21 May 2021

Information Required When Raising an IP Office Escalation to Avaya

ADMS 159999

Issue 10

Abstract

This document specifies the technical information required when raising an IP Office escalation to Avaya.

Contents

1 Mandatory Technical Requirements When Raising an Escalation

The following information must be provided when raising an IP Office escalation to Avaya.

IP Office components not listed within this section have no specific mandatory requirements.

1.1 Common to all Technical Escalations

1. An accurate description of the problem being escalated.
2. A copy of the configuration that was running on the IP Office at the time the problem occurred.
3. The versions of any IP Office application software involved in the problem.
4. Written step by step instructions detailing how the problem can be reproduced. If the problem cannot be reproduced then details of what has been tried so far to reproduce or solve the issue must be included.
5. Where trace or config files are encrypted then passwords to allow decryption must be provided.

1.2 IP Office Core Reboot Issues

1. IP500v2 Reboot.

   A SysMon trace showing the reboot and a corresponding config.

   Please note a TLB decode cannot be provided if the code is all zeros or if the restart is caused by memory or buffer depletion.

   On the IP500v2 platform memory or buffer depletion issues can be identified from the information contained in the system resource (RES) messages in the sysmon trace. If the FreeMem value or the value of any of the 4 buffer pools constantly reduces then this is an indication of these problems. If this is the case then please provide the trace and Avaya will advise on what additional information will need to be obtained.

2. Server Edition IP Office Service Reboot.

   A core dump file (arc_core.ipoffice.tar.gz) and corresponding profile file (profile.ipoffice.core.txt) must be provided. These can be downloaded via Web Manager as follows:

   - Login to Web Manager and select Platform.
   - Select Logs>Download. In the Debug Files pane select Create Archive. Any core dump and corresponding profile files available will now be listed.

   The corresponding sysmon archive logs (sysmon_logs<date_time>.tar.gz) should be generated as soon as possible after the event and provided.

   Please note that in the case of a Server Edition IP Office service reboot the TLB information in the SysMon trace contains no useful information.

1.3 Windows Server and Client Application Issues

1. For all PC's running IP Office applications the operating system version information (including service packs) and the system information (use msinfo32 on Windows based PCs) must be provided.
2. If multiple systems are involved (e.g. server and client applications) then this information must be provided for all relevant systems.
3. If your operating system generates an error, a copy of the System Event Viewer log files must be provided.
4. If the application utilizes a browser, the type and version must be provided.

1.4 Call issues

1.4.1 IP Office Core Call issues

1. A SysMon trace must be provided that covers the problematic call scenario along with details that will allow Avaya to identify the problematic call (e.g. The date and time when the problem occurred, filename of trace if multiple traces). Default trace options must be present in the trace as a minimum.

2. Wireshark traces must be provided for a speech path, speech quality or call setup VoIP problem.

1.4.2 IP Office Voicemail Pro Server and Client related Call issues

1. A level 9 or Verbose debug trace output from the IP Office Voicemail Server must be provided.

   The VMPro debug level can be set from the VM Client in General system preferences. On a Server Edition or Application Server platform the VMPro debug level can also be set from Web Manager.

2. The VMPro database .mdb file must be provided.

3. If the problem is related to a call scenario then a SysMon trace must be provided that captures the call. The SysMon trace must have the default trace options enabled plus:

   - Call>PC Voicemail>Voicemail Events
   - Call>PC Voicemail>Voicemail Messaging

1.4.3 Avaya Communicator for Windows

1. Communicator diagnostic logs obtained from the application.

   These first need to be enabled by selecting Settings -> Support -> Enable Diagnostic logging within the application. Once enabled and the problem has reoccurred the logs can be obtained by selecting “Settings>Support>Report a problem”. This creates an email with the diagnostics logs attached. The user can then email these logs to a recipient of their choice.

   The Communicator configuration file (config.xml) must also be attached. This is located in the following directory :-

   C:\Users\”Username”\AppData\Roaming\Avaya\Avaya Communicator

   The following 1XP logs must also be included (1XP logging level must be set to DEBUG) :-

   1XoverallRollingFile.log

2. Sysmon traces must be provided with default trace options plus:

   - SIP>Events>SIP = Verbose
   - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line)

1.5 IP Office Server Edition and Applications Server Issues

1. For installation, upgrade, Web Control and Web Manager problems the following logs from Logs > Download in Web Manager are required:

   - Installation – install_logs_<date>.tar.gz
   - Upgrade – upgrade_logs_<date>.tar.gz
   - System logs – system_logs_<date>.tar.gz
   - Webcontrol logs – webcontrol_logs_<date>.tar.gz
   - Web Management logs – webmanagement_logs_<date>tar.gz
   - IP Office – ipoffice_logs_<date>.tar.gz

   The Web Manager logging level must be set to DEBUG.

2. Specifically for Web Manager issues a SysMon trace capturing the problem is also required with default trace options plus the following enabled:

   - Services > Web Services
   - Services > HTTP

3. For VMPro problems the following files are required:

   - VMPro logs – voicemail_logs_<date>.tar.gz. Please note Verbose debugging must be set before logs are generated.
   - SysMon trace with default trace options plus Call>PC Voicemail>All.

4. For One-X Portal problems the following files are required:

   - one-X Portal logs – onex_logs_<date>.tar.gz. Please note the Master Logging Level must be set to DEBUG before logs are generated.

5. For Contact Recorder problems the following files are required:

   - VMPro logs – voicemail_logs_<date>.tar.gz. Please note Verbose debugging must be set before logs are generated.
   - Contact Recorder logs – contact_recorder_logs_<date>.tar.gz. Please note the Debug level must be set to DEBUG before logs are generated.

6. For Media Manager problems the following files are required:

   - VMPro logs – voicemail_logs_<date>.tar.gz. Please note Verbose debugging must be set before logs are generated.
   - Media Manager logs – mediamanager_logs_<date>.tar.gz. Please note the Log level must be set to DEBUG before logs are generated.

7. For WebRTC Gateway problems the following files are required:

   - WebRTC logs – WebRTCGateway_logs_<date>.tar.gz. Please note the log level must be set to debug before the logs are generated. This can be set via Web Manager in Applications>WebRTC Configuration>System Settings.

8. Supplied Server Edition configs must be accompanied by the corresponding .cfi file.

1.6 1XP Generic Information for All Issues

1. 1XP Logs must be provided. The Master Logging Level must be set to DEBUG.

   On Windows installations these are found in C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat-6.0.18\logs. All files in this directory should be zipped and provided.

   On Linux installations these files are available in the Logs > Download page in Web Manager as specified in section 1.5 above.

   Ideally the problem should be captured in a “clean” set of logs, i.e. stop the 1XP service, delete all the log files, restart the 1XP service and reproduce the issue.

   By default the 1XP logging level is set to error only. Full debugging needs to be enabled in order to obtain the correct information. This can be done by going into 1XP Administration/Diagnostics/Logging Configuration/Master Logging Level and changing the threshold from ERROR to DEBUG.

   Please note that with the master logging level set to DEBUG the number and size of the log files may rapidly increase and start to fill up the hard drive. The logging level should be set back to ERROR when the required traces have been captured.

1.6.1 1XP Memory and Performance Issues

1. If a performance issue is encountered or a memory leak is suspected then a Heap and Thread dump must be taken via the Administration Dashboard. This can be done by selecting Diagnostics -> Generate Memory Dump and Generate Thread Dump. Once these have been generated then these will be included in the 1XP logs generated via Web Manager.

   These dumps and logs should be generated every 2 days for a week so that any memory leak can be tracked and identified over time. At the same time a screenshot every 2 days of the 1XP Administrator Dashboard should be taken to record the overall 1XP health.

1.6.2 1XP Call Assistant Issues

1. The 1XP logs as specified in section 1.6 above.
2. Call Assistant log files covering the problem. These can be accessed by right clicking on the Call Assistant system tray icon and selecting “Logs”.
3. Sysmon traces MUST be provided. The Sysmon options that MUST be set are all the default options plus:
   - SIP>Events>SIP = Verbose
   - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line)

1.6.3 1XP Outlook Plugin Issues

1. The 1XP logs as specified in section 1.6 above.
2. The local log file from the machine running the plug-in available in the following location: C:\Users\<Windows user name>\AppData\Roaming\Avaya\IP Office\Avaya IP Office Plug-In\Logging
3. Sysmon traces must be provided (the Sysmon options that must be set are all the Default options plus:
   - SIP>Events>SIP = Verbose
   - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line)

1.6.4 Lync Integration

1. The 1XP logs as specified in section 1.6 above.
2. Lync Integration diagnostic logs obtained from the application.

   These can be obtained by selecting “(Avaya) Settings>Support>Report a problem” within the application. This creates an email with the diagnostics logs attached. The user can then email these logs to a recipient of their choice.

   The “Enable Debug Mode” option must be enabled.

   The logs can also be found on the User’s PC in the following location :- C:\Users\xxxxxx\AppData\Roaming\Avaya\Avaya Microsoft Lync Integration (where xxxxxx is the logged on user).

3. Sysmon traces must be provided (the Sysmon options that must be set are all the default options plus:
   - SIP>Events>SIP = Verbose
   - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line)

1.6.5 1XP Salesforce Plugin

1. The 1XP logs as specified in section 1.8 above.
2. The following logs must be provided:

   - browser_connector.log
   - cti_connector.log.

1.6.6 One-X Mobile Preferred Edition Issues

1. The 1XP logs as specified in section 1.6 above.
2. The make and model of phone being used.
3. The Operating System and version.
4. A diagram or description of the network topology.

1.7 Unified Communications Module (UCM)

1. The following log files from the Logs section of the Web Control Logs page:

   - Installation / Upgrade – install_logs_<date>.tar.gz
   - System logs - system_logs_<date>.tar.gz
   - Webcontrol logs - webcontrol_logs_<date>.tar.gz
   - Vmpro logs - voicemail_logs_<date>.tar.gz.
   - One-X Portal logs - onex_logs_<date>.tar.gz

   Logs can then be captured and retrieved using webcontrol.

   To provide full debugging information the VMPro logs must be set to Verbose. This setting can be checked and changed if necessary in the Settings tab.

   For 1XP problems the Master Logging Level must be set to DEBUG before the logs are generated.

   Please note that with the master logging level set to DEBUG the number and size of the log files may rapidly increase and start to fill up the hard drive. The logging level should be set back to ERROR when the required traces have been captured.

   Where the problem is a crash of the VMPro application then a core dump file must also be provided. This can be obtained from the Debug Files section of the Download tab as follows:

   - Login to Web Manager and select Platform.
   - Select Logs>Download. In the Debug Files pane select Create Archive. Any core dump files available will now be listed.

1.8 IPOCC

1. A description of the problem with the details below:

    a) Date/time when the bug occurs.
    b) Type of phone and trunk type.
    c) Internal/external call.
    d) Media type (voice, email, chat).
    e) Impact of the bug.
    f) Is the bug reproducible.
    g) Target topic.
    h) Site history. When was system first installed and when was problem first observed.

2. Export files containing all Task Flows and IVR Scripts.
3. The IPO Config file.
4. A sysmon trace covering the time period the problem occurred. The trace must contain all default filter options plus:

    - SIP>Events>SIP = Verbose
    - Services>TAPI, Services>TAPI>(TAPI Call Log), Services>TAPI>(TAPI Line)

5. Details of the affected task flow (if applicable).
6. A compressed copy of the TTrace directory from the day the problem occurred.

    Further specific TTracing may be required once the bug has been analysed. This can't be enabled until after the initial escalation as there's a risk of excessive disk usage with some trace options enabled. Information on these trace categories can be found in section 2.25 below.

7. The IPOCC configuration export csv files. These can be generated as follows:

    - Login to the IPOCC as Administrator and select Configuration>System>Configuration Report.
    - Ensure all boxes are ticked, select format .csv and select Export.
    - Zip the resultant .csv files and provide them with the escalation.

8. Full details of the versions of the IPOCC components installed. The output report of the WhatIsInstalled.exe application should be provided with the escalation.

9. Details of the IPOCC Server type and specification.

    Where the server is a Virtual Machine then the following details must be provided:

    a) The CPU allocation and reservation settings.
    b) The memory allocation and reservation settings.
    c) The hard disk provisioning and resource settings. The disk must be thick provisioned.

    The best way of providing this information is with screenshots of the following:

    - The Virtual Machine Properties>Resource tab with CPU selected.
    - The Virtual Machine Properties>Resource tab with Memory selected.
    - The Virtual Machine Properties>Resource tab with Disk selected.
    - The Virtual Machine Properties>Hardware tab with the Hard disk selected.

    Where the server is a physical machine then details of the CPU, RAM and Operating System are required. These should be gathered using msinfo32.

    The minimum requirements for an IPOCC Server are specified in the Avaya IP Office Contact Center Reference Configuration on the Knowledgebase.

From IPOCC version 10.1 onwards an audit tool is provided to make capturing the necessary diagnostics easier. The tool is installed in C:\Program Files (x86)\Avaya\IP Office Contact Center\Trace System\Log Collector. Full instructions on how to use it are provided in a Readme.txt file in this location.

1.9 Cloud Operations Manager

1. Debug log files with the logging level set to debug.

   The logging level can be set by logging into Cloud Manager and selecting Settings>Preferences. The logs can be downloaded from the same screen.

1.10 Equinox / IX Workplace

1. Debug logs from the client. These can be obtained from the application by selecting Settings>Support>Report a Problem.
2. Sysmon traces with default trace options plus:

   System>Development Tracing
   SIP>Events>SIP = Verbose
   CTI>MTCTI Events
   CTI>MTCTI Tx Full
   CTI>MTCTI Rx Full

3. Screenshots of any errors shown on the client.
4. Confirmation that certificates are in place.
5. A System Status snapshot capturing any alarms or errors.
6. A packet capture for any media related issues.

1.11 SoftConsole

1. A sysmon trace capturing the failure scenario with default trace options. 2. A copy of the SoftConsole profile .pfs file.	

1.12 ACCS IP Office Issues

1. A sysmon trace capturing the problem with the default trace options plus the following enabled: - SIP>Events>SIP = Verbose - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line) 2. If the problem is media related then a Wireshark trace capturing the problem must also be provided.	

2 Technical Requirements That May Be Required After Raising an Escalation

The following information may be requested after an issue has been escalated to allow further investigation into the problem. This information would also be useful at the initial point of escalation if available.

2.1 Common to all Technical Escalations

3. The frequency of the problem.
4. The Calling Party Number.
5. The Called Number (or Number Dialed).
6. A trace of a good call if applicable so comparisons can be made.
7. If the unit is part of a multi-site network then configurations from each site should be obtained as well as detailed network diagrams.
8. If a problem relates to inter-connectivity, whether to another Avaya PBX platform or to any other 3rd party device (i.e. a Cisco Router, Firewall etc.) then a network diagram should be provided. The diagram should provide details of all PC/PBX/Router IP addresses, IP routes configured, Bandwidth available on links, details of any 3rd party equipment e.g. Switch/Router make, model & Software level, etc.
9. Any background information relating to the issue (e.g. No problem on previous s/w).
10. If there have been any significant changes recently at the customer site then these should also be noted e.g. Recent platform upgrade; recently reconfigured Voice Mail auto-attendant; voice recording now enabled for all calls.
11. Details of whether the customer is using a TAPI, Web Config Service or other 3rd party CTI application. If yes then details of whether it's a DevConnect approved solution or not should be provided.

2.2 Server and Client Application Issues

1. Information on any other software packages installed on that system.
2. For SoftConsole a file containing the debug output for the application. Details on how to enable this tracing can be found on the Knowledgebase.
3. Screenshots or video capture.
4. For a Manager issue the generic requirements can be limited to:
    - config
    - full description
    - a Wireshark trace may be required to investigate some problems.
5. The IP address(s) of the client machines experiencing the problem.

2.3 Server Edition Virtual Machine Deployment

1. Screenshots of Server Edition virtual machine settings so allocated resources can be verified against requirements.

2. A copy of the VMware log if it's suspected that VMware is related to the problem.

2.4 Call issues

2.4.1 IP Office Core Call issues

1. Details of the phone types and firmware versions being used (and which keys pressed if appropriate). Also include any extras such as headsets, BLF modules or PC applications.
2. If it is found that the problem is related to buffer or memory depletion then SysMon traces covering the period since the last system restart are required.
3. Date of the last upgrade of the IP Office software.
4. Number of phones in use and details of the call levels, concurrent and totals.
5. If the problem cause is unclear then a longer period of SysMonitor trace prior to the problem symptoms being noticed should be provided (suggest 24 hours).
6. The *55 stamp log shortcode can be used to mark the point in the sysmon trace immediately after the point where the problem occurs.

2.4.2 IP Office VoIP (H323 and SIP) issues

1. Details of the customer's network infrastructure. This should include:

    - An accurate network topology diagram covering all sites involved.
    - IP Address Scheme information, IP Address and Masks of main switches, routers and other relevant equipment

2. Information on any 3rd party routers, switches or endpoints:

    - Make & Model number
    - QoS Capabilities i.e. Layer 2 VLAN or Layer 3 Diffserv etc.
    - Other relevant capabilities (bandwidth, managed/unmanaged, etc).
    - Configurations if available, preferably in a non-proprietary format.

3. Whether IP Hard phones or Soft phones are in use:

    - Make & Model number.
    - Number of phones in use or planned.
    - Version number of H323 IP Phone &/or Software/firmware. This can by provide via a screenshot of SysMon>Status>H323 Phone Status.
    - Configuration Type, i.e. DHCP or Static.
    - Provide a typical configuration and list settings.

4. Wireshark trace(s) capturing the problem at both the IPO and phone end if applicable. Details of the points on the network from which the trace(s) have been taken should be provided.
5. SysMon Trace file/s with the correct trace options enabled. If unsure of what options to enable please seek advice from Avaya.
6. If problem is SIP Provider specific then test account details should be provided so the problem can be replicated.
7. The following SysMon trace options should be enabled for SIP problems in addition to the default:

    - SIP>Events>SIP = Verbose

2.4.3 IP Office Voicemail Pro Server and Client related issues

1. Information regarding the Voicemail Installation including a copy of the call flow currently in use is required.
2. Details of which components are also installed. E.g. Campaigns, Text to Speech, Web Voicemail etc.
3. Details of how VMPro is configured. This information can be found in the following locations :-

   PC running 32 bit Windows OS - register hive ->
   HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\Media Services\Directories
   PC running 64 bit Windows OS – register hive ->
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya\Media Services\Directories
   PC running Linux (SE/UCM/Apps Server) - .ini file -> /etc/ vmpro_settings.ini

4. If the issue is related to 3rd party database access then a copy of the database and details of how to access it should be provided.

2.4.4 IP Office CTI (TAPI/WAV and DevLink Pro) issues

1. Software level of Tapi or DevLink DLL files – in the case of Tapi, which version is installed; i.e. tapi2 or tapi3 (TSPI2W.tsp and TSPI3W.tsp).
2. Contact details of the developer or company who authored the 3rd Party CTi software.
3. Name of application and DevConnect certification status.
4. A SysMon trace with the default trace options plus Services>TAPI.
5. A TAPI debug trace from the PC. This can be enabled as follows:

   - Using the registry editor navigate to HKEY_LOCAL_MACHINE\SOFTWARE\AVAYA\IP400\TSPI
   - Right click and add a new String Value. Give this value a name of DebugFile and in value data enter C:\TAPI_Trace.
   - Restart the PC.
   - This will create a file on the C Drive called TAPI_trace.
   - The trace file will become active after the re-start and log the initial and subsequent activity of the TSP driver.

On a 64-bit OS TAPI debug tracing can be enabled as follows:

   - Create a folder on the PC to contain the traces (e.g. C:\TAPI).
   - Right click the folder and select Properties.
   - Select the Security tab and click Edit.
   - Click Add and add Network Service as a user. Click apply and ok.
   - Using the registry editor navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\AVAYA\IP400\TSPI
   - Right click and add a new String Value. Give this value a name of DebugFile and in value data enter a file path to the newly created folder (e.g. C:\TAPI\TAPI_Trace).
   - Re-start the PC.
   - This will create a file on the C Drive called TAPI_trace.
   - The trace file will become active after the re-start and log the initial and subsequent activity of the TSP driver.

6. TAPI issues should be reproduced using the TAPI test harness.
7. Any additional information regarding the PC that is running the CTi application. For instance:
   - What anti-virus software is running?

- When was the last Service Pack applied?
- What other applications is the customer running?

2.5 1XP Generic Information for All Issues

1. 1XP Configuration Database on Windows. These are found in C:\Program Files\Avaya\oneXportal\Tomcat\apache-tomcat<version>\bin\onexportal.

2. 1XP Configuration Database on Linux. These are found in /opt/Avaya/oneXportal/<version>/apache-tomcat/bin/onexportal

   Ideally the whole bin\onexportal directory will be zipped and submitted. Ensure the 1XP service is stopped before doing this.

3. A copy on the 1XP PostgreSQL database.

4. A sysmon trace with default trace options plus:
   - SIP>Events>SIP = Verbose
   - CTI>TAPI, CTI>TAPI>(TAPI Call Log), CTI>TAPI>(TAPI Line)
   - Services>HTTP
   - Servies>Web Services

2.6 1XP Installation Issues

1. Data entered into the installer and options chosen. e.g. were default values overridden. (Submission as screenshots or video capture of the installation is acceptable).
2. Windows Event Log entries for the installation process.
3. The environmental variables being used on the server (before & after installation). This can be simply obtained from the command line by typing the ‘set’ command and submitting a screen shot.
4. Where an incompatibility with a third-party application or service is the suspected issue, supply an indication of the network ports that they use.

2.7 1XP Initial Start-up Issues

1. IP Addresses, firmware versions, installed licenses of the IP Offices being provisioned. The information may be submitted as screenshots or video capture taken during the provisioning process.
2. If the issue is LDAP related, the LDAP Server configuration details entered are required. This can be supplied as a screenshot of the entered details.
3. Where the provisioning process appeared to complete successfully, but there is still an issue, the component status details should be provided as a screenshot from the administration view.
4. Where a user appears to have been provisioned in 1XP however the user ‘cannot login’ provide:
   - a screenshot of the login page showing response to the login attempt.
   - a confirmation that, in IP Office Manager, the Avaya one-X Portal option is checked for that user.
   - the user name for the user attempting login to 1XP.

2.8 1XP Software “Exceptions”

1. Where any exception condition is evident in the browser submit a screenshot of the browser message. Also provide context of what the user was attempting to do. This should be done from a fresh login after first clearing the browser cache manually.
2. The Application and System event logs from the 1XP server covering the period the problem occurred.

2.9 1XP User Interface Issues (Administration View)

1. Server Environment, as indicated in the administration view ‘Environment’ control. Supply as a screenshot.
2. Where there is a suspected issue with Administration of a certain IP Office unit, a screenshot of the IP Office connection test should be supplied.

2.10 1XP User Interface Issues (User View)

1. Screen shots of issues, with context description.

2.11 1XP Locale Issues

1. If a translation problem please provide annotated screenshots or video capture.
2. If the problem is locale specific and is not a translation issue please provide all the locale information for the server, including:

    - Regional Options, Time/Date, Keyboard, Location, Languages.
    - The information may be submitted as screenshots or video capture of the tabs of the Windows Regional and Language options control.

2.12 1XP Call Assistant Issues

1. Screenshots or description of the configuration settings.

2. Call Assistant log files covering the problem. These can be accessed by right clicking on the Call Assistant system tray icon and selecting “Logs”.

2.13 1XP Microsoft Exchange Calendar Integration

1. The following log file should be supplied in addition to those specified in the generic 1XP issue section:
    - 1XSCSServicesRollingfile (yy-mm-dd).log. Details of the time and date the problem occurred should be provided.

2. Windows Server system, application and security event logs. Details of the time and date the problem occurred should be provided.

2.14 1XP Microsoft Outlook Plug-in

1. The following log file is required in addition to those specified in the generic 1XP issue section:

    - 1XSCSServicesRollingfile (yy-mm-dd).log

2. Windows Server system, application and security event logs. Details of the time and date the problem occurred should be provided.

3. The local log file from the machine running the plug-in available in the following location:

    Windows XP:

    C:\Documents and Settings\<Windows user name>\Application Data\Avaya\IP Office\Avaya IP Office Plug-In\Logging\ AvayaOnexPortalClientLog.yyyy-mm-dd.log

    Windows 7 onwards:

    C:\Users\<Windows user name>\AppData\Roaming\Avaya\IP Office\Avaya IP Office Plug-In\Logging

2.15 Salesforce.com

1. The following log files may be required:

    - Logs browser_connector.log
    - cti_connector.log

    These are stored in the following location: C:\Program Files\Avaya\IP Office\Avaya IP Office Plug-in for Salesforce.com

2.16 One-X Mobile Issues

1. Traces from the One-X Mobile application can be taken from the phone as follows:

   For Android
   Note: The phone must be registered with the IP Office for logs to be collected automatically.

   To set the logging information:
   - On the Home screen press the menu button.
   - Select “Settings”.
   - Scroll down and select “Advanced”.
   - Select “Logging Level” and set “Verbose”.
   - Enable “XMPP debugging” if advised by Avaya.

   To save the logs:
   - On the Home screen press the menu button.
   - Select “About”.
   - On the “About” screen press the menu button again, “Log upload” will be seen.
   - Select “Log Upload” - logs from the client will be sent to the One-X Portal server.

   To collect the logs:
   For a Linux server use WinSCP to connect and collect the logs which are saved in:
   /opt/Avaya/oneXportal/<One-X version>/apache-tomcat/logs/smack-file-transfer.

   For a Windows server the logs are saved in the following location:
   C:\Program Files (x86)\Avaya\onexportal\Tomcat\Server\logs\smack-file-transfer.

   The log file can be identified by the filename. The One-X Mobile extension is seen immediately after logs, followed by the date and time.

   If there are connectivity problems, the logs can be copied from the following location in the phone:
   Android/data/com.avaya.ScsCommander/files/staging

   Note: Remember to set the logging level back to the original setting.

   For iPhone
   Note: The sending of logs requires a functional email account on the iPhone, logs are sent via email.

   To set the logging information:
   - In the iPhone Settings menu, select "Avaya Mobile" towards the bottom of the list.
   - Scroll down and ensure that "Verbose Logging" is selected.
   - Update the email address to that of the Avaya engineer you are working with on the problem.
   - Enable “XMPP debugging” if advised by Avaya.

   To collect the logs:
   - In the One-X Mobile application enter the Settings menu.
   - Scroll down until "Send Logs" is seen.
   - Enter the option 'System Messages".
   - Select "Report Problem" seen at the bottom of the screen.
   - Enter the details as shown in the pre-populated email.
   - Change the email address to that of the Avaya engineer you are working with on the problem [if not done above].
   - Click Send - logs are automatically archived and attached to the email.

   Note: Remember to set the logging level back to the original setting.

2.17 Applications Server Issues

1. Screenshot of the Web Control Home page showing service and system status.
2. Any debug files present in the Debug Files section of the Web Control Logs page.

2.18 Web Configuration Service Issues

1. Name and version of the application being used.
2. Devconnect certification status of the application. Details of the IP Office version it was certified against should be provided.
3. Provision of customer's web configuration service and application software to allow replication and investigation of the issue.

2.19 P DECT and DECT R4 Issues

1. Number, type and software versions of handsets
2. DECT system configuration file if available. Failing that screenshots or video capture showing significant configuration settings.
3. Tracing as specified in VoIP (H323 SIP) sections above.

2.20 D100 DECT Issues

1. The firmware version of the handsets.
2. For call issues tracing as specified in the VoIP (H323 SIP) sections above.
3. The log files from the D100 itself. The log files can be retrieved as follows:
    - Log into the base station using a browser: http://<Base Station IP Address>, user id d100, password d100
    - Navigate to "Retrieve Logs". The Critical and System logs can be opened and then saved as .txt files.

    The base station logging level should be set to 5.

4. Where handset signal is dropping out a site survey should be carried out and a plan provided showing repeater positions with associated signal strengths noted.

2.21 3rd Party Devices (E.g. GSM gateways)

1. Provision of 3rd party device to enable replication and investigation of issue.

2.22 Unified Communications Module (UCM)

1. Screenshot of the Web Control Home page showing service and system status.
2. Any debug files present in the Debug Files section of the Web Control Logs page.

2.23 IPOCC

1. Specific TTrace categories may need to be enabled as directed after initial case escalation. The following may be requested depending on the type of issue reported:

   General call routing:

   Kernel:
   - K_Routing

   MonStat statistic_srv:
   - S_CallCalc (this generates a compact summary for each call).

   Taskserver_IPO
   - TS_AgentWorkstate
   - TS_Routing
   - TS_TAPI
   - TS_TAPID
   - TS_TAPIEventing
   - TS_TSERouteServer
   - TS_TSI

   CHAP related issues:

   - CHAP_SIP_Adapter
   - CHAP_SIP_Call
   - CHAP_SIP_Controller
   - CHAP_SIP_Detail
   - CHAP_SIP_Message
   - CHAP_SIP_Media
   - CHAP_SIP_UAInterface
   - CHAP_NetworkServiceImpl
   - CHAP_VoiceServiceImpl
   - CHAP_InformationServiceImpl
   - CHAP_Adapter
   - CHAP_Controller

   IVR issues:

   - VC_Chap_Interface
   - VC_Chap
   - VC_Audio
   - VC_TSE_Interface
   - VC_TSE

   Licensing issues:

   - K_License
   - TC_LicenseDebug
   - TC_LicenseInfo

Revision History		
Version	Date	Changes
1	14 January 2013	Document Created
2	14 October 2013	Updated and corrected for IPO 9.0. Section 1.4.1 Added second requirement - Wireshark traces must be provided for a speech path, speech quality or call setup VoIP problem. Section 1.4.3 Corrected log file locations for installs on Windows 7 onwards. Section 1.4.4 Avaya Flare Communicator changed to Avaya Flare Experience. Section 1.5 Server Edition and Application Server the following changes have been made: - changes made to the files required depending on the reported problem. - updated requirements for Web Manager. - Added requirement that supplied Server Edition configs must be accompanied by the corresponding .cfi file. - Added Contact Recorder requirements for 9.0. Section 1.8 added information on where to find logs on Linux 1XP installations. Section 2.12 corrected Windows XP log file locations for 1XP Outlook plugin and added Windows 7 onwards location. Section 2.21 Added details of 1XP database location on Linux.
3	24 March 2014	Sections 1.11 and 2.30 added detailing IPOCC escalation requirements. Section 2.26 D100 logging level requirements simplified. Level 5 should be set in all cases. Section 1.5 clarified description and added details on how a core dump file can be retrieved from a Server Edition system. Added a note that a config .cfi file won't be present for a single node SE installation. Section 1.4.2 added reference to Verbose VMPro debugging previously known as level 9 tracing. Section 1.9 changed name from One-X Mobile to One-X Mobile Preferred Edition. There are no mandatory requirements for One-X Mobile Essential Edition. Added section 2.3 to cover Server Edition virtual machine deployment.
4	12 February 2015	Section 1.1.4 Changed the sentence "Details of how the problem can be reproduced." To "Written step by step instructions detailing how the problem can be reproduced". Section 1.1.5 added to request passwords for encrypted sysmon or config files.

		Section 1.2 reworded for clarity. Section 1.3 changed msinfo to msinfo32. Section 1.4.4 Added requirement for 1XP overall rolling log file to also be provided in all Flare cases. Added Section 1.4.5 Avaya Communicator. Section 1.5 vmpro_logs name has now been changed to voicemail_logs Added openfire logs for 1XP. Added Open fire logs for 9.1 1XP escalations. Conatct Recorder - added note that debug level must be set to DEBUG. Section 1.10 vmpro_logs name has now been changed to voicemail_logs. Added section detailing how to get VMPro core dump from UCM Section 1.12 added trace requirements for the Salesforce plugin. Section 1.11 IPOCC added point 7 requirement to provide IPOCC configuration .csv files. Added section 1.13 Lync Integration requirements. Section 2.4.4 TAPI added information on enabling TAPI tracing on 64-bit Operating Systems.
5	19th February 2016	Section 1.2 added the profile.ipoffice.core.txt file as a mandatory requirement in the case of a Server Edition core reboot issue. Also re-worded section to clarify that a SysMon trace is NOT a mandatory pre-requisite for a Server Edition IPO service reboot. Section 1.4.2 added the VMPro database and sysmon trace with PC voicemail events as mandatory requirements. Section 1.5 Added SysMon trace with HTTP and Web Services tracing enabled as mandatory requirements for a Web Manager problem. Section 1.11.8 Added a requirement for full details of the installed IPOCC component versions in the form of a WhatIsInstalled.exe report. Section 2.30.1 Added details of IPOCC TTrace categories that may be required for different types of problems. Removed all references to Windows XP. Removed all references to PhoneManager.
6	28 April 2016	Section 1.11.1 added requirement h) Site history details must be provided. Section 1.11 Added section 9 details of the IPOCC Server type and specification must be provided.

		Section 2.17 Corrected file locations.
7	09 November 2016	Section 1.2.2 Added requirement to provide sysmon_logs<date>.tar.gz file for SE reboots on version 10.0 onwards. Section 1.4.4 Avaya Communicator. Removed reference to Flare. Added requirement for SysMon traces with TAPI options enabled. Section 1.8 1XP restructured to add separate requirements for the Call Assistant and Outlook Plugin. Section 1.10 IPOCC added requirement 9c details of the VMWare disk provisioning settings must be provided. Section 2.17 One-X Mobile section re-written.
8	21 July 2017	Media Manager added to section 1.5 Server Edition and Application Server Issues. Section 1.9 Integrated Contact Reporter (ICR) added. Sections 1.6, 1.7, 2.20, 2.21, 2.22, 2.23, 2.24 removed and replaced as the CCR is no longer supported by CPE. Section 1.8 IPOCC added a note referring to the new log collection audit tool now provided with version 10.1. Section 2.17 updated to include instructions on how to retrieve One-X Mobile logs from an Android phone that cannot register to the One-X Portal.
9	16 May 2018	Added sections 1.10 Cloud Operations Manager and 1.11 Equinox.
10	21 Mar 2021	Document comprehensively updated to bring it in line with its internal equivalent.