



Application Notes for EPOS Connect and EPOS IMPACT D Series wireless DECT Headset with Avaya Workplace Client for Windows - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate EPOS Connect and EPOS IMPACT D Series wireless DECT Headset 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 EPOS IMPACT D Series wireless DECT Headset together with EPOS Connect software allows connection and call control of Avaya Workplace Client for Windows (hereafter referred to as Avaya Workplace) using a cable via the USB interface to the PC. The EPOS Connect is a collection of programs that enable remote call control with EPOS headsets and Avaya Workplace for Windows. With an EPOS headset connected to the PC USB interface, users can directly answer, end, mute/unmute and adjust volume with the headset.

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 EPOS headset, and verifying two-way audio. The call types include calls to voicemail, local extensions, and the PSTN. Auto-answer, call hold and resume, mute and un-mute, and volume are also tested.

The serviceability testing focused on verifying the usability of the EPOS headset solution after restarting the Avaya Workplace, restarting the PC, reconnecting the headset USB cable to the PC and moving away from DECT range.

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 control button on the headset, and the soft button on Avaya Workplace.
- Using 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, and verifying the mute status.
- Verifying incoming call notification.
- Verifying call ended notification.

The serviceability testing focused on verifying the usability of the headset solution after restarting the Avaya Workplace, restarting the PC, reconnecting the USB interface to the PC and moving away from DECT range.

2.2. Test Results

All test cases were completed successfully.

2.3. Support

For support on this EPOS headset solution, contact EPOS Technical Support below where sign-in is required:

- Website: <https://eposaudio.com/support/>

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the EPOS Connect and EPOS IMPACT D Series wireless DECT headset with Avaya Workplace. The EPOS Connect software were installed on the PCs together with Avaya Workplace. The EPOS headsets are connected via a cable into the PCs' USB interface. The following EPOS IMPACT D Series wireless DECT headsets are tested:

- IMPACT D10 USB ML
- IMPACT D30 USB ML

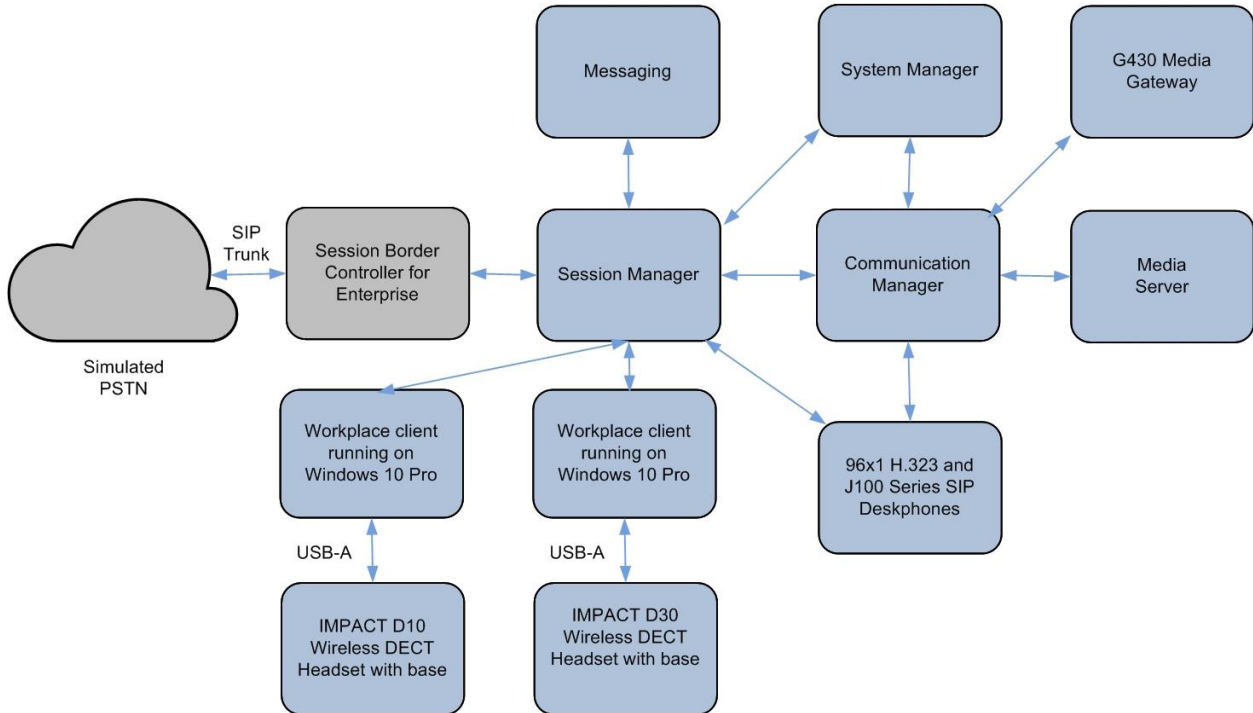


Figure 1: Test Configuration

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	10.1.0 (10.1.0.0.974.27247)
Avaya G430 Media Gateway	42.4.0
Avaya Aura® System Manager	System Manager 10.1.0.0 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Aura® Session Manager	10.1.0 (10.1.0.0.1010019)
Avaya Aura® Media Server	8.0.2.218
Avaya Messaging	10.8 SP1SU2
Avaya 96x1 Series H.323 Deskphones	6.8511
Avaya J100 Series SIP Deskphones	4.0.11.0
Avaya Workplace Client running on Windows 10 Pro	3.25
EPOS IMPACT D Series wireless DECT Headsets <ul style="list-style-type: none">• IMPACT D10 USB ML• IMPACT D30 USB ML	182 182
EPOS Connect for Windows	7.1.0.24484

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 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.

<input type="checkbox"/>	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

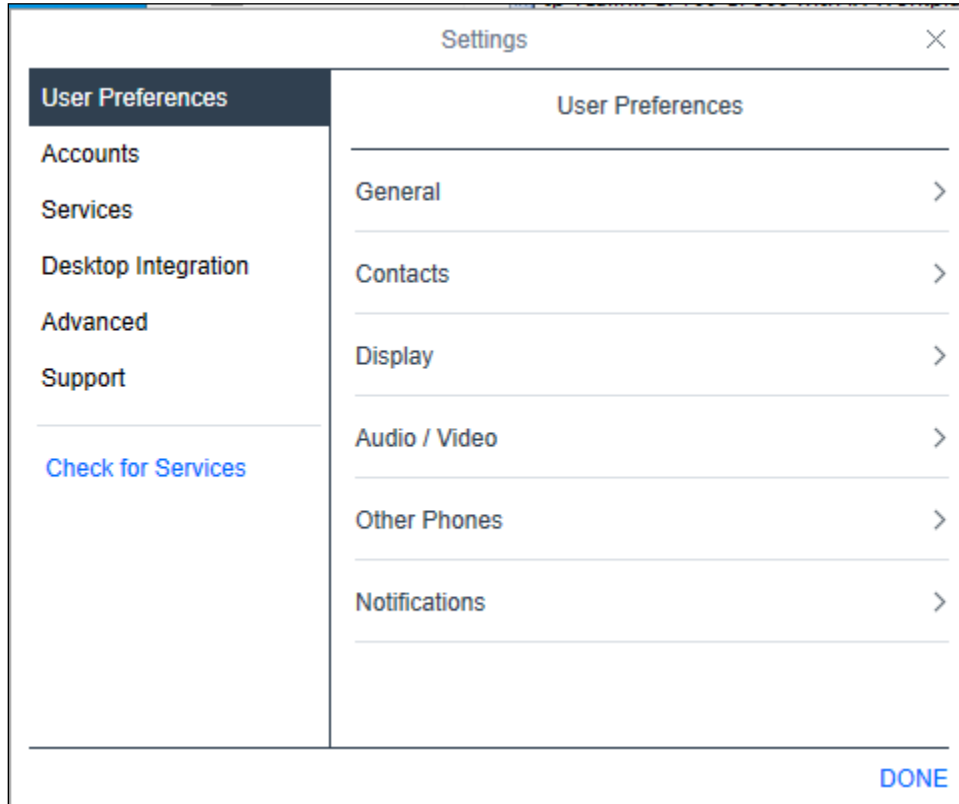
6.2. Add SIP User




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 [4].

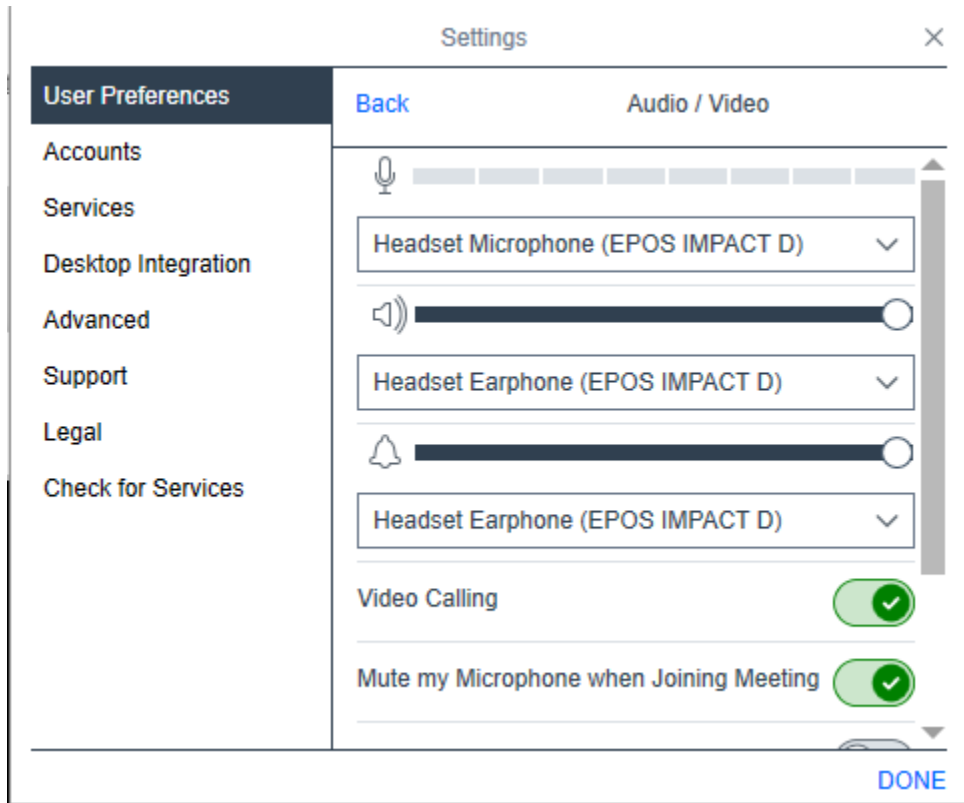
7. Configure Avaya Workplace

Avaya Workplace is a SIP soft phone application that provides users with access to Unified Communications (UC) services. This section shows how to configure the EPOS IMPACT D Series wireless DECT to use with Avaya Workplace.

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



Select *EPOS IMPACT D* for Microphone  and the same for Speakers  as shown below assuming IMPACT D30 is used. It is optional for Ringing on incoming calls  to be set as *EPOS IMPACT D*.



8. Configure EPOS IMPACT D Series wireless DECT headset Solutions

This section covers the steps to integrate EPOS IMPACT D Series wireless DECT headset with Avaya Workplace, including:

- Installing the EPOS Connect Software
- Connect the EPOS headset
- Configuring EPOS headset with EPOS Connect

Note: After successfully performing this procedure, the EPOS headset will be detected in Avaya Workplace as described in **Section 7**.

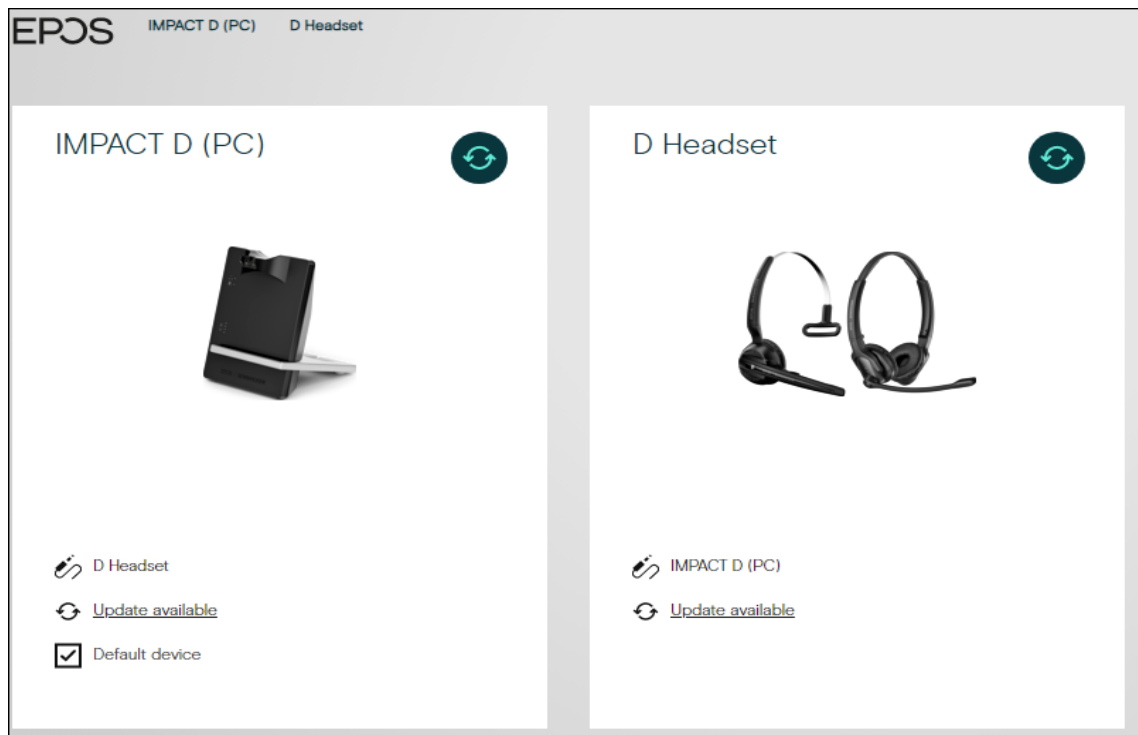
8.1. Installing the EPOS Connect Software

EPOS Connect software can be obtained from EPOS support portal at <https://eposaudio.com/support/>. Installation of the software is done through executing the .exe file and following the prompt.

8.2. Connect the EPOS headset

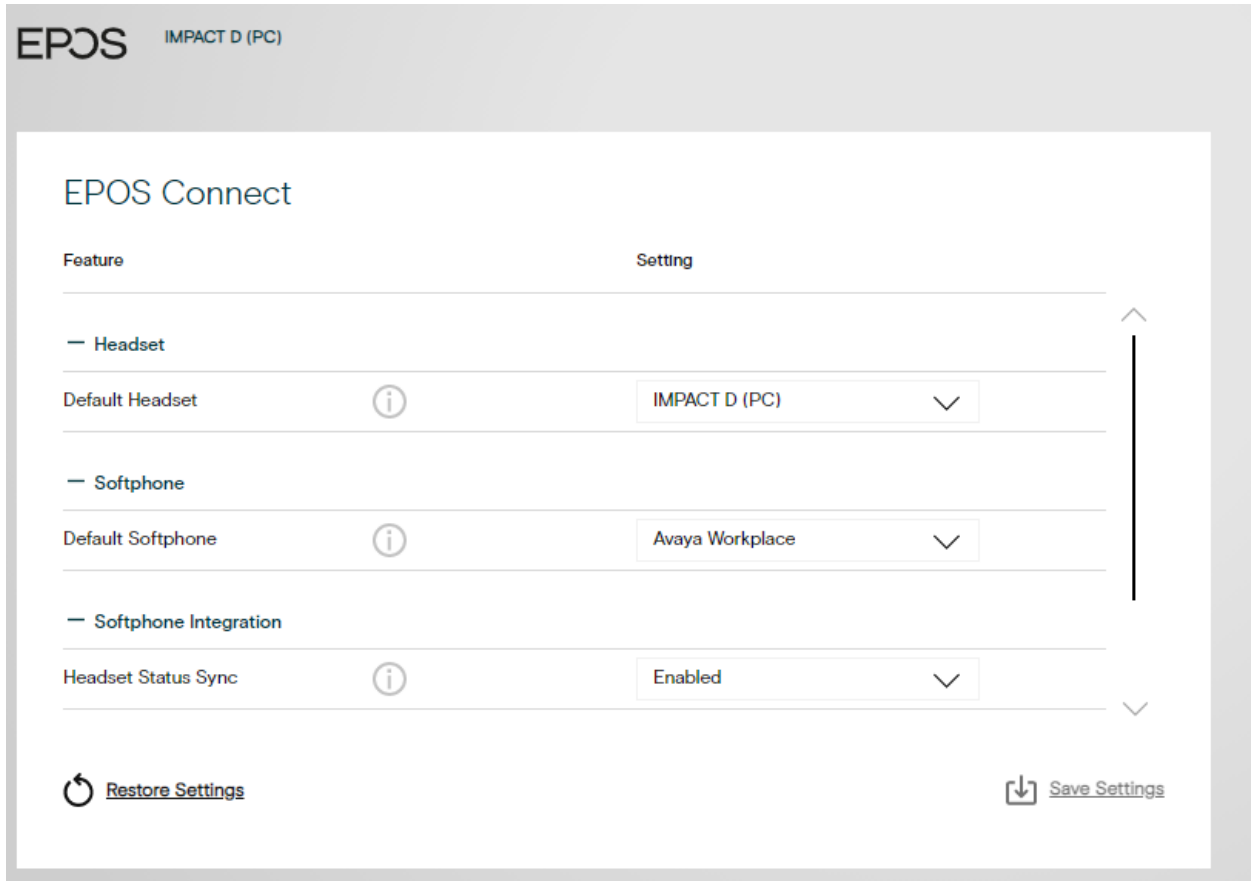
Plug the EPOS IMPACT D Series wireless DECT headset base into the USB port of the PC. The device drivers will automatically be installed.

Open the EPOS Connect program installed on the PC. Select the **Home** icon and check that the headset is detected as shown below which is for one of the headset IMPACT D30 USB ML tested.



8.3. Configuring EPOS headset with EPOS Connect

Open the Avaya Workplace program and click EPOS Connect program **Settings** at the bottom (not shown). Verify the **Default Headset** is properly detected. Check that the **Default Softphone** is set as **Avaya Workplace**. Otherwise, click the drop-down menu of **Default Softphone** to select. Click **Save Settings** at the bottom right to retain it.

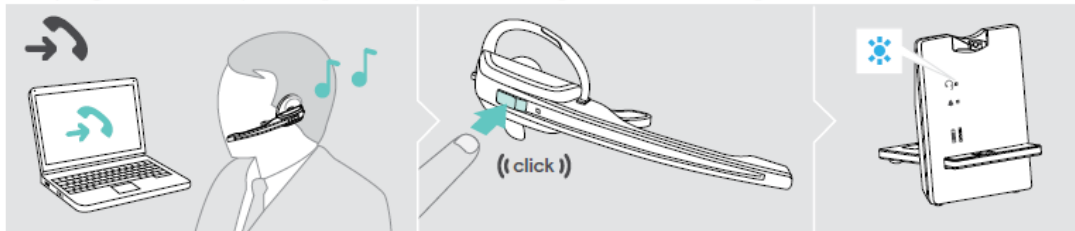


9. Verification Steps

This section verifies that the EPOS solution has been successfully integrated with Avaya Workplace.

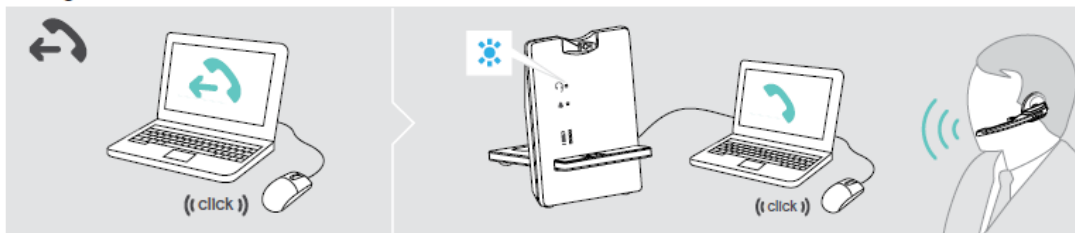
1. Open the EPOS Connect program to verify that the headset has been successfully connected to PC for use with Avaya Workplace running. Observed that EPOS IMPACT D Series wireless DECT headset is detected as detailed in **Section 8.2**.
2. Make incoming and outgoing calls and verify that calls can be established with two-way audio. For incoming calls, answer the call by pressing the call control button on the headset (as shown below for D10 USB ML).
3. End the call by pressing the same call control button on the headset.
4. Verify also that the headset is able to remotely control call functions such as mute/unmute and adjust the volume. Similarly, verify such call control functions could be done on the Avaya Workplace.

Accepting a call: The softphone signals that you are receiving a call. You hear a ring tone in the headset.



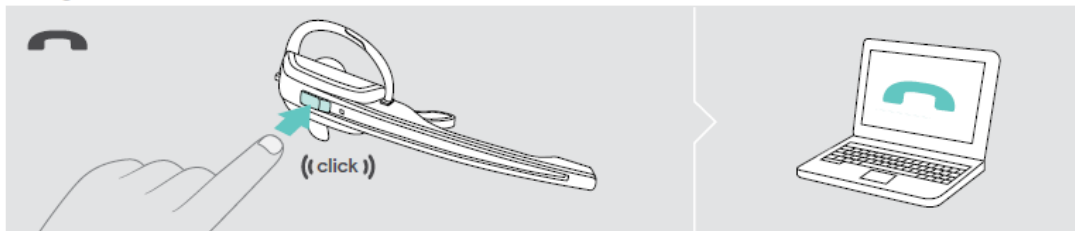
▷ Press the Link button on the headset to accept the call.

Making a call:



▷ Start the call using your softphone, the audio signal is automatically transmitted to the headset.

Ending a call:



▷ Press the Link button. If the other party hangs up, your softphone and your headset become automatically ready to receive the next call.

10. Conclusion

These Application Notes describe the configuration steps required to integrate EPOS Connect and EPOS IMPACT D Series wireless DECT Headset with Avaya Workplace Client for Windows. All test cases were completed successfully.

11. Additional References

This section references the Avaya and EPOS 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 10.1, Issue 1, Dec 2021.

[2] *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac and Windows*, May 31, 2021.

[3] *Using Avaya Workplace Client for Android, iOS, Mac, and Windows*, May 31, 2021.

[4] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 1, Dec 2021.

The following EPOS documentation can be found at <http://www.eposaudio.com>.

[5] *EPOS IMPACT D Series User Guide*.

©2022 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.