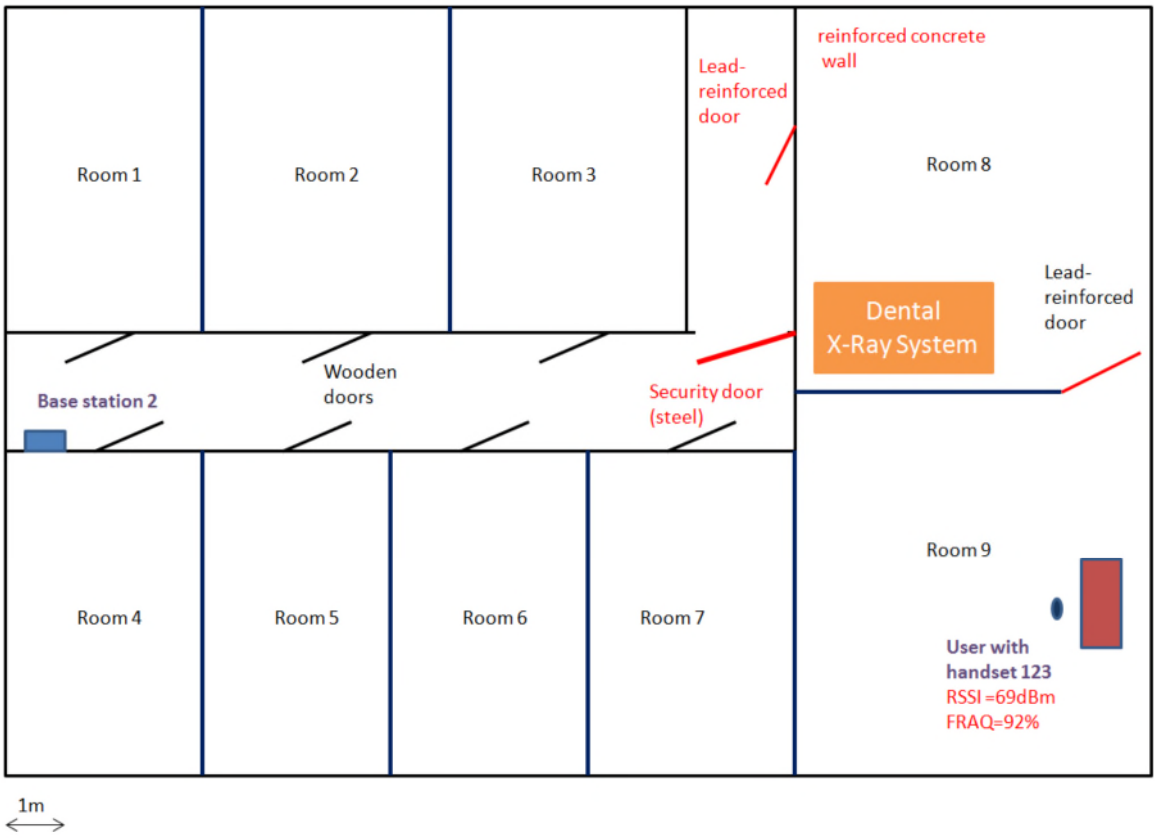
Example for Call related problems

!this is only an example!

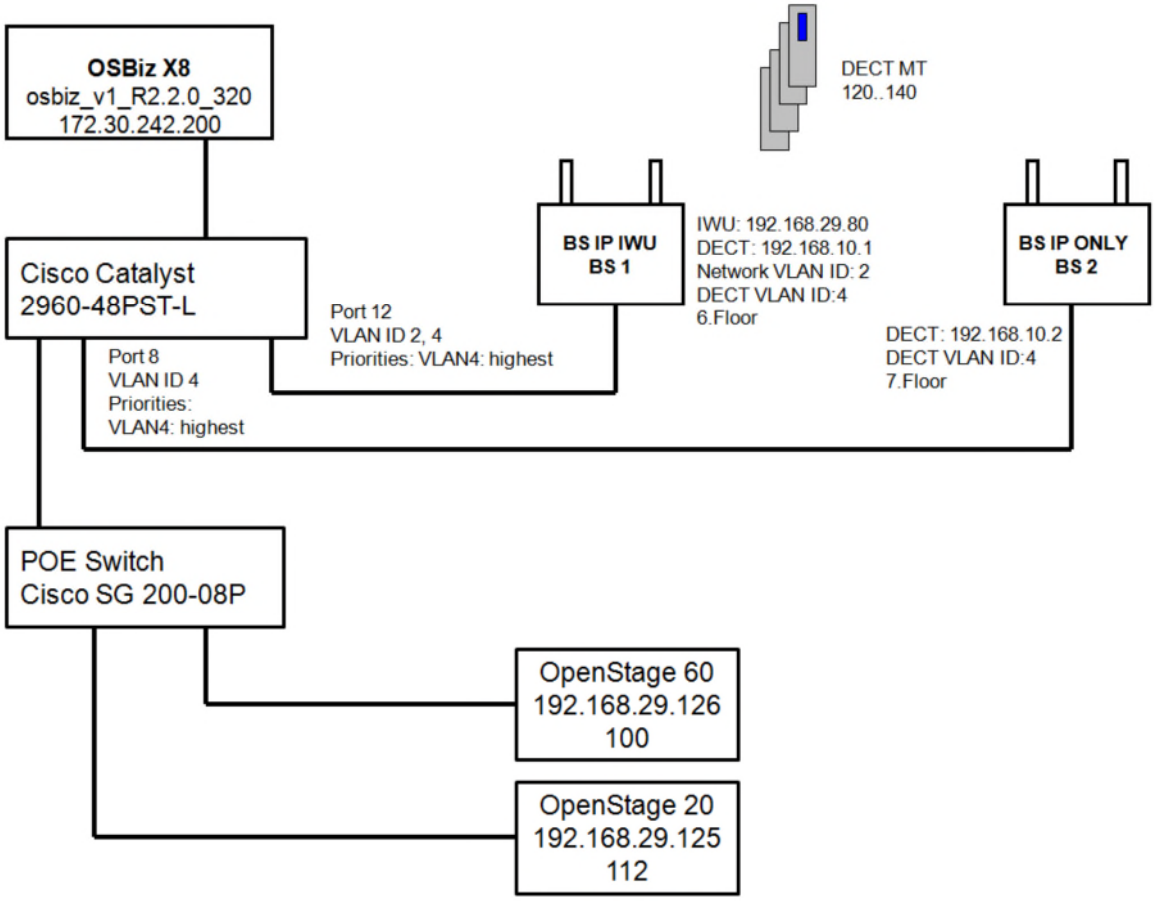
- *the DECT user “Meyer with the internal phone number 123 with an SL4 with SW*
  Version V1 R2.1.0 has called the external partner “Lehmann” with the number 00987654321
- *user 123 calls 00987654321*
  user 123 got a ringing tone
  user 00987654321 accepts the call and is successfully connected with 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 2014-07-23 at 17:50*
- *the problem is not reproducible*

- *the user with the handset 123* sits during telephone call in 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 500 Dect calls per day.*
- *The problem occurs mostly at the seventh floor.*
- *The problem occurs mostly at the proximity of base station two.*

7.floor



Floorplan:
Networkplan:



Attachments: iwu_config.tgz
logfiles.tgz
coredump.tgz
screenshots.zip
wireshark_2014_07_23__17_00.pcap
photo_location_bs2.jpg
172.30.242.200-gw-2014-07-23-diagfiles.tgz
PSR_Example_Customer.pdf
!END of example!

Problems concerning WBM

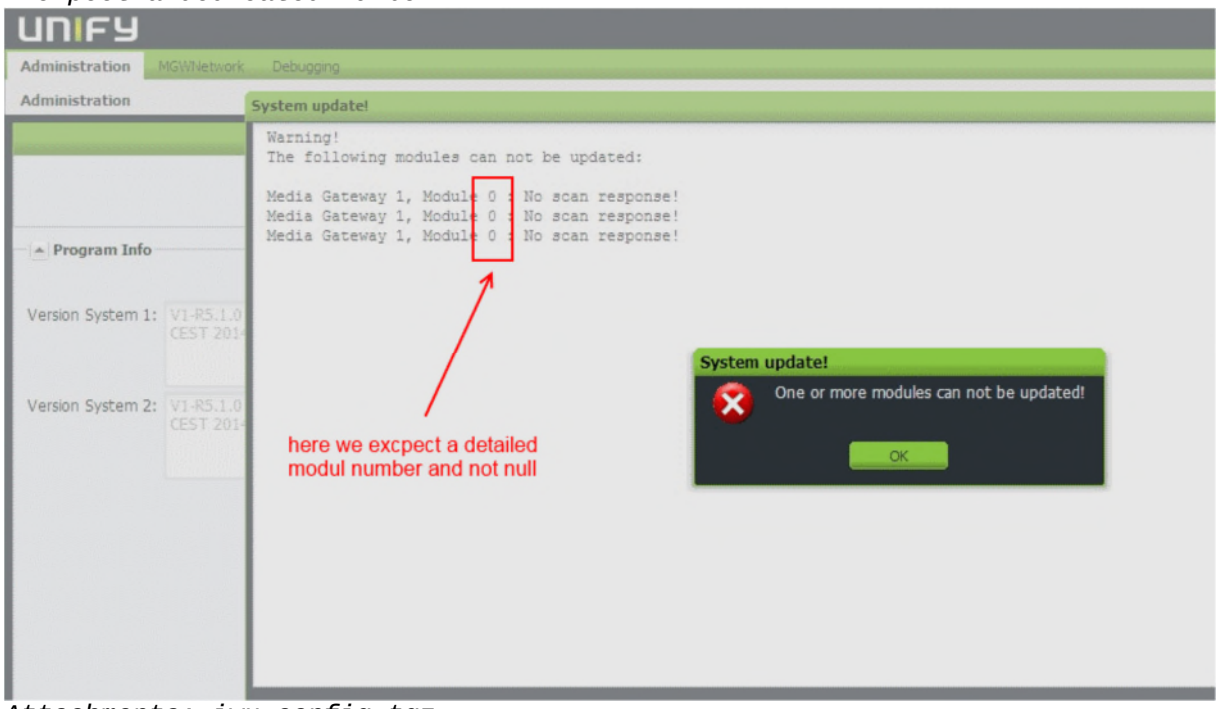
The following info is required for all problems with the use of the WBM:

1. The detailed, actual problem description including the following info:
   1.1. Please describe step by step, which operation of usage of the WBM causes a problem.
   1.2. Please document this as screenshots or as video sequence.
   1.3. Please describe which behavior you expect.
   1.4. Please note the point of time when the problem occurred.
   1.5. Is the problem reproducible?
2. If it is problem relevant, please attach the network deployment plan like described in chapter 7.5.1.
3. Please log in at the BSIP web based management as "UnifyAdmin" and provide the following data:
   3.1. BSIP backup (Administration > Backup Config)
   3.2. the BSIP log data (Debugging > Download Logfiles)

3.3.BSIP coredump (Debugging > Download Corefiles)

Example for problems concerning WBM

!this is only an example!
I try to update the firmware via the WBM > Administration > System Update.
The update of some base stations fails because of network problems.
I got an error message, but the Modul number is ever zero.
I expect a dedicated number.



Attachments: iwu_config.tgz
logfiles.tgz
coredump.tgz
!END of example!

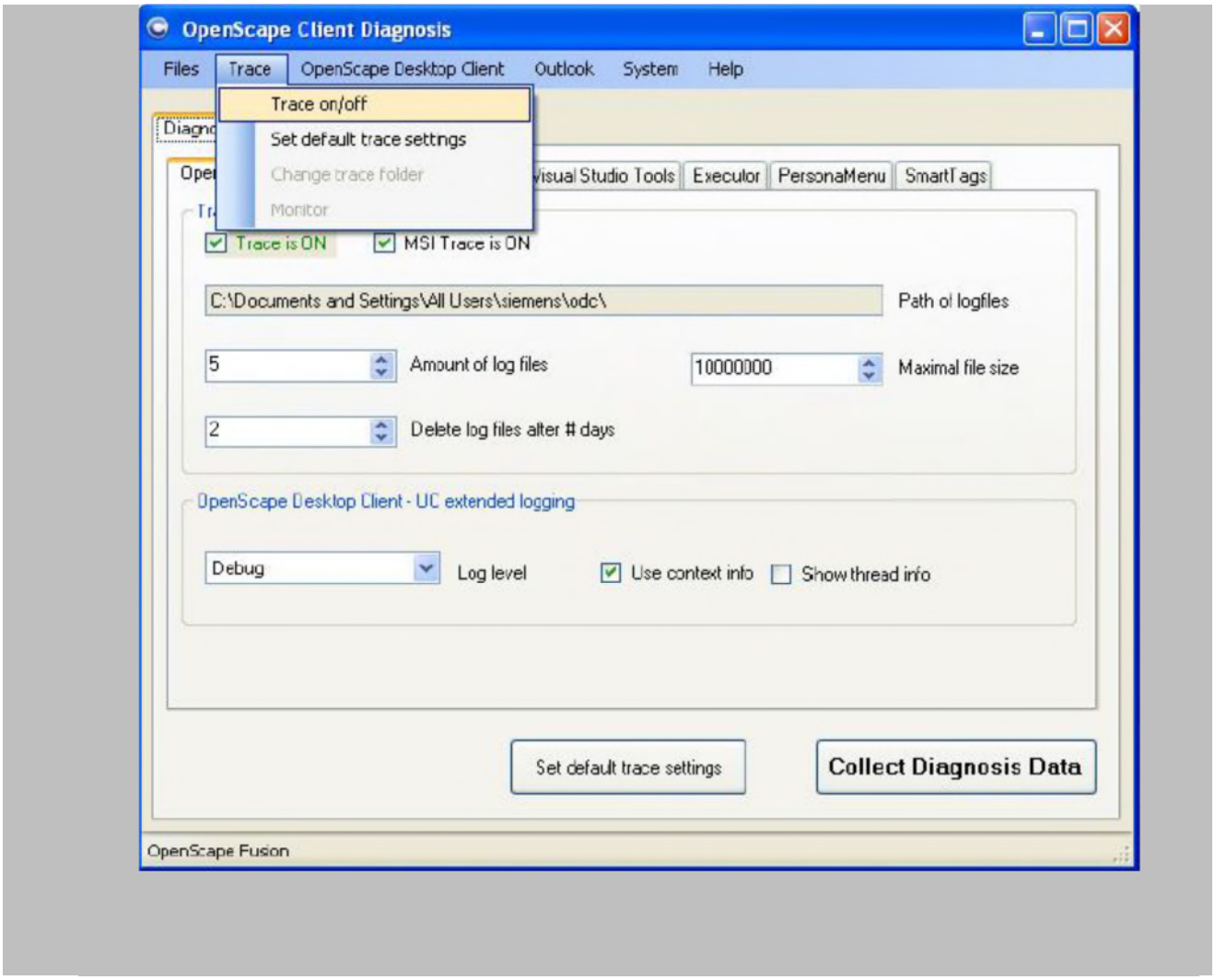
2.3.20. Fusion Issues

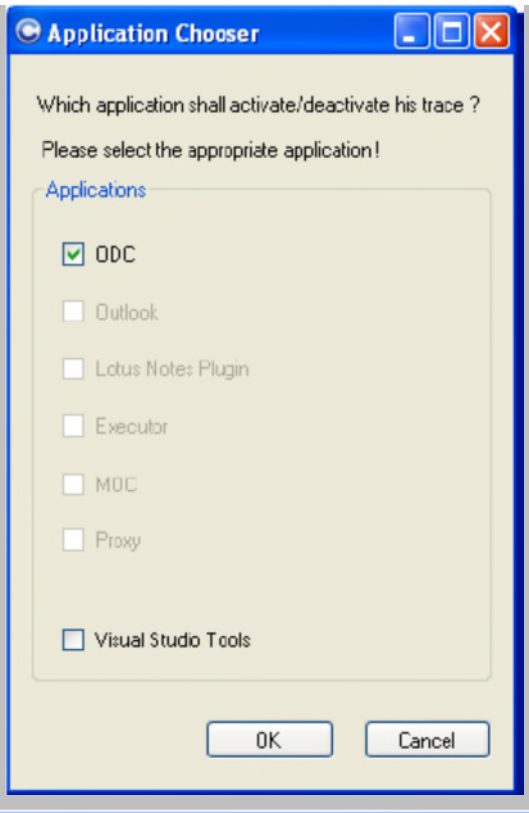
- Start the diagnosis tool

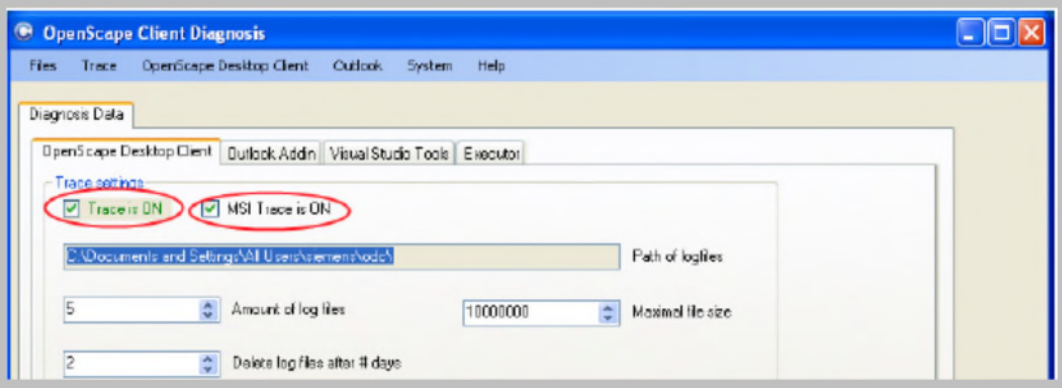
  Please open the MS Windows Explorer and navigate to the installation folder of the Fusion client.
  Navigate now to the subfolder tools.

  For OpenScape Fusion for Outlook this should be as default:
  C:\Program Files\Siemens\OpenScape for Outlook\tools
  Start the diagnosis tool for the Fusion Clients:
  OpenScapeClientDiagnosis.exe

- Activate ODC based tracing
  - **This requires admin rights for the related user!**

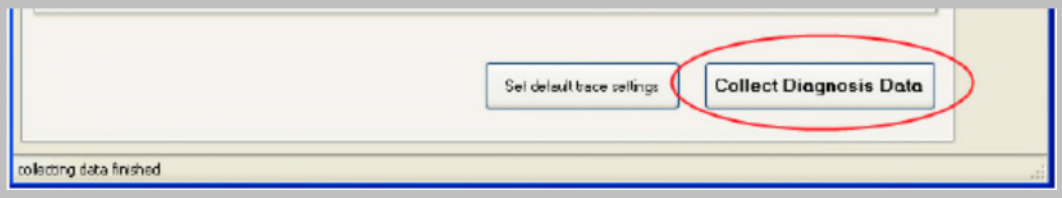

OpenScape Client Diagnosis
Files
Trace
OpenScape Desktop Client
Outlook
System
Help
Trace on/off
Set default trace settings
Change trace folder
Monitor
Visual Studio Tools
Executor
PersonaMenu
SmartTags
Trace is ON
MSI Trace is ON
C:\Documents and Settings\All Users\siemens\odc\
Path of logfiles
5
Amount of log files
10000000
Maximal file size
2
Delete log files after # days
OpenScape Desktop Client - UC extended logging
Debug
Log level
Use context info
Show thread info
Set default trace settings
Collect Diagnosis Data
OpenScape Fusion





  - Activate the standard ODC trace and the MSI trace for the ODC (see the screenshot above).
  - Select the checkboxes marked with the red ellipses like the screenshot above.
  - Close the groupware client, e.g. MS Outlook.
  - Close the OpenScape Fusion client via the OpenScape pearl at the taskbar.
  - Restart the groupware client, e.g. MS Outlook.
  - Restart the Fusion Client, if no automatic start is configured inside the groupware client.
- Reproduce the problem behavior.
- Collect the diagnosis data via the diagnosis tool
  - Press the Button "Collect Diagnosis Data" at the diagnosis tool.
  - This can take some minutes. You can see the activities of the tool inside the bottom bar at the tool.

- If the collection process is finished, you can find a zipped file at your file system.
- Please attach this file to your ticket.



- Deactivate ODC trace setting.
  - After reproducing the failure behavior and collecting the diagnosis data, please deactivate the ODC trace setting

2.3.21. OpenScape Contact Centre

For ALL faults reported on an OSCC, the following should ALWAYS be provided.

- Detailed description of issue , including affected Server / Client Machine names and credentials (if possible, a GOOD case and a BAD case should be provided for comparison)
- The current version including all applicable patches on both server and clients
- Remote access details and a contact on site to assist with further info if required
- Diagnostic Files from OSCC
- Windows EVT files for System, Application and Security
- If the system has CDSS rather than XMU/SBX , then log files from CDSS Server should be provided (warn and messages file)
- Up to date Design Database from the affected OSCC server(s)
- OSCC Manager Error Log / Agent Activity and Change Logs Reports where relevant

In addition to these basic requirements, and depending on the precise nature of the issue experienced, further information will be required, so other logs/traces should be provided. They are usually:

OSCC service failure

For this, the main requirements are the OSCC Diagnostic Files, Windows Event Viewer Logs, Details of Any Domain/Group Policies and A/V Software that could possibly affect the normal running of a service.

If created, any crash dump files (see Windows Support for creation of these)

If High Availability, please also include relevant Windows clustering logs

OSCC Telephony Issues

Relevant traces from the Voice Switch side (e.g. RTT trace for OSV)

Any available Wireshark traces for traffic between CC and Voice Switch

Client / Manager GUI Issues

Manager or Client Logs from the affected user(s) along with credentials for testing purposes. Note – it's good practice where possible to have both client and Manager applications installed on the main server so we can test with these if required. If the affected site is a V9 and using Agent Portal, Java version etc should also be provided. Agent Activity, Error and Change Log Reports should also be provided for any affected users.

Email / Web Chat Issues

Information regarding the Corporate Email Server / IIS server, such as credentials, current state, version.

Wireshark or similar traces between.

IVR (CDSS or XMU/SBX) related Issues

CDSS logs if using CDSS, current CDSS version and logon credentials, Wave File Format Design DB

Network Issues

Wireshark traces between solution components, network topology where available, including all applicable firewalls, SBC's etc (rules etc should also be provided if relevant)

Reporting Issues

Level 0 DB back up of affected Server(s)

Example Reports highlighting issue

2.4. Remote Access

This filed should be as detailed as possible but do not violate customer security rules.

It should be always be filled in; if there is not Remote Access this needs to be stated.

3. OPTIONAL INFORMATION

3.1. Hints

This is filled in when there is some additional information which might be relevant. Also if SD found something interesting it can be posted here:

i.e.

- Expected result of the scenario described
- Screenshot of the error for applications (UC clients etc.)

3.2. Customer

Customer name - optional, if different from the one mentioned in the tool

3.3. Partner Contact on Site

If there is a Partner Engineer on site that can be contacted, please provide contact details:

- Name
- E-mail
- Telephone Number

4. TICKET PRIORITY

The ticket priority is a key attribute to manage ticket processing and often determines the relevant applicable SLAs.

Once a ticket is created, the ticket priority can NOT be changed. To change the ticket priority, GCS must use the Ticket-Copy ticket action to create a new ticket. Therefore, it is very important to select the proper ticket priority when creating the initial ticket.

4.1. Priority Definition

The priorities are defined for tickets on a scale from 1 (highest priority) to 3 (low priority). Priorities are used for all tickets in GSI.flow.

4.1.1. Priority 1

- Major Incident
- Total System Unavailability: Complete breakdown of a system, network, function, or application that causes severe performance problems and customer impact.
- Partial System Unavailability: Partial breakdown of a system, network, function, or application that causes severe performance problems and customer impact: >=50% of users / ports affected
- Partial breakdown of a system, network, function, or application that causes severe performance problems and customer impact: >=25% of users / ports affected
- Severe impact to business operation of system, functions, or applications in a production environment
- Continuous or near continuous interruption of service occurs and no workaround is available.
- Product- and/or Solution issues which are hindering planned and committed roll outs causing NCC's in a way that business of Unify is heavily impacted and customer satisfaction heavily violated.

4.1.2. Priority 2

- Incident which restricts usage of the system, functions, or applications
- Faults which cause a very restricted availability of applications or applications with poor quality (background noises, transmission faults, call processing is altered in such a way as to degrade service quality or handling of business data.)
- Failure of a single component, module, or router
- Intermittent disruption of service without a stable workaround available.

4.1.3. Priority 3

- The usage of the affected system, functions, or applications is slightly restricted
- Failure of subscriber lines, trunk lines, hardware, applications that are less business critical for the customer.

GLOSSARY

B&R	Backup and Recovery
BoM	Bill of Material
CAB	Change Advisory Board
CDC	Customer Data Collection sheet
CGW	Customer Gateway
CI	Configuration Item
CMDB	Configuration Management Database
CSI	Continual Service Improvement
CSP	Customer Service Portal
Customer Gateway (CGW)	Access from the data center of the service provider to the customer network via a HW/SW gateway (equipment of the service provider) that is located at the customer site.
e2e	End to end
ECAB	Emergency Change Advisory Board
Equipment	Components that are the subject of the service and are listed in the directory of system components.
FMO	Future mode of operation
GCS	Global Customer Service
G-DMS	Global Document Management System of Unify
GSI.CMDB	Configuration Management Database of Unify
GSI.CSP	Customer Service Portal of Unify
GSI.FLOW	Workflow System of Unify
GSI.MON	Monitoring Solution of Unify
GSI.RSP	Remote Service Platform of Unify
GST	Global Service Tools
HW	Hardware
ICT	Information and Communication Technology
ISO	International Organization for Standardization
IT	Information Technology
ITIL®	Information Technology Infrastructure Library
KPI	Key Performance Indicator
LAN	Local Area Network
LC	Local Company

LE	Local Entity
m2m	Machine to machine
MoP	Method of Procedure
MS	Managed Service
NBD	Next Business Day
OBSO	OpenScape Baseline Security Office
OCC	outside covered contract (efforts)
OEM	Original Equipment Manufacturer
OLA	Operational Level Agreement
OPD	Operational Process Document
OS	Open Stage
OSB	OpenScape Branch
OSBR	OpenScape Backup & Recovery
OSV	OpenScape Voice
PIR	Post Implementation Review
PM	Project Management
Product milestones	M0 Package formation M1 Implementation release M2 Sales release M3 Unrestricted production release M4 Release of product discontinuation M42 Communication of product discontinuation, order stop for new deliveries M43 End of production M44 End of support by development M45 End of Level 3 Support M46 End of delivery of user and service documentation M47 End of hardware support by production and end of spare parts production; repairs are still possible M48 End of activities in central customer service M5 End of product activities
RfC	Request for Change
SE	Service Element
SESAP	Secured Enterprise Service and Administration Platform
SIRA	Secured Infrastructure for Remote Access
SLA	Service Level Agreement

SLES	Suse Linux Enterprise
SLM	Service Level Management (process/person(s))
SPoC	Single Point of Contact
SW	Software
TDS	Technical Design Specification
TM	Transition Management
UC	Unified Communication
VPN	Virtual Private Network
WD	Workday

Table 1: Glossary

About Unify

Unify is one of the world's leading communications software and services firms, providing integrated communications solutions for approximately 75 percent of the Fortune Global 500. Our solutions unify multiple networks, devices and applications into one easy-to-use platform that allows teams to engage in rich and meaningful conversations. The result is a transformation of how the enterprise communicates and collaborates that amplifies collective effort, energizes the business, and enhances business performance. Unify has a strong heritage of product reliability, innovation, open standards and security.

unify.com

UNIFY Harmonize your enterprise