



Avaya Solution & Interoperability Test Lab

Application Notes for Journey Identity Platform with Avaya Experience Portal – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Journey Identity Platform 3.0.114 with Avaya Experience Portal 8.1. Avaya Experience Portal answers inbound calls from mobile phones to the call center and begins the process of authenticating the caller using caller ID or Automatic Number Authentication (ANI). Avaya Experience Portal provides the caller's ANI to the Journey Identity Platform, a cloud-based solution, via the Journey REST API, which in turn verifies the caller against a customer database. After the caller is verified as a current customer, Avaya Experience Portal transfers the call to an available agent.

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

These Application Notes describe the configuration steps required to integrate the Journey Identity Platform with Avaya Experience Portal. A sample application on Avaya Experience Portal answers inbound calls from mobile phones to the call center and begins the process of authenticating the caller using caller ID or Automatic Number Authentication (ANI). Avaya Experience Portal provides the caller's ANI to the Journey Identity Platform, a cloud-based solution, via the Journey REST API, which determines if the caller is a current customer. If the caller is a current customer, the Journey Identity Platform sends a push notification directly to the caller's mobile phone requesting the caller to sign into the Journey mobile app using onboard biometrics. Once the caller is authenticated, Avaya Experience Portal transfers the call to an available agent by calling a Vector Directory Number (VDN). This is the focus of these Application Notes.

The Journey Identity Platform can also securely collect and verify Personal Identifiable Information (PII) provided by the customer using onboard biometrics from a Journey mobile app when a customer is interacting with services, such as banking, that require a higher level of proof of identity. In addition to the Journey Identity Platform communicating with Avaya Experience Portal, the Journey Identity Platform can communicate directly with a business's mobile app, using the Journey mobile SDK, running on the caller's mobile phone and a Journey screen pop on the agent desktop¹ using encrypted data channel. After the caller has been authenticated, the Journey Identity Platform provides the caller's authentication status to the agent via a screen pop on the agent desktop and also provides the agent's identity credentials to the caller so the caller knows with whom they are speaking.

The agent can request additional PII from the caller via the screen pop, which triggers a push notification from the Journey Identity Platform to the caller's mobile phone. The caller can then provide the requested information via the business's mobile app, which is verified by the Journey Identity Platform using a customer database. The verification status of the data the customer entered is then provided to the agent via the screen pop on the agent desktop while part of the customer data is masked for privacy. If the verification fails, the agent can request the data again.

The configuration to support this verification process between the Journey Identity Platform, the Journey mobile app, and the screen pop on the agent desktop is outside the scope of these Application Notes, but is mentioned because it is a key feature of the Journey solution.

¹ For information on the agent desktops supported by the Journey Identity Platform, contact Journey as detailed in Section 2.3.

2. General Test Approach and Test Results

The feature test cases were performed manually. Inbound calls from a mobile phone to a call center were answered by a sample application on Experience Portal, which began the process of authenticating the caller's ANI. Experience Portal used the Journey REST API to request the Journey Identity Platform to verify the ANI against a customer database. After the caller was verified as a current customer, Experience Portal transferred the call to an available agent. If the caller couldn't be verified, the call was still transferred to an agent.

Once the call was delivered to an agent, the agent requested additional customer data via the screen pop on the agent desktop. The Journey Identity Platform sent the push notification to the caller's mobile phone to collect the data and verify it. The verification status was then provided to the agent desktop via the screen pop. This part of the testing didn't involve Experience Portal. It was an interaction between the Journey Identity Platform, the Journey mobile app, and the screen pop on the agent desktop. This feature was exercised as part of the complete Journey solution.

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 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.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Sample application on Experience Portal using the Journey REST API to request the Journey Identity Platform to verify the caller's ANI against a customer database.
- After verifying the caller's ANI, whether it passed or failed, the sample application on Experience Portal transferring the call to an agent.
- After connecting the agent, Journey Identity Platform presenting the call in the Journey screen pop on the agent desktop with the caller's verification status.
- Journey Identity Platform sending push notification to caller's mobile phone running the Journey mobile app with connected agent's identification.
- Agent requesting additional customer information via the Journey screen pop.

- Journey Identity Platform sending push notifications to caller's mobile phone requesting more information from caller.
- Caller submitting additional information via the Journey mobile app.
- Journey Identity Platform verifying the customer data against the customer database and providing the verification status to the agent via the Journey screen pop.
- Ending the conversation between the Journey screen pop and the Journey Identity Platform.

2.2. Test Results

All test cases passed.

2.3. Support

For information on the Journey Identity Platform, contact Journey through one of the following:

- **Website:** <https://journeyid.com/contact/>
- **Email:** info@journeyid.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of the Journey Identity Platform (cloud-hosted) with an Avaya Aura® Contact Center. Caller places an inbound call from the PSTN to the call center from a mobile phone running the Journey mobile app. The call is routed to Experience Portal through Avaya Session Border Controller for Enterprise (SBCE) and Avaya Aura® Session Manager. The call is answered by a sample application on Experience Portal. The sample application communicates with the cloud-based Journey Identity Platform via the Journey REST API to verify the caller's ANI. The Journey Identity Platform verifies the ANI against a customer database (not shown). The sample application then transfers the call to an available agent by calling a VDN on Avaya Aura® Communication Manager. The call is delivered to the agent on Avaya Agent for Desktop and an agent desktop with a Journey screen pop. The agent desktop solution monitors the call center via TSAPI link on Avaya Aura® Application Enablement Services. The agent can then use the Journey screen pop to request additional information from the caller through the Journey Identity Platform. The Journey Trusted Identity Platform communicates directly with Experience Portal, the Journey mobile app, and the Journey screen pop on the agent desktop using an encrypted data channel. However, these Application Notes will focus on the interaction between the Journey Identity Platform and Experience Portal.

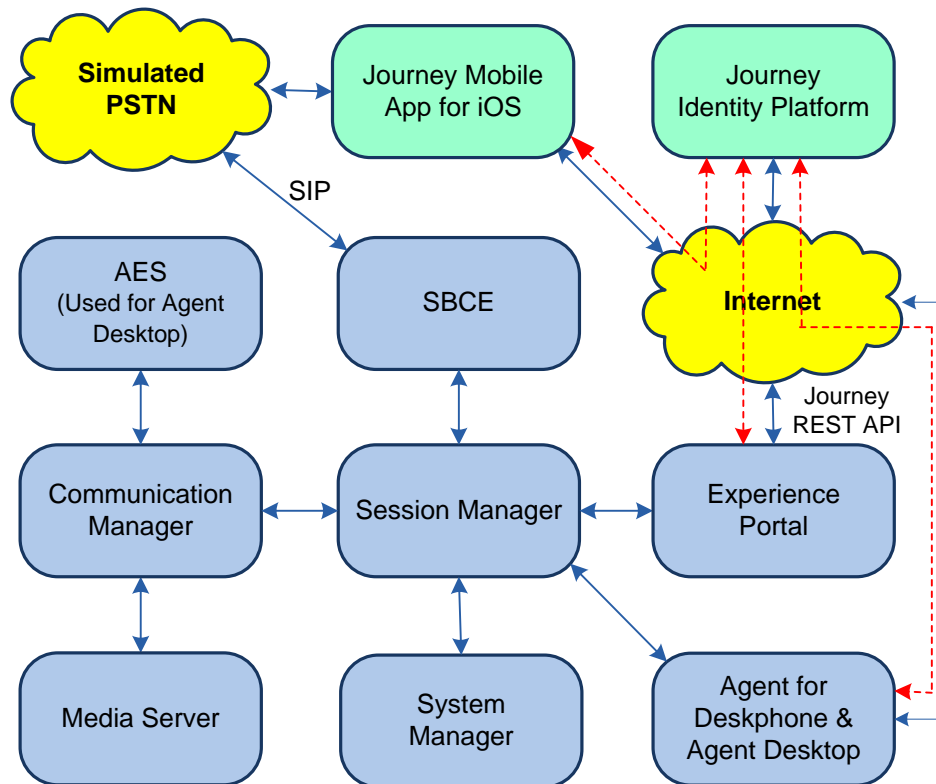


Figure 1: Journey Identity Platform (cloud-based) with Avaya Experience Portal

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	8.0.1.2.0-FP1SP2
Avaya Aura® Media Server	v.8.0.2.184
Avaya Aura® System Manager	8.0.1.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.0.038826 Feature Pack 1
Avaya Aura® Session Manager	8.0.1.0.801007
Avaya Session Border Controller for Enterprise	8.1.3.0-31-21052
Avaya Aura® Experience Portal	8.1.0.0.0223
Avaya Aura® Application Enablement Services	8.1.3.1.0.7-0
Avaya Agent for Desktop	2.0.6.14.3002
Journey Identity Platform	3.0.114
Journey Mobile App on iOS	2021.08 (23.20)

5. Configure Avaya Aura® Communication Manager

This section covers the configuration of a sample call center on Communication Manager, including the VDN, Vector, and Hunt Group. Administration of Communication Manager was performed using the System Access Terminal (SAT).

For the compliance test, agents logged into a skill/hunt group using agent login IDs. For example, an agent with Agent for Desktop and an agent desktop logged into hunt group 65 using agent login ID 3000. The configuration of SIP stations for Agent for Desktop and the agent login IDs are not shown in these Application Notes.

5.1. Administer VDN

The sample application on Experience Portal transfers the caller to an agent by calling a VDN. To add a VDN, use the **add vdn** command. Enter a descriptive **Name** and the vector number from **Section 0** for **Destination**. Set the **1st Skill** to the hunt group configured in **Section 5.3**. Retain the default values for all remaining fields.

```
add vdn 5001003                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
                                         Extension: 500-1003          Unicode Name? n
                                         Name*: CC VDN
                                         Destination: Vector Number    65
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: external Report Adjunct Calls as ACD*? N

VDN of Origin Annc. Extension*:
1st Skill*: 65
2nd Skill*:
3rd Skill*:

SIP URI:

*Follows VDN Override Rules
```

5.2. Administer Vector

The VDN configured in **Section 5.1** will invoke the following vector to queue the call to a hunt group. The call will be queued to the 1st Skill specified in the VDN. Modify an available vector using the **change vector** command.

```
display vector 65                                     Page 1 of 6
CALL VECTOR
Number: 65 Name: Call Center
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 queue-to skill11st pri m
02 wait-time 5 secs hearing ringback
03 goto step 1 if unconditionally
04
05
06
07
08
09
10
11
12
Press 'Esc f 6' for Vector Editing
```


5.3. Administer Hunt Group

The sample application on Experience Portal transfers calls to an available agent logged into the following hunt group. To add a hunt group, use the **add hunt-group** command.

add hunt-group 65	HUNT GROUP	Page 1 of 4
Group Number: 65	ACD? y	
Group Name: Call Center	Queue? y	
Group Extension: 3701	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold: Port:		
Time Warning Threshold: Port:		
SIP URI:		

On Page 2 of the hunt group form, set **Skill** to 'y' as shown below.

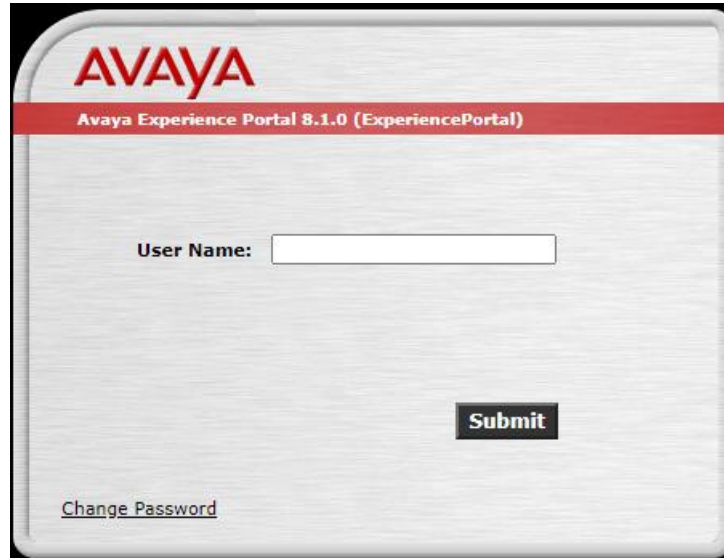
add hunt-group 65	HUNT GROUP	Page 2 of 4
Skill? Y	Expected Call Handling Time (sec): 180	
AAS? N	Service Level Target (% in sec): 80in 20	
Measured: external		
Supervisor Extension:		
Controlling Adjunct: none		
Multiple Call Handling: none		
Timed ACW Interval (sec): 10 After Xfer or Held Call Drops? N		

6. Configure Avaya Aura® Experience Portal

This section covers the configuration of a sample VXML application in Experience Portal using the Experience Portal Manager (EPM) web interface.

6.1. Launch Experience Portal Manager

Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://<ip-addr>** as the URL in a web browser, where <ip-addr> is the IP address of EPM. Log in using the appropriate credentials.

The image shows the login interface for the Avaya Experience Portal 8.1.0. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Avaya Experience Portal 8.1.0 (ExperiencePortal)". The main area is light gray and contains a "User Name:" label followed by a white text input field. Below the input field is a black "Submit" button. At the bottom left, there is a link labeled "Change Password".

The main page of the EPM web interface is displayed as shown below.

AVAYA Welcome, cust
Last logged in today at 10:36:47 AM CDT

Avaya Experience Portal 8.1.0 (ExperiencePortal) Home ? Help Logoff
Expand All | Collapse All

You are here: Home

Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

Proactive Outreach Manager
Avaya Proactive Outreach Manager (POM) provides a solution for unified, multichannel, inbound and outbound architecture, with the capability to communicate through different channels of interaction, from Short Message Service (SMS) to e-mail to the traditional voice.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: June 1st, 2020

THESE GLOBAL SOFTWARE LICENSE TERMS ("SOFTWARE LICENSE TERMS") GOVERN THE USE OF PROPRIETARY SOFTWARE AND THIRD- PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, THE END USER, ON BEHALF OF THEMSELF AND THE ENTITY FOR WHOM THEY ARE DOING SO (HEREINAFTER REFERRED TO AS "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN END USER AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF THE END USER IS ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THE END USER REPRESENTS THAT THEY HAVE THE AUTHORITY TO

6.2. Add Application

This section covers the configuration of a sample VXML application that answers inbound calls to the call center. It will send a request to the Journey Identity Platform to verify the caller's ANI as a current customer and then transfer the call to an agent.

On the left pane, navigate to **System Configuration → Applications**. The **Applications** page is displayed (not shown). Click **Add** to add the application. Note that the following **Change Application** page shows the VXML application that was already configured.

- **Name:** Provide a descriptive name (e.g., *WFinbound*).
- **Enable:** Set to **Yes** to enable the application.
- **Type:** Set to *VoiceXML*.
- **VoiceXML URL:** Specify the VXML application URL. For the compliance test, the application was located in an application server co-resident on the EPM server.
- **ASR Speech Servers:** Select a previously configured ASR speech server.
- **Selected Languages:** Select the language (e.g., *English(USA) en-US*).

AVAYA Welcome, cust
Last logged in today at 10:36:47 AM CDT

Avaya Experience Portal 8.1.0 (ExperiencePortal) Home ? Help Logoff

Expand All | Collapse All

▼ User Management
Roles
Users
Login Options

▼ Real-time Monitoring
System Monitor
Active Calls
Port Distribution

▼ System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

▼ System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

▼ System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

▼ Security
Certificates
Licensing

▼ Reports
Standard
Custom
Scheduled

▼ Multi-Media Configuration
Email
HTML
SMS

▼ POM
POM Home
POM Monitor

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > Change Application

Change Application

Use this page to change the configuration of an application.

Name: WFinbound

Enable: ☒ Yes ☐ No

Type:

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

ASR Speech Servers ▼

Engine Types

ASR:

Selected Engine Types

LumenVox

Languages

Selected Languages

Scroll down to the TTS Speech Servers section and configure a previously configured TTS speech server. Select a supported TTS voice (e.g., *English(USA) en-US Jennifer F*).

In the **Application Launch** section, set the **Called Number** associated with the application and click **Add**. The called number will be added to the text below the field. This is number to be dialed by callers.

The screenshot displays the Avaya Experience Portal 8.1.0 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message, and a 'Last logged in today at 10:36:47 AM CDT' timestamp. The sidebar on the left lists various management categories: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'TTS Speech Servers' and contains several sections:

- TTS:** A dropdown menu set to 'Nuance'.
- Voices:** A list box showing '<None>'.
- Selected Voices:** A list box showing 'English(USA) en-US Jennifer F'.
- Application Launch:** A section with radio buttons for 'Inbound', 'Inbound Default', and 'Outbound'. Below this, there are radio buttons for 'Number', 'Number Range', and 'URI'. The 'Number' option is selected.
- Called Number:** A text input field with an 'Add' button next to it.
- Remove:** A button next to a list of numbers (888, 1888, 682) that have been added.
- SIP Header Source:** A dropdown menu set to 'Any'.
- Speech Parameters:** A section with a right-pointing arrow.
- Reporting Parameters:** A section with a right-pointing arrow.
- Advanced Parameters:** A section with a right-pointing arrow.
- Buttons:** At the bottom of the main content area, there are four buttons: 'Save', 'Apply', 'Cancel', and 'Help'.

Scroll down and expand the **Advanced Parameters** section and configure the following parameters:

- **Generate UCID:** Set to *Yes*.
- **Operation Mode:** Set to *Shared UI*.
- **Transport UCID in Shared Mode:** Set to *Yes*.
- **Maximum UI Length:** Use default value of *128*.

The screenshot displays the Avaya Experience Portal 8.1.0 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, a welcome message for 'cust', and a timestamp 'Last logged in today at 10:36:47 AM CDT'. The main menu on the left lists various sections: User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, Multi-Media Configuration, and POM. The 'Advanced Parameters' section is expanded, showing a list of configuration options. The 'Generate UCID' is set to Yes, 'Operation Mode' is set to Shared UI, 'Transport UCID in Shared Mode' is set to Yes, and 'Maximum UI Length' is set to 128. Other settings include 'Support Remote DTMF Processing' (No), 'DTMF Type Ahead Enabled' (Yes), 'Converse-On' (No), 'Network Media Service' (No), 'Early Media' (No), 'Sync FROM and PAI Headers' (No), 'Dialog URL Pattern' (empty), 'VoiceXML Event Handler' (Default), 'CCXML Event Handler' (Default), 'Fax Detection Enabled' (No), 'Fax Phone Number' (empty), 'Video Enabled' (No), 'Video Screen Format' (QCIF), and 'Video Minimum Picture Interval' (2). The bottom of the configuration panel has buttons for 'Save', 'Apply', 'Cancel', and 'Help'.

7. Configure Journey Identity Platform

The configuration of the Journey Identity Platform isn't covered in these Application Notes since it is configured by Journey. This includes the configuration of the Journey screen pop on the agent desktop and providing the Journey mobile app to customers.

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Experience Portal and Journey Identity Platform.

8.1. Avaya Aura® Communication Manager

Verify that an agent is logged into the hunt group using the **list agent-loginID** command. The following example shows agent login ID 3000 logged into hunt group 65.

```
list agent-loginID 3000
```

AGENT LOGINID									
Login ID		Name		Extension		Dir	Agt	AAS/AUD	COR AgPr SO
		Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
3000		Pat Jones		200-0001				1	lvl
1/01	2/01	4/01	65/01	/	/	/	/		

8.2. Avaya Experience Portal

This section provides the verification steps that may be performed to verify that Experience Portal MPP and its ports are in-service.

From the EPM web interface, verify that the MPP server is online by navigating to **System Management → MPP Manager**. The **Mode** of the MPP should be *Online* and the **State** should be *Running*.

Welcome, cust

Last logged in yesterday at 3:22:41 PM CDT

Avaya Experience Portal 8.1.0 (ExperiencePortal)

Expand All | Collapse AllHome Help Logout

You are here: [Home](#) > System Management > MPP Manager

[Refresh](#)

MPP Manager (Sep 24, 2021 9:20:41 AM CDT)

This page displays the current state of each MPP in the Experience Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: Sep 24, 2021 9:20:28 AM CDT

<input type="checkbox"/>	Server Name	Mode	State	Config	Auto Restart	Restart Schedule Today Recurring	Active Calls In Out
<input type="checkbox"/>	mppco-res	Online	Running	OK	Yes	No None	0 0

State Commands

Start Stop Restart Reboot Halt Cancel

Restart/Reboot Options

☒ One server at a time
☐ All servers

Mode Commands

Offline Test Online

Help

From the EPM web interface, verify that the ports on the MPP server are in service in the by navigating to **Real-time Monitoring → Port Distribution** and selecting the MPP in the **Port Distribution** page (not shown).

AVAYA Welcome, cust
Last logged in yesterday at 3:22:41 PM CDT

Avaya Experience Portal 8.1.0 (ExperiencePortal) Home Help Logoff

Expand All | Collapse All

You are here: [Home](#) > [Real-Time Monitoring](#) > [Port Distribution](#) > Port Distribution Report

Port Distribution Report (Sep 24, 2021 9:28:05 AM CDT) Refresh

This page displays information about how the telephony resources have been distributed to the MPPs. You configure the telephony resources on the VoIP Connections page.

Servers: mppco-res
Total Ports: 10 Last Poll: Sep 24, 2021 9:28:03 AM CDT

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
10	Online	In service	asm	SIP_Trunk	mppco-res	

Help

Verify that the **Speech Servers** are UP. Navigate to **Real-time Monitoring → System Monitor** and select the **ExperiencePortal Details** tab. Click on the **MPP**. In the **MPP Details** page, click **Service Menu**. Finally, navigate to **Resources → Speech Servers** in the left pane to view the status of the speech servers as shown below. The **Status** of the speech servers should be **UP**.

8.3. Journey Identity Platform

To verify the Journey Identity Platform is operational, follow these steps:

1. From a mobile phone running the Journey mobile app, place an inbound call to the sample application on Experience Portal
2. Verify that the sample application provides a greeting to the caller indicating to the caller that the system is checking if they're a current customer.
3. Verify that caller is verified and that the Journey Identity Platform sends a push notification to the mobile phone requesting the caller to sign into the Journey mobile app to complete the authentication.
4. Verify the sample application transfers the caller to an available agent.
5. Verify the Journey screen pop on the agent desktop indicates that the caller has been verified.
6. Verify that the agent can request additional customer information via the Journey screen pop and the data can be verified by the Journey Identity Platform.
7. Verify the verification status of the caller data has been provided to the agent via the agent desktop.

9. Conclusion

These Application Notes have described the configuration steps required to integrate the Journey Identity Platform with Avaya Experience Portal. Inbound calls were answered by Experience Portal, which verified the caller's ANI with the Journey Identity Platform, and then transferred the caller to an available agent. The agent was also able to request additional private information from the caller securely that was verified by the Journey Identity Platform. All test cases passed.

10. Additional References

This section references the product documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021, available at <http://support.avaya.com>.
- [2] *Administering Avaya Experience Portal*, Release 8.1, Issue 1, July 2021, available at <http://support.avaya.com>.

©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.