



Application Notes for JPL-400B-USB Headset using JPL Gateway with Avaya Workplace Client for Windows - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate JPL-400B-USB Headset using JPL Gateway with Avaya Workplace Client for Windows.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The JPL-400B-USB Headset with JPL Gateway software allows connectivity to Avaya Workplace Client for Windows (hereafter referred to as Avaya Workplace) via a USB-A interface on the PC.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on placing calls with Avaya Workplace, answering, and ending calls using the call control button on the headset, and verifying two-way audio. The call types include calls to voicemail, local extensions, and the PSTN. Call hold and resume, mute and un-mute, and volume are also tested.

The serviceability testing focused on verifying the usability of the headset solution after restarting Avaya Workplace, restarting the PC, and reconnecting the USB cable to the PC.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and endpoints utilized enabled capabilities of TLS/SRTP.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability, or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

2.1. Interoperability Compliance Testing

All test cases were performed manually. The following features were verified:

- Placing calls to the voicemail system. Voice messages were recorded and played back to verify that the playback volume and recording level were good.
- Placing calls to internal extensions to verify two-way audio.
- Placing calls to the PSTN to verify two-way audio.
- Answering and ending calls using the call button on the headset and the soft button on Avaya Workplace.
- Using the call button on the headset and the soft button on Avaya Workplace to hold and resume the audio.
- Using the volume buttons on the headset to adjust the audio volume.
- Using the mute button on the headset and the soft button on Avaya Workplace to mute and un-mute the audio.
- Verifying incoming call notification on headset cable.
- Verifying call ended notification on headset cable.

The serviceability testing focused on verifying the usability of the headset solution after restarting Avaya Workplace, restarting the PC, and reconnecting the USB cable to the PC.

2.2. Test Results

JPL-400B-USB Headset does not support Call Control (answering and hanging-up calls) by using the headset with this solution. Only two-way audio, mute/unmute and volume control were verified successfully.

2.3. Support

For support on this JPL headset solution, contact JPL at:

- Phone: +44(0)1258 820100
- Website: <http://www.jpltele.com/>

3. Reference Configuration

- **Figure 1** illustrates the test configuration used to verify the JPL-400B-USB headset using JPL Gateway with Avaya Workplace. The configuration consists of Avaya Aura® Communication Manager running on a virtualized server with an Avaya G430 Media Gateway. Avaya Aura® Session Manager was used as the registrar/proxy for Avaya Workplace as a SIP softphone and Avaya Aura® System Manager was used to configure Session Manager. Avaya Aura® Messaging was used as the voicemail system. Avaya Aura® Media Server provided the audio media processing. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution. The JPL Gateway was installed on the PC together with Avaya Workplace. The JPL cable is connected via USB to the PC.

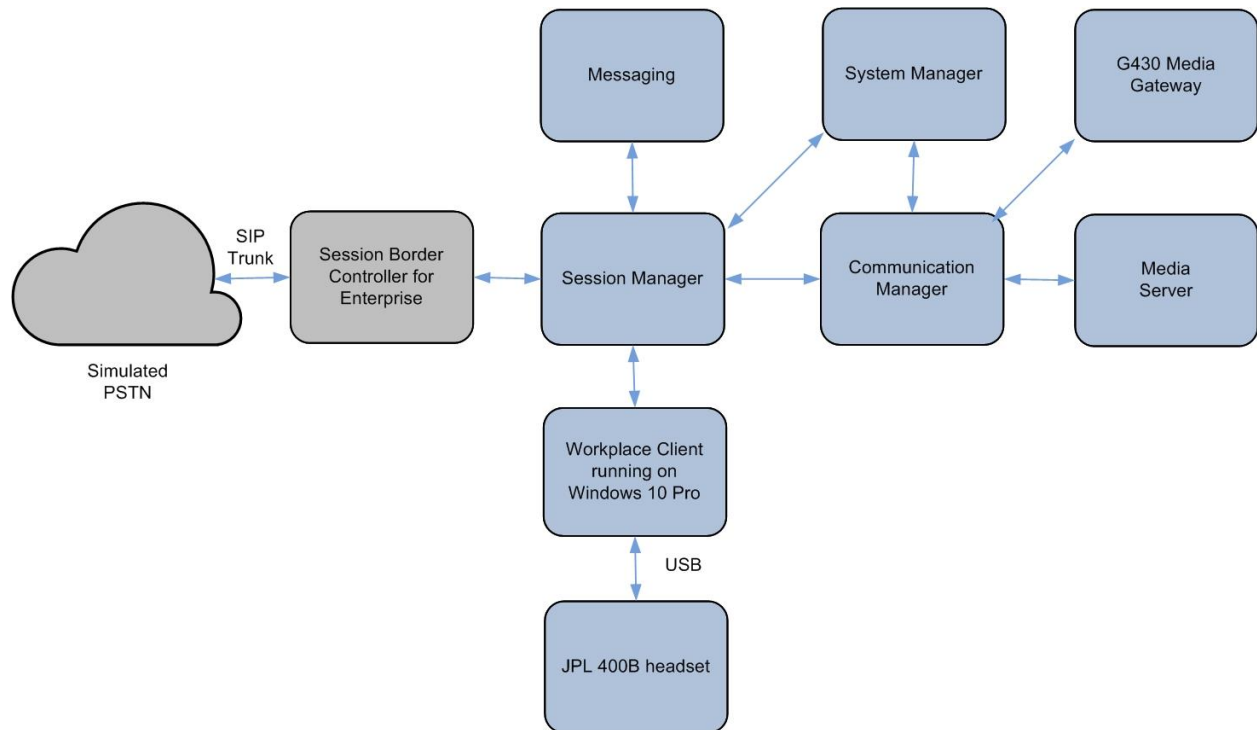


Figure 1: Test Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.3
Avaya G430 Media Gateway <ul style="list-style-type: none">• MGP	41.34.0
Avaya Aura® System Manager	8.1.3
Avaya Aura® Session Manager	8.1.3
Avaya Aura® Media Server	8.0.2.138
Avaya Aura® Messaging	7.1 SP2
Avaya Workplace Client running on Windows 10 Pro	3.12
JPL-400B-USB Headset	0254
JPL Gateway Software	2.8.1

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the verification of Communication Manager System Capacity for this solution.

It is implied a working Communication Manager system is already in place, including dial plans and SIP trunks to a Session Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 11**.

5.1. Verify System Capacity

Using Avaya Site Administrator Emulation Mode, enter the **display system-parameters customer-options** command to determine the values of user license for **Maximum Off-PBX Telephones** allowed in the system. One OPS station is required per SIP User.

```
display system-parameters customer-options                               Page 1 of 12
                                OPTIONAL FEATURES

G3 Version: V18                                                         Software Package: Enterprise
Location: 2                                                             System ID (SID): 1
Platform: 28                                                            Module ID (MID): 1

                                USED
Platform Maximum Ports: 81000    385
Maximum Stations: 41000    186
Maximum XMOBILE Stations: 41000    0
Maximum Off-PBX Telephones - EC500: 41000    1
Maximum Off-PBX Telephones - OPS: 41000    33
Maximum Off-PBX Telephones - PBFMC: 41000    0
Maximum Off-PBX Telephones - PVFMC: 41000    0
Maximum Off-PBX Telephones - SCCAN: 0    0
Maximum Survivable Processors: 313    2

(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options form**, verify that the number of **Maximum Administered SIP Trunks** and **Maximum Concurrently Registered IP Stations** supported by the system is sufficient.

If there is insufficient capacity in either one of these parameters, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	90
Maximum Concurrently Registered IP Stations:	18000	17
Maximum Administered Remote Office Trunks:	12000	0
Max Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	2
Maximum Administered SIP Trunks:	40000	38
Max Administered Ad-hoc Video Conferencing Ports:	24000	0
Max Number of DS1 Boards with Echo Cancellation:	999	0

(NOTE: You must logoff & login to effect the permission changes.)

6. Configure Avaya Aura® Session Manager

This section describes aspects of the Session Manager configuration required for Avaya Workplace to register. It is assumed that the Domains, Locations, SIP entities, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured where appropriate for Communication Manager, Session Manager and Aura® Messaging.

Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

6.1. Verify Session Manager Ports for SIP endpoint registration

Each Session Manager Entity must be configured so that the SIP endpoint can register to it. From the home page, under **Elements**, click **Routing → SIP Entities** (not shown) and select the Session Manager entity used for registration. Make sure that **TCP**, **UDP** and **TLS** entries are present under **Listen Ports**. During the compliance test, Avaya Workplace registered to the Session Manager using TLS transport.

Listen Ports		Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	sglab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	sglab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	sglab.com	<input checked="" type="checkbox"/>	

Select : All, None

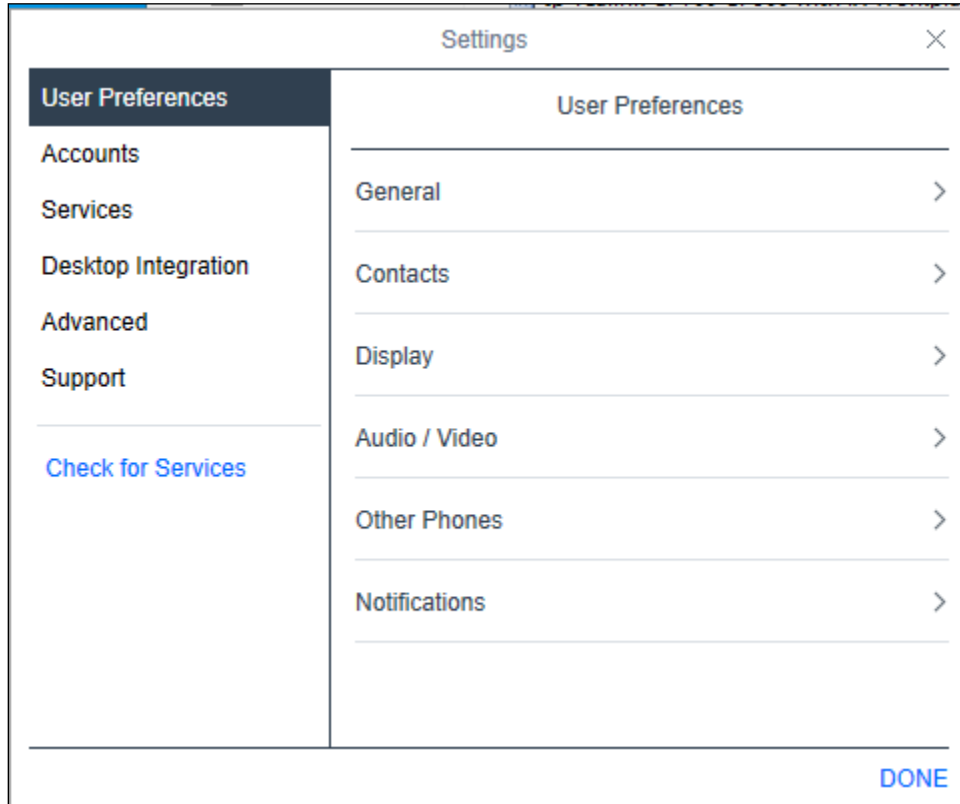
6.2. Add SIP User




The addition of SIP User will not be detailed here. Refer to details in adding user in the administration document for Avaya Aura® Session Manager in **Section 11**.

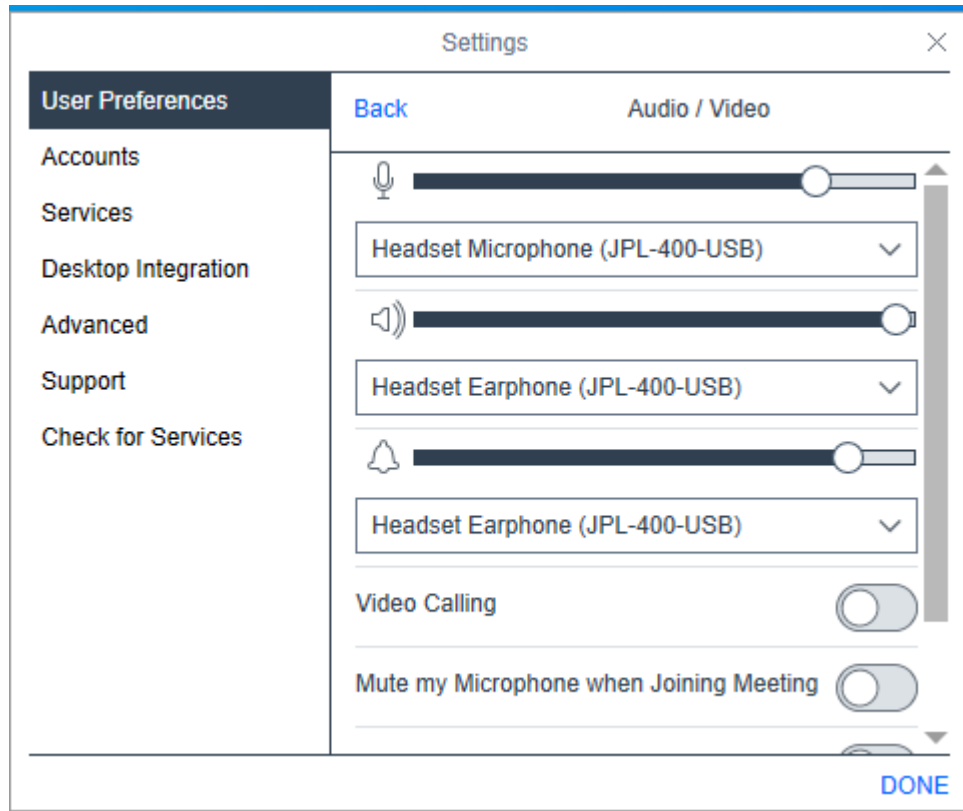
7. Configure Avaya Workplace Client for Windows

Avaya Workplace is a SIP softphone application that provides users with access to Unified Communications (UC) services. This section shows how to configure Avaya Workplace to use with the JPL-400B-USB Headset.

From Avaya Workplace, navigate to **Settings** → **User Preferences** → **Audio/Video**.



Select **Headset Microphone (JPL-400-USB)** for *Microphone*  and **Headset Earphone (JPL-400-USB)** for *Speaker*  as shown below. It is optional for *Ringing on incoming calls*  to be set.



8. Configure JPL-400B-USB headset Solution

This section covers the steps to integrate JPL-400B-USB headset with Avaya Workplace, including:

- Install the JPL Gateway software
- Connect JPL cable

Note: After successfully performing this procedure, the JPL-400B-USB headset will be detected in Avaya Workplace as described in **Section 7**.

8.1. Install the JPL Gateway Software

JPL Gateway software can be obtained from JPL support portal at <https://www.jpltele.com/default.aspx>. Installation of the software is done through executing the setup file and following the prompt.

8.2. Connect JPL Cable

Plug the JPL-400B-USB headset cable into the USB-A port of the PC. The device drivers will automatically be installed.

Open the JPL Gateway program installed on the PC. It shows the **Device ready for use** for the **JPL-400-USB**.

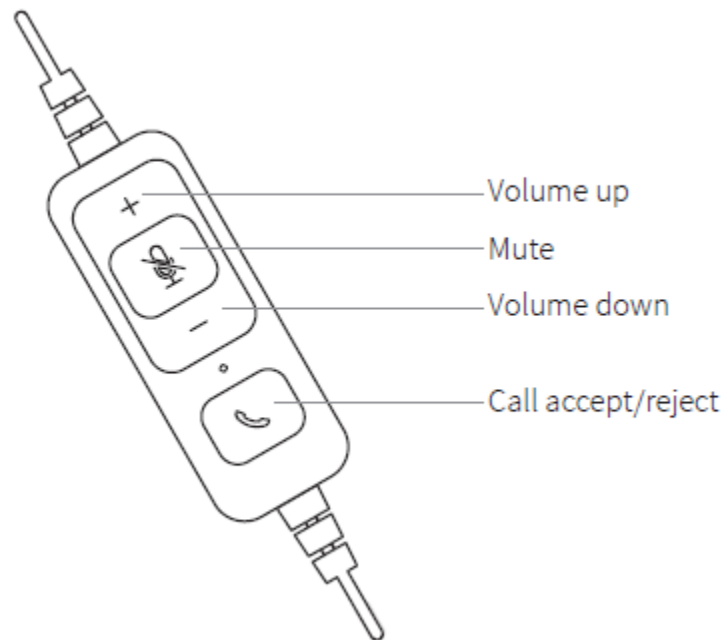


9. Verification Steps

This section verifies that the JPL-400B-USB headset has been successfully integrated with Avaya Workplace.

1. Open the JPL Gateway program to verify that the JPL cable has been successfully connected for use with Avaya Workplace as in **Section 8.2**.
2. Make incoming and outgoing calls and verify that calls can be established with two-way audio. For incoming calls, answer the call with the Avaya Workplace.
3. End the call by hanging up on the Avaya Workplace.
4. Verify also that user is able to remotely control call functions such as mute/un-mute, hold/resume and adjust the volume on the Avaya Workplace. Similarly, verify the same thing on the headset (see diagram below).

Note: JPL-400B-USB headset does not support call control functions as mentioned in **Section 2.2**. Call answer/end button will not work in this case.



10. Conclusion

These Application Notes describe the configuration steps required to integrate JPL-400B-USB Headset using JPL Gateway with Avaya Workplace Client for Windows. All test cases were executed with observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and JPL documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, Mar 2020
- [2] *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac and Windows*, Sep 25, 2020.
- [3] *Using Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*, Aug 4, 2020.
- [4] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, Aug 2020.

The following JPL documentation can be found at <http://www.jpltele.com/>.

- [1] *JPL-400 Data Sheet 2019*.

©2021 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.