



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for MModal Fluency Voice Server with Avaya Aura® Session Manager 7.0 – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for MModal Fluency Voice Server to interoperate with Avaya Aura® Session Manager 7.0 and Avaya Aura® Communication Manager 7.0 using SIP trunks. MModal FVS is an Interactive voice response (IVR) that records dictations.

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 for MModal Fluency Voice Server (FVS) to interoperate with Avaya Aura® Session Manager 7.0 and Avaya Aura® Communication Manager 7.0 using SIP trunks.

In the compliance testing, calls from internal and external callers were routed over SIP trunks to FVS. FVS played greeting announcements, used DTMF digits to determine the action such as enter User ID then a soft talkdown tone is played until user speak FVS start to record dictations, enter DTMF digit to interrupts, play, resume or end recording.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were placed manually from users on the PSTN and on Communication Manager to FVS. Speech and DTMF input were used from the callers for recording dictations, interrupts, play, resume or end recording.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to FVS.

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 this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and the MModal FVS is UDP. FVS does not utilize any capabilities of TLS.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included:

- G.711MU with shuffling option off.
- FVS receives an incoming call.
- Caller hangs up a call. FVS hangs up a call.
- Receiving a call with delayed offer (SDP in OK instead of INVITE).
- Receiving DTMF as RFC2833.
- Caller putting call on hold/resume call from hold.
- FVS responses to a re-INVITEs.
- FVS responds to OPTIONS ping.
- Load balancing between 2 FVSs.

The serviceability testing focused on verifying the ability of FVS to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to FVS or one FVS server is out of service and incoming call is routed to available FVS without any delay.

## 2.2. Test Results

All test cases were executed, and the following were observations on FVS:

- The application only supports the G.711MU codec, and does not support codec negotiation and media shuffling.
- Load balancing is not fully round robin. By design, Session Manager will randomly route calls to any available FVS.

## 2.3. Support

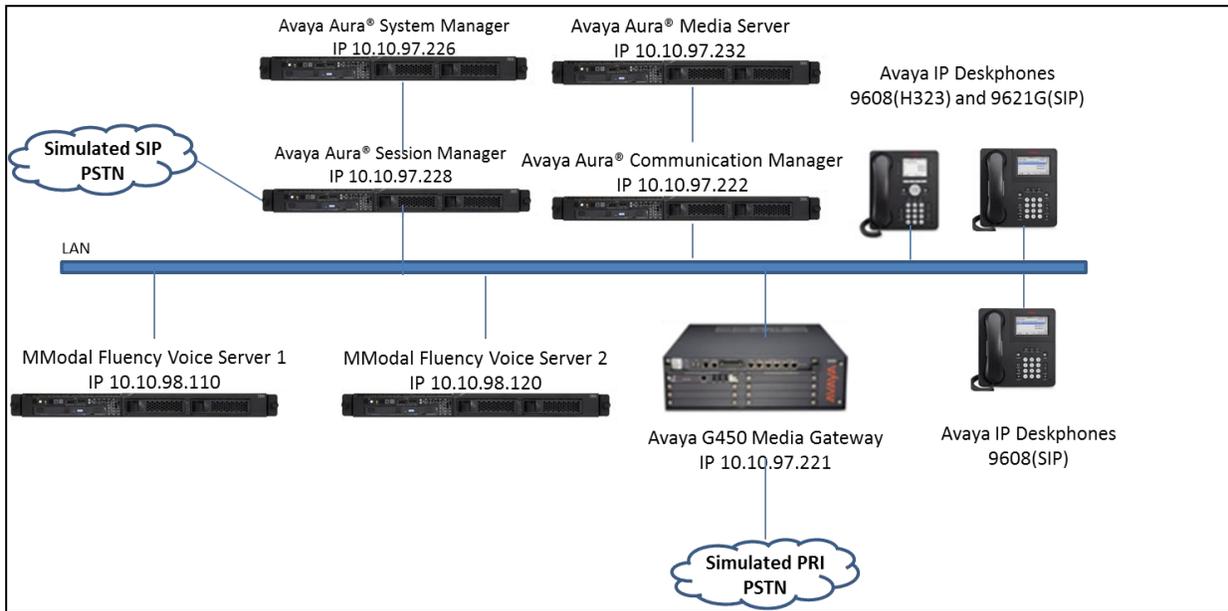
Technical support on FVS can be obtained through the following:

- **Phone:** 1-888-dictate

### 3. Reference Configuration

As shown in **Figure 1**, SIP trunks were used between Session Manager and FVS. A 10 digit Uniform Dial Plan (UDP) was used to facilitate routing with FVS.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager is not the focus of these Application Notes and will not be described.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® Communication Manager in Virtual Environment	7.0.1.2 SP2
Avaya G450 Media Gateway	37.41
Avaya Aura® Media Server in Virtual Environment	7.8
Avaya Aura® Session Manager in Virtual Environment	7.0.1.2
Avaya Aura® System Manager in Virtual Environment	7.0.1.2
Avaya 9608 IP Deskphone (H.323)	6.6.4
Avaya 9608 & 9621G IP Deskphones (SIP)	7.0.1.4
MModal FVS on Microsoft Windows Server 2012	3.6 R2 Standard 64 bit

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer system parameters features
- Administer SIP signaling group
- Administer SIP trunk group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer uniform dial plan
- Administer AAR analysis

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with FVS.

### 5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                               Page 2 of 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 10
      Maximum Concurrently Registered IP Stations: 1800 1
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 41000 1
      Maximum Video Capable IP Softphones: 24000 20
      Maximum Administered SIP Trunks: 24000 54
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0
```

## 5.2. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or “procr”.
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with MModal.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with MModal.
- **Far-end Domain:** The applicable domain name for the network.
- **Direct IP-IP Audio Connections:** “n”, FVS requires shuffling off.

```
display signaling-group 1                                     Page 1 of 3
                                                           SIGNALING GROUP

Group Number: 1                                           Group Type: sip
IMS Enabled? n                                           Transport Method: tls
  Q-SIP? n
  IP Video? n                                           Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr                               Far-end Node Name: SM-VM
  Near-end Listen Port: 5061                             Far-end Listen Port: 5061
                                                         Far-end Network Region: 1

Far-end Domain: bvwdev.com

Incoming Dialog Loopbacks: eliminate                     Bypass If IP Threshold Exceeded? n
  DTMF over IP: rtp-payload                             RFC 3389 Comfort Noise? n
  Session Establishment Timer(min): 3                    Direct IP-IP Audio Connections? n
  Enable Layer 3 Test? y                                IP Audio Hairpinning? y
                                                         Alternate Route Timer(sec): 6
```

### 5.3. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “5”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”

```
add trunk-group 5                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 5                                     Group Type: sip          CDR Reports: y
  Group Name: ToFVS                                COR: 1                  TN: 1          TAC: #005
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                    Member Assignment Method: auto
                                                    Signaling Group: 1
                                                    Number of Members: 20
```

Navigate to **Page 3**, and enter “private” for **Numbering Format**.

```
add trunk-group 5                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                Measured: internal
                                                    Maintenance Tests? y
  Suppress # Outpulsing? n  Numbering Format: private
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n
                                                    Hold/Unhold Notifications? y
                                                    Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
DSN Term? n                                         SIP ANAT Supported? n
```

## 5.4. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.2**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. For **Codec Set**, enter an available codec set number for integration with FVS.

```
change ip-network-region 1                               Page 1 of 20
                                                         IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: bvwdev.com
  Name: Region1    Stub Network Region: n
MEDIA PARAMETERS  Intra-region IP-IP Direct Audio: yes
  Codec Set: 1     Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048      IP Audio Hairpinning? y
  UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
```

Navigate to **Page 4**, and specify this codec set to be used for calls with network regions used by Avaya endpoints and by the trunk to the PSTN. In the compliance testing, network region “1” was used by the Avaya endpoints and by the trunk to the PSTN.

```
change ip-network-region 1                               Page 4 of 20
Source Region: 1    Inter Network Region Connection Management  I      M
                                                           G  A  t
dst codec direct  WAN-BW-limits  Video    Intervening  Dyn  A  G  c
rgn set  WAN Units  Total Norm  Prio Shr Regions  CAC  R  L  e
1    1
2
3
4
5
6
7
8
```

## 5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.4**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that FVS only supports the G.711 Mu-law codec variant. The codec shown below was used in the compliance testing.

```
change ip-codec-set 1                                     Page 1 of 2

                               IP Codec Set

Codec Set: 2

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU           n         2        20
2:
3:
4:
5:
```

## 5.6. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach FVS, in this case “5”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

```
change route-pattern 5                                     Page 1 of 3

                               Pattern Number: 52  Pattern Name: MModal
                               SCCAN? n      Secure SIP? n

Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC
No      Mrk Lmt List Del  Digits          QSIG
                               Dgts          Intw
1: 5    0
2:
3:
4:
5:
6:

          BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM  No. Numbering LAR
          0 1 2 M 4 W      Request          Dgts Format
1: y y y y y n  n          rest          unk-unk          none
```

## 5.7. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed 10 digits 7219675800 to FVS. Note that other routing methods may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing of digits 721, as shown below.

```
change uniform-dialplan 0                                     Page 1 of 2
                                UNIFORM DIAL PLAN TABLE
                                Percent Full: 0
```

Matching Pattern	Len	Del	Insert Digits	Net Conv	Node Num
721	10	0		aar	n

## 5.8. Administer AAR Analysis

Use the “change aar analysis 7” command, and add an entry to specify how to route calls to 721. In the example shown below, calls with digits 721 will be routed as an AAR call using route pattern “5” from **Section 5.6**.

```
change aar analysis 7                                       Page 1 of 2
                                AAR DIGIT ANALYSIS TABLE
                                Location: all                 Percent Full: 2
```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
721	5	10	5	aar		n

## 6. Configure Avaya Aura® Session Manager

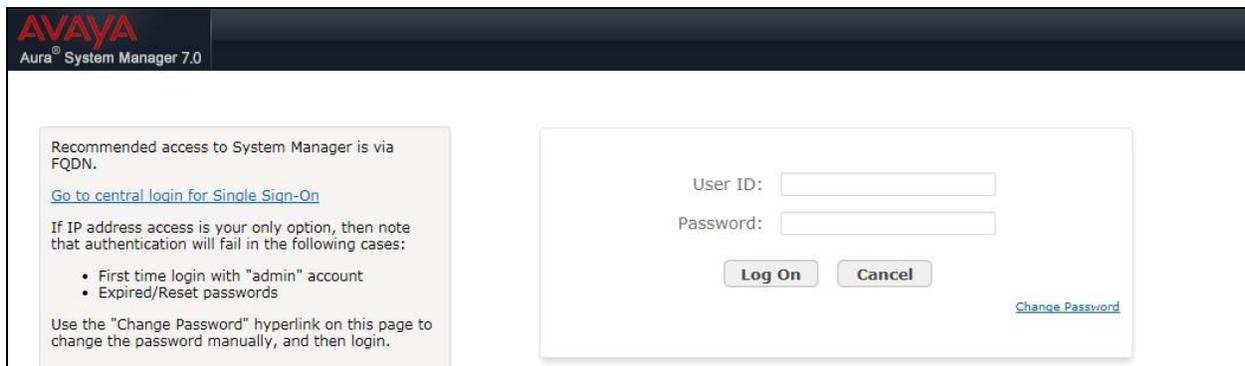
This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer Domains
- Administer Locations
- Administer Adaptations
- Administer SIP entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

Since the configuration was created during compliance test and the screenshots were capture after testing therefore the screenshot will display in modify mode instead of new create objects.

### 6.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



AVAYA  
Aura® System Manager 7.0

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.

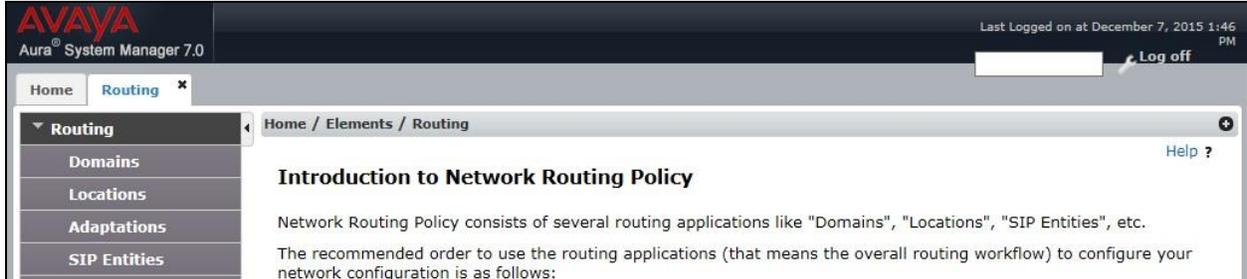
User ID:

Password:

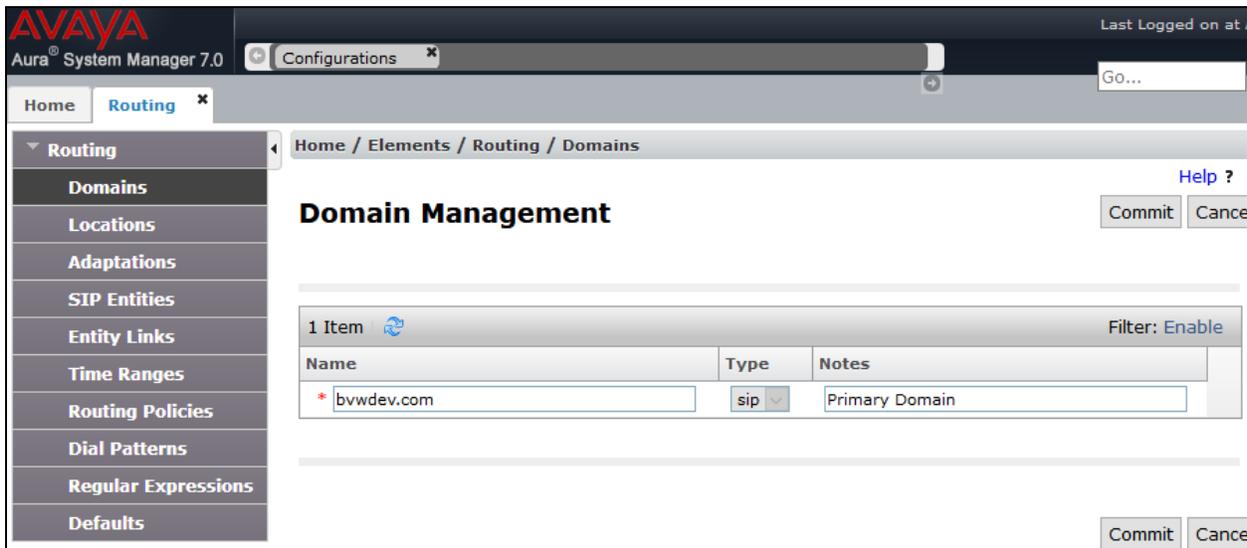
[Change Password](#)

## 6.2. Administer Domains

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen below.



Select **Routing** → **Domains** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for FVS. The **Domain Management** screen is displayed. In the **Name**, enter a domain name used in **Section 5.2**, select **Type** and optional **Notes**.



### 6.3. Administer Locations

Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for FVS. The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

AVAYA  
Aura System Manager 7.0

Configurations

Last Logged on at April 2

Home Routing

Home / Elements / Routing / Locations

Location Details

Help ?

Commit Cancel

General

\* Name: Belleville

Notes: Belleville DevConnect Lab

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of FVS in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

4 Items Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.5.*	Phones and Servers on private lab network
<input type="checkbox"/>	* 10.10.97.*	Lab PBX
<input type="checkbox"/>	* 10.10.98.*	
<input type="checkbox"/>	* 172.29.187.*	opentrade

Select : All, None

Commit Cancel

## 6.4. Administer Adaptations

Add two new Adaptations, one for FVS1 and one for FVS2. Select **Routing → Adaptations** from the left panel, and click **New** in the subsequent screen (not shown) to add a new Adaptation for FVS.

The **Adaptation Details** screen is displayed. Enter the following values for specified fields and retain the default value for the remaining fields.

- **Adaptation Name:** A descriptive name.
- **Module Name:** Select DigitConversionAdapter.
- **Module Parameter Type:** Select Name-Value Parameter.

Click Add to add new item for parameter:

- **Name:** iodstd and **Value:** bwdev.com.
- **Name:** ioscrd and **Value:** bwdev.com.
- **Name:** odstd and **Value:** FVS's IP address, for example, 10.10.98.110.

The screenshot shows the 'Adaptation Details' configuration page in Avaya Aura System Manager 7.0. The page is titled 'Adaptation Details' and has a breadcrumb trail: 'Home / Elements / Routing / Adaptations'. The left sidebar shows a navigation menu with 'Routing' selected, and 'Adaptations' highlighted. The main content area contains the following fields:

- \* Adaptation Name:** ForFVS1
- \* Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table with columns 'Name' and 'Value'. The table contains three entries:

Name	Value
iodstd	bwdev.com
ioscrd	bwdev.com
odstd	10.10.98.110

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.

Repeat the same step for FVS2 as display below:

Home / Elements / Routing / Adaptations

### Adaptation Details

Commit Cancel

**General**

\* Adaptation Name: ForFVS2

\* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	iodstd	bvwdev.com
<input type="checkbox"/>	ioscrd	bvwdev.com
<input type="checkbox"/>	odstd	10.10.98.120

Select : All, None

## 6.5. Administer SIP Entities

Add two new SIP entities, one for FVS1 and one for FVS2. Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for FVS.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the FVS1 server.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the FVS location name from **Section 6.3**.
- **Time Zone:** Select the applicable time zone.

**SIP Entity Details** Commit Cancel

**General**

\* **Name:** FVS\_SIPTrunk1

\* **FQDN or IP Address:** 10.10.98.110

**Type:** SIP Trunk

**Notes:**

**Adaptation:** ForFVS1

**Location:** Belleville

**Time Zone:** America/New\_York

\* **SIP Timer B/F (in seconds):** 4

**Credential name:**

**Securable:**

**Call Detail Recording:** egress

**Loop Detection**

**Loop Detection Mode:** On

**Loop Count Threshold:** 5

**Loop Detection Interval (in msec):** 90

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DevvmSM”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The FVS entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that FVS can support both UDP and TCP and the compliance testing used the UDP protocol.

**Entity Links**

Override Port & Transport with DNS SRV:

Add Remove

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinkToFVS1	DevvmSM	UDP	* 5060	FVS_SIPTrunk1	* 5060	trusted	<input type="checkbox"/>

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

0 Items Filter: Enable

	Mark Entity Up/Down	Notes
<input type="checkbox"/>		

Commit Cancel

Repeat same step for FVS2, below is the screenshot for FVS2 SIP Entity and Entity Link:

### SIP Entity Details

Commit Cancel

**General**

\* Name: FVS\_SIPTrunk2

\* FQDN or IP Address: 10.10.98.120

Type: SIP Trunk

Notes:

Adaptation: ForFVS2

Location: Belleville

Time Zone: America/New\_York

\* SIP Timer B/F (in seconds): 4

Credential name:

Securable:

Call Detail Recording: egress

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 90

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

### Entity Links

Override Port & Transport with DNS SRV:

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinkToFVS2	DevvmSM	UDP	* 5060	FVS_SIPTrunk2	* 5060	trusted	<input type="checkbox"/>

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

## 6.6. Administer Routing Policies

Add two new routing policies, one for FVS and one for the new SIP trunks with Communication Manager. Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for FVS.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the FVS entity name from **Section 6.5**. The screen below shows the result of the selection.

### Routing Policy Details

Commit Cancel  
**General**  

\* **Name:**

**Disabled:**

\* **Retries:**

**Notes:**

**SIP Entity as Destination**  
Select  

Name	FQDN or IP Address	Type	Notes
FVS_SIPTrunk1	10.10.98.110	SIP Trunk	

Repeat the same step for FVS2:

### Routing Policy Details

Commit Cancel  
**General**  

\* **Name:**

**Disabled:**

\* **Retries:**

**Notes:**

**SIP Entity as Destination**  
Select  

Name	FQDN or IP Address	Type	Notes
FVS_SIPTrunk2	10.10.98.120	SIP Trunk	

## 6.7. Administer Dial Patterns

Same dial pattern will be created for FVS1 and FVS2. Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach FVS. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “721”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.
- **SIP Domain:** The signaling group domain name from **Section 5.2**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching FVS1 and FVS2. In the compliance testing, FVS routing policies from **Section 6.6** were selected as shown below.

### Dial Pattern Details

Commit Cancel

**General**

\* **Pattern:**

\* **Min:**

\* **Max:**

**Emergency Call:**

**Emergency Priority:**

**Emergency Type:**

**SIP Domain:**

**Notes:**

**Originating Locations and Routing Policies**

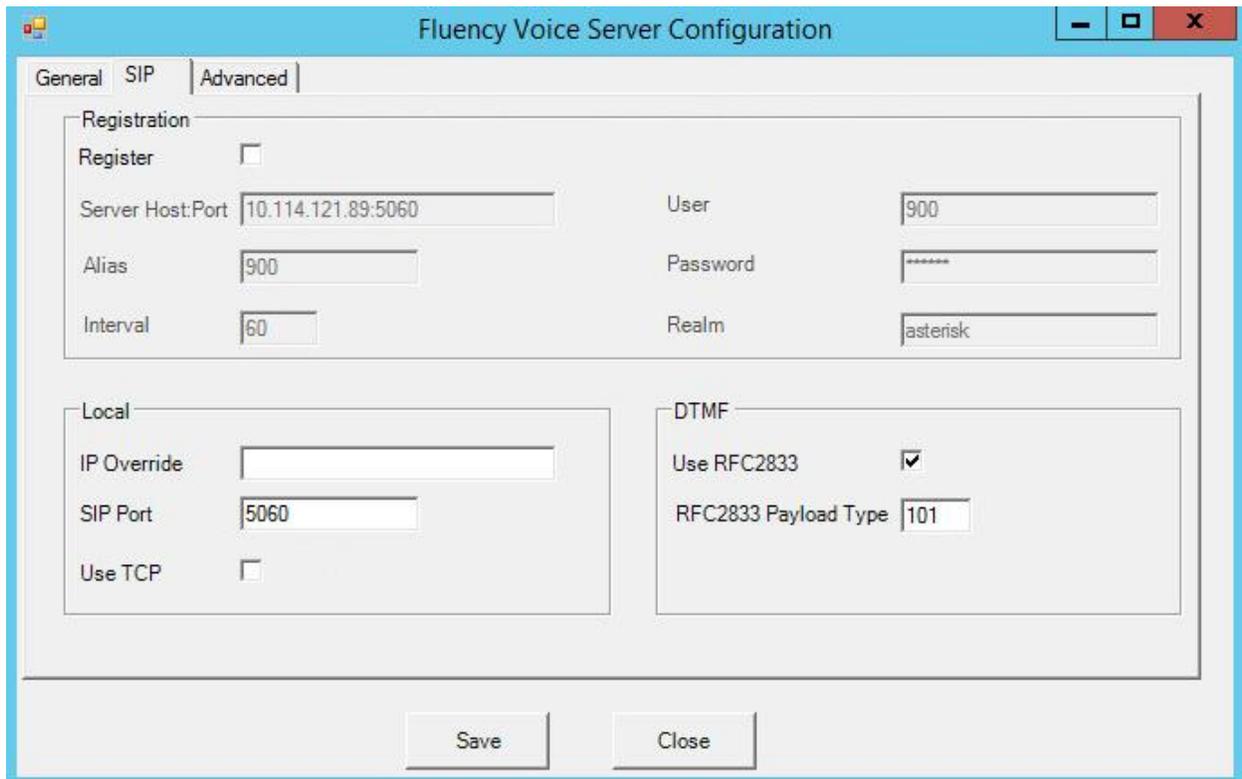
Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	RouteToFVS2	0	<input type="checkbox"/>	FVS_SIPTrunk2	
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	RouteToFVS1	0	<input type="checkbox"/>	FVS_SIPTrunk1	

## 7. Configure MModal FVS

This section provides the procedures for configuring FVS. It is assumed that FVS is already installed and operational. The procedures include configuring DTMF use RFC2833. On FVS, launch **Fluency Voice Server Configuration** application, in **SIP** tab verify option **Use RFC2833** is checked as displayed below:



The screenshot shows the 'Fluency Voice Server Configuration' application window with the 'SIP' tab selected. The window has three tabs: 'General', 'SIP', and 'Advanced'. The 'SIP' tab is active, showing the following configuration options:

- Registration:**
  - Register:
  - Server Host:Port:
  - User:
  - Alias:
  - Password:
  - Interval:
  - Realm:
- Local:**
  - IP Override:
  - SIP Port:
  - Use TCP:
- DTMF:**
  - Use RFC2833:
  - RFC2833 Payload Type:

At the bottom of the window, there are two buttons: 'Save' and 'Close'.

## 8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and FVS.

### 8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 5

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0052/001 T00146   in-service/idle    no
0052/002 T00147   in-service/idle    no
0052/003 T00148   in-service/idle    no
0052/004 T00149   in-service/idle    no
0052/005 T00150   in-service/idle    no
0052/006 T00151   in-service/idle    no
0052/007 T00152   in-service/idle    no
0052/008 T00153   in-service/idle    no
0052/009 T00154   in-service/idle    no
0052/010 T00155   in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.2**. Verify that the **Group State** is “in-service”, as shown below.

```
status signaling-group 1

                                STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

Group State: in-service
```

## 8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click the FVS entity name from **Section 6.5**.

The screenshot shows the Session Manager interface. The left sidebar contains the following menu items: Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, SIP Entity Monitoring (selected), Managed Bandwidth Usage, Security Module Status, SIP Firewall Status, Registration Summary, and User Registrations.

The main content area is titled "SIP Entities Status for All Monitoring Session Manager Instances" and includes a "Run Monitor" button. It displays a table with 1 item:

Session Manager	Type	Monitored Entities						Total
		Down	Partially Up	Up	Not Monitored	Deny		
<a href="#">Devvmsm</a>	Core	11	0	14	1	0	26	

Below the table, there is a "Select: All, None" option and a section titled "All Monitored SIP Entities" with another "Run Monitor" button. This section lists 25 items, with the following visible:

SIP Entity Name
<a href="#">CS1K_Bottom</a>
<a href="#">FVS_SIPTrunk1</a>

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are “UP”, as shown below.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The breadcrumb trail is Home / Elements / Session Manager / System Status / SIP Entity Monitoring. The page title is "SIP Entity, Entity Link Connection Status". Below the title, it states: "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." The selected SIP entity is "FVS\_SIPTrunk1". A "Summary View" button is present. Below it, a table displays the connection status for one item:

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DevvmSM	10.10.98.110	5060	UDP	FALSE	UP	200 OK	UP

Repeat the same step for FVS2:

The screenshot shows the Avaya Aura System Manager 7.0 interface. The breadcrumb trail is Home / Elements / Session Manager / System Status / SIP Entity Monitoring. The page title is "SIP Entity, Entity Link Connection Status". Below the title, it states: "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." The selected SIP entity is "FVS\_SIPTrunk2". A "Summary View" button is present. Below it, a table displays the connection status for one item:

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DevvmSM	10.10.98.120	5060	UDP	FALSE	UP	200 OK	UP

Make two phones call to FVS as mention in **Section 8.3**, verify the traces display detail of the calls as shown below (last 2 calls):

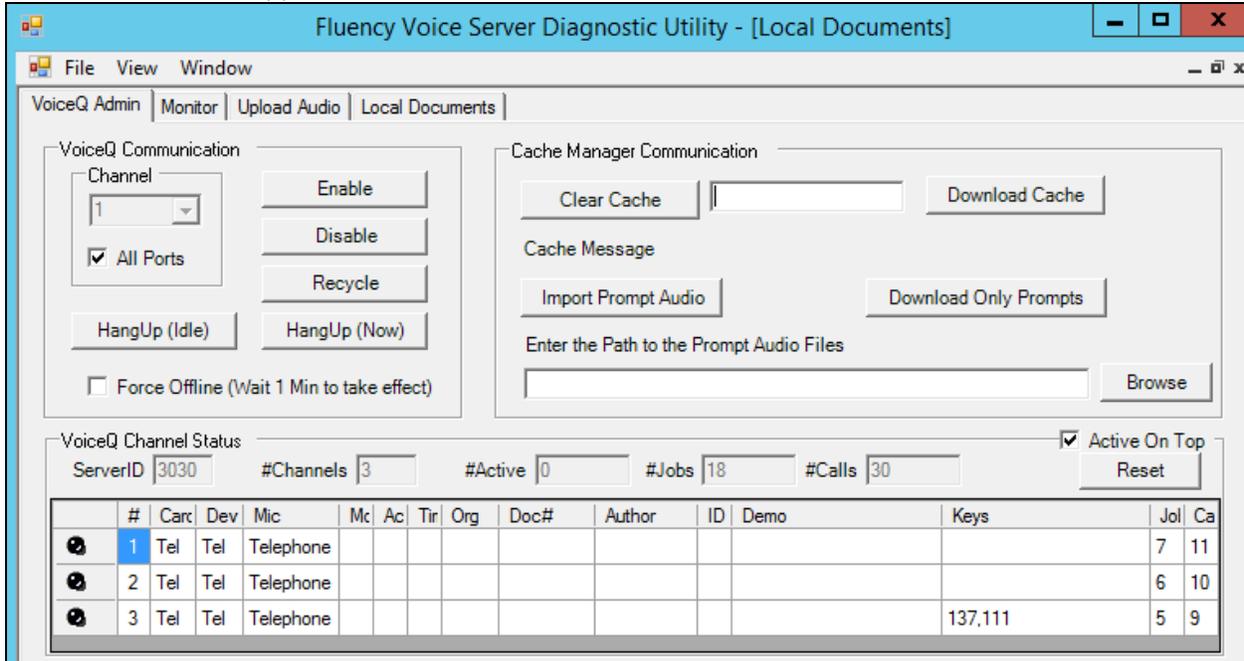
```

DevvmSM - traceSM V3.22 - FILTERED - Captured: 1014 Displayed: 31
-----
10.10.97.228      10.10.98.120
10.10.98.110
-----
13:03:54.897 |----BYE---->| | (17) sip:7219675800@ 10.10.98.110
13:03:55.397 |----BYE---->| | (17) sip:7219675800@ 10.10.98.110
13:03:55.952 |<--200 OK--| | (17) 200 OK (BYE)
13:04:41.394 |<----BYE---->| | (21) sip: 10.10.97.222
13:04:41.399 |--200 OK-->| | (21) 200 OK (BYE)
13:07:05.562 |-----INVITE----->| | (89) T:7219675800 F:anonymous@anonymous U:7219675800 P:terminat
13:07:05.608 |<-----Ringing-----| | (89) 180 Ringing
13:07:05.610 |<-----200 OK-----| | (89) 200 OK (INVITE)
13:07:05.615 |-----ACK----->| | (89) sip:7219675800@ 10.10.98.120
13:07:05.655 |-----reINVITE----->| | (89) T:7219675800 F:anonymous@anonymous U:7219675800
13:07:05.659 |<-----Trying-----| | (89) 100 Trying
13:07:05.663 |<-----200 OK-----| | (89) 200 OK (INVITE)
13:07:05.666 |-----ACK----->| | (89) sip:7219675800@ 10.10.98.120
13:07:06.942 |-----INVITE----->| | (92) T:7219675800 F:anonymous@anonymous U:7219675800 P:terminat
13:07:06.993 |<-----Ringing-----| | (92) 180 Ringing
13:07:06.996 |<-----200 OK-----| | (92) 200 OK (INVITE)
13:07:07.001 |-----ACK----->| | (92) sip:7219675800@ 10.10.98.120
13:07:20.165 |-----OPTIONS----->| | (95) sip: 10.10.98.120
13:07:20.167 ||-----200 OK-----| | (95) 200 OK (OPTIONS)
-----
SIP ERR CallE TLS | s=Stop q=Quit ENTER=Details f=Filters w=Write a=ShowSM c=Clear i=Name r=RTP g=GoTo d=Call>

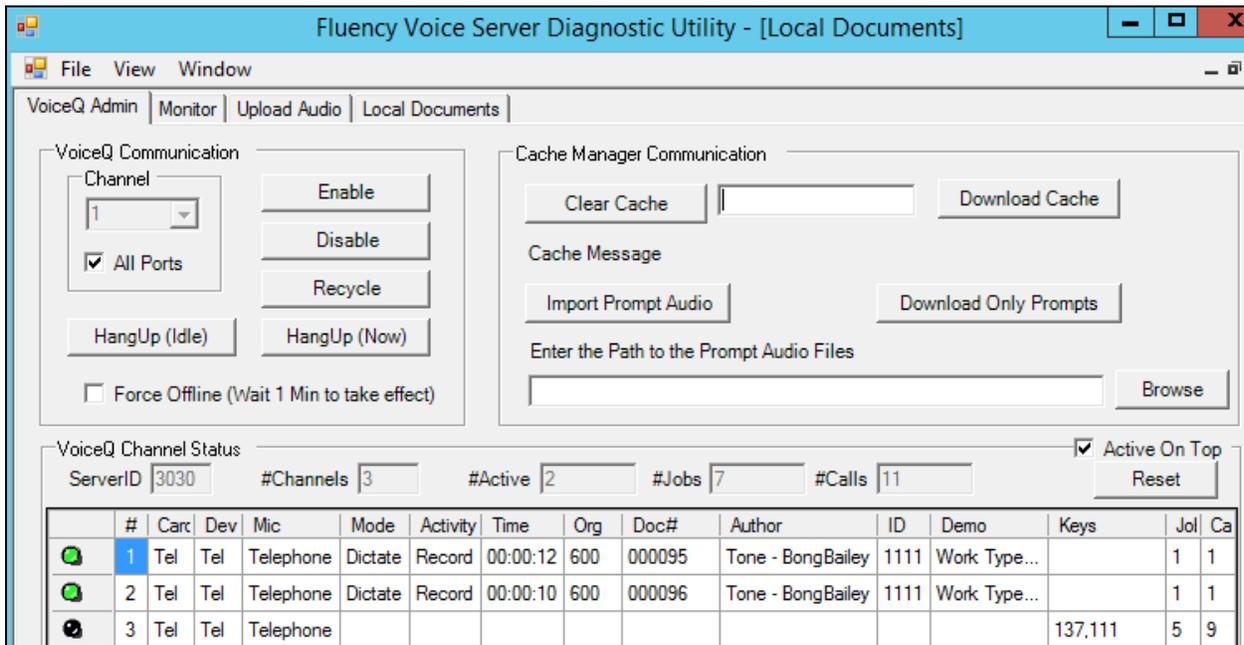
```

### 8.3. Verify MModal FVS

On Fluency Voice Server launch Fluency Voice Server Diagnostic Utility verify all voice channels are Enable(s) as shown below:



Make couples phone calls to FVS, for example, two call were made and connected to FVS2, below is the status of 2 voice channels are in the call:



Please reference back to **Section 8.2** for trace log of two calls on Session Manager.

## 9. Conclusion

These Application Notes describe the configuration steps required for MModal FVS to successfully interoperate with Avaya Aura® Session Manager 7.0 and Avaya Aura® Communication Manager 7.0 using SIP trunks. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1 555-245-205 Issue 3 October 2016.
2. *Administering Avaya Aura® Session Manager*, Release 7.0.1 Issue 2 May 2016.
3. *Administering Avaya Aura® System Manager*, Release 7.0.1

MModal document available upon request.

---

**©2017 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](mailto:devconnect@avaya.com).