



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring DuVoice DV2000 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes contains interoperability instructions for configuring DuVoice DV2000 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Compliance testing was conducted to verify the interoperability.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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

This application notes contain instruction for configuring DuVoice DV2000 with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya endpoints. In the compliance testing SIP trunks were used between the DuVoice DV2000 Voice Messaging System and Avaya Aura® Session Manager.

DuVoice DV2000 is a hospitality application that provides voicemail, automated attendant, and wake-up call features. The compliance testing focused on integrating the DuVoice DV2000 with Avaya Aura® Communication Manager and Aura® Session Manager.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls and inbound trunk calls that were ultimately answered by the DuVoice DV2000. Depending on the type of call, the user then had the option to leave a voicemail message, retrieve a voicemail message, and schedule a wake-up call or transfer to another extension. All inbound calls were routed by Communication Manager to the DuVoice DV2000 hunt group via Session Manager, which were answered by the DV2000 with the automated attendant greeting. Internal calls that were unanswered were covered to the DV2000 hunt group. The DV2000 would answer these calls with the voice mailbox greeting of the subscriber extension. Lastly, internal calls placed to the DV2000 directly were answered by the DV2000 with the voicemail menu of the originating extension with an option to retrieve messages. For serviceability testing, the DV2000 and Communication Manager were each restarted separately.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing focused on exercising the core features of the DV2000 to validate the integration interface to Session Manager using SIP Trunks. This included the automated attendant, voicemail, wakeup call and performing guest check-in and checkout using the Room Status Monitor functionality. The serviceability testing introduced failure scenarios to verify operation of the DuVoice DV2000 after failure recovery.

2.2. Support

Interoperability testing of the sample configuration was completed with successful results for DuVoice DV2000.

2.3. Support

Technical support on DuVoice can be obtained through the following:

- **Phone:** (425) 250-2393
- **Email:** support@duvoice.com

3. Reference Configuration

Figure 1: Test configuration used during compliance testing consisted of following:

- Avaya G450 Media Gateway with Avaya 8300D Media Server running Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- DuVoice DV2000 running on Windows 7 Enterprise

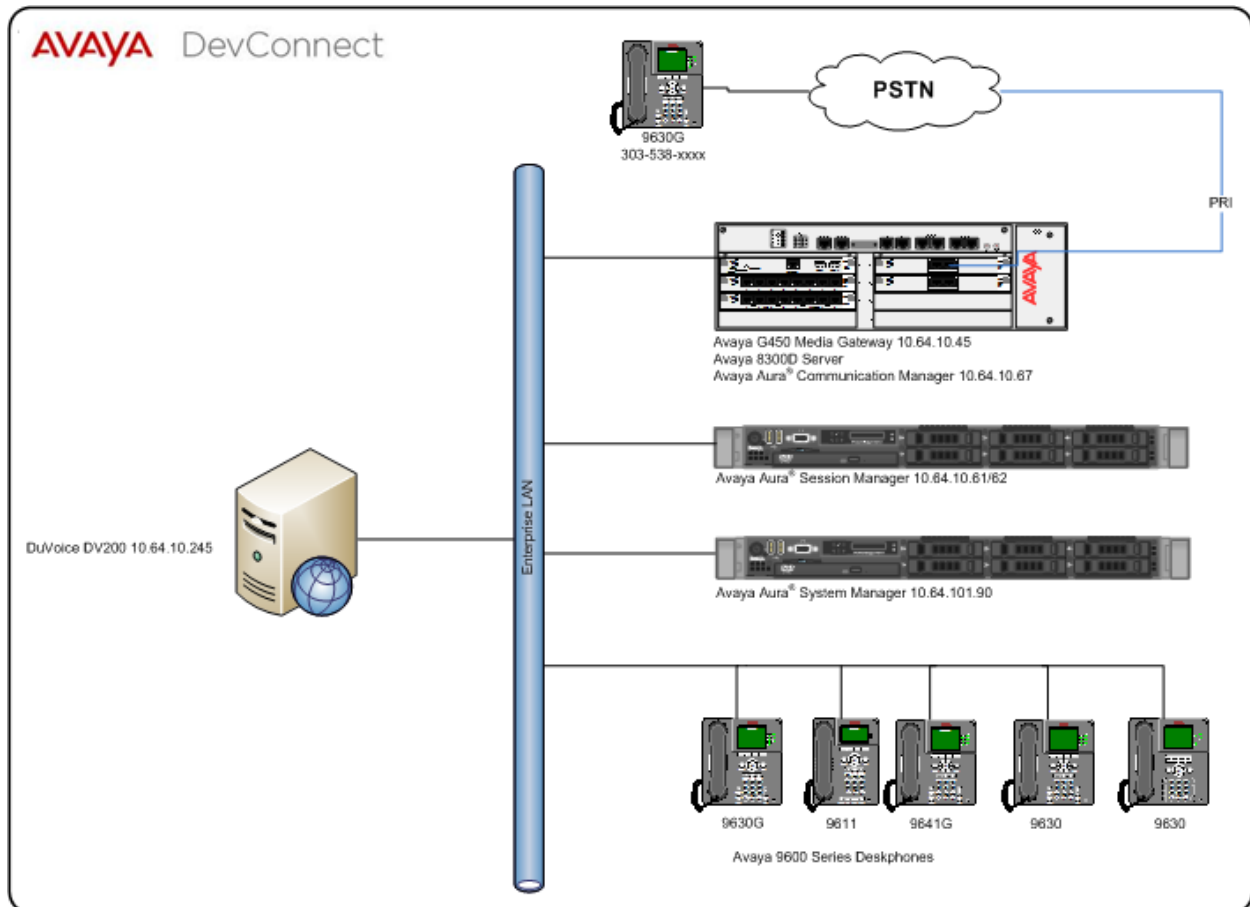


Figure 1: Reference Configuration

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 running on Avaya S8300D Server	6.2 SP5
Avaya Aura® Session Manager	6.3 SP5
Avaya Aura® System Manager	6.3 SP4
DuVoice DV2000 running on Windows 7 Enterprise	5.2.0

5. Configure Avaya Aura® Communication Manager

This section provides steps for configuring Communication Manager. All configuration for Communication Manager is done through System Access Terminal (SAT).

5.1. Administer IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where *n* is an existing network region.

Configure this network region as follows:

- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter and **Authoritative Domain**, e.g. avaya.com

change ip-network-region 1	Page 1 of 20
IP NETWORK REGION	
Region: 1	
Location: 1	Authoritative Domain: avaya.com
Name:	
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? n
UDP Port Max: 3329	
DIFFSERV/TOS PARAMETERS	
Call Control PHB Value: 46	
Audio PHB Value: 46	
Video PHB Value: 26	
802.1P/Q PARAMETERS	
Call Control 802.1p Priority: 6	
Audio 802.1p Priority: 6	
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS	RSVP Enabled? n
H.323 Link Bounce Recovery? y	
Idle Traffic Interval (sec): 20	
Keep-Alive Interval (sec): 5	

5.2. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where *n* is an existing codec set number.

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1** to **G.711MU**

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

	Audio	Silence	Frames	Packet
	Codec	Suppression	Per Pkt	Size(ms)
1:	G.711MU	n	2	20
2:				
3:				
4:				
5:				
6:				
7:				

Media Encryption

1:

2:

3:

5.3. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm** and **10.64.10.62** entry was added.

change node-names ip		Page	1	of	2
IP NODE NAMES					
Name	IP Address				
default	0.0.0.0				
msgsrvr	10.64.10.67				
procr	10.64.10.67				
procr6	::				
sm	10.64.10.62				

5.4. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number.

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.3**, i.e. **sm**
- Set **Far-end Network region** to the configured region in **Section 5.1**, i.e. **1**
- Enter a **Far-end Domain**, e.g. **avaya.com**

add signaling-group 1		Page 1 of 2
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: Others	
Near-end Node Name: procr	Far-end Node Name: sm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.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? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Note: Signaling Group, Trunk Group and Route Pattern for simulated PSTN calls for inter-site calls over ISDN/PRI and SIP were pre-configured and are not shown in this document.

5.5. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where *n* is an available trunk group number.

Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. SM
- Enter a valid **TAC**, e.g. *001
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.4**, i.e. 1
- Enter a desired number in **Number of Member** field

```
add trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip       CDR Reports: y
  Group Name: SM                                     COR: 1           TN: 1         TAC: *001
  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: 25
```

On **Page 3**:

- Set **Number Format** to **private**

```
add trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                               Measured: none
                                                Maintenance Tests? y

Numbering Format: private                           UI Treatment: service-provider
                                                Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```


5.6. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where *n* is an available route pattern.

Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 5.5**, i.e. 1
- For line 1, set **FRL** to 0

change route-pattern 1										Page 1 of 3	
					Pattern Number: 1		Pattern Name: Voice				
					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: 1		0							n user		
2:							n user				

5.7. Administer Hunt Group

Use the **add hunt-group *n*** command to configure a hunt group, where *n* is an available hunt group number.

Configure the hunt group as follows:

- Type a descriptive name in **Group Name** field
- Type in a available extension number for **Group Extension**

add hunt-group 6		Page 1 of 60	
HUNT GROUP			
Group Number: 6		ACD? n	
Group Name: DuVoice Voicemail		Queue? n	
Group Extension: 25099		Vector? n	
Group Type: ucd-mia		Coverage Path:	
TN: 1		Night Service Destination:	
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			

5.8. Administer Coverage Path

Use the **add coverage path *n*** command to add a coverage path, where *n* is available coverage path number.

Configure the coverage path as follows:

- Under **COVERAGE POINTS**, for **Point1** type in the hunt group that was configured in previous section. e.g., h6, where h stands for hunt group and 6 is the hunt group number.

```
add coverage path 6                                     Page 1 of 1

                                COVERAGE PATH

                                Coverage Path Number: 6
                                Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n
                                Next Path Number:                          Linkage

COVERAGE CRITERIA
  Station/Group Status   Inside Call   Outside Call
    Active?              n              n
    Busy?                y              y
    Don't Answer?        y              y      Number of Rings: 2
    All?                 n              n
  DND/SAC/Goto Cover?    y              y
  Holiday Coverage?      n              n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h6             Rng:          Point2:
  Point3:                 Point4:
  Point5:                 Point6:
```

5.9. Administer Private Numbering

Use the **change private-numbering 1** command to define the calling party number to send to Session Manager.

Configure private numbering as follows:

- Add entries for trunk group configured in **Section 5.5**

Note: For compliance testing, 5-digit hunt group extension 25099 routed over trunk groups 1 resulted in a 5-digit calling party number.

```
change private-numbering 1                             Page 1 of 2

                                NUMBERING - PRIVATE FORMAT

Ext  Ext      Trk      Private      Total
Len  Code     Grp(s)   Prefix     Len
  5   25099    1          5          5      Total Administered: 1
                                Maximum Entries: 540
```

5.10. Administer AAR Analysis

Use the **change aar analysis *n*** command to configure routing for hunt group extension number *n*. For compliance testing, hunt group extension 25099 was used for routing calls to DV2000.

- Set **Dialed String** to hunt group extension, e.g. 25099
- Set **Min** and **Max** to 5 for 5 digit extensions
- Set **Route Pattern** to pattern configured in **Section 5.6**, i.e. 1
- Set **Call Type** to **aar**

Note: An entry to dial plan will need to be added for extension range used in this step.

change aar analysis 25099						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 Req'd
	25099	5	5	1	aar		n
	252	5	5	2	aar		n
	257	5	5	10	aar		n
	258	5	5	10	aar		n
	25990	5	5	13	aar		n
	25999	5	5	98	aar		n
	26	5	5	10	aar		n
	27	5	5	21	aar		n

5.11. Administer Stations

Administration of Avaya Stations/Extensions in Communication Manager and Session Manager is not shown in this document. Please refer to document [1] and/or [2] in reference section of this document.

6. Configure Avaya Aura® Session Manager

Configuration of Avaya Aura® Session Manager is performed via System Manager. Access the System Manager Administration web interface by entering <https://<ip-address>/SMGR> URL in a web browser, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials

AVAYA
Aura® System Manager 6.3

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.

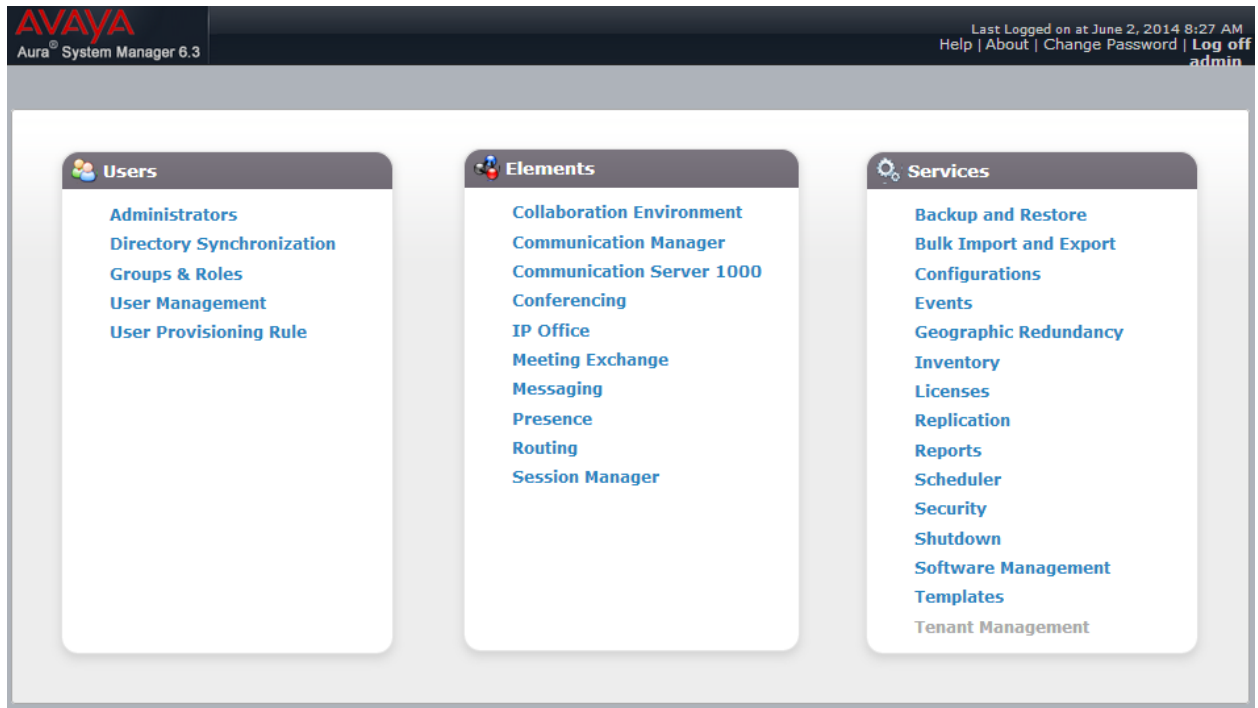
User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

Once logged in, the following screen is displayed.



6.1. Add SIP Domain

Navigate to **Home → Elements → Routing → Domains**, click on **New** button (not shown) and configure as follows:

- In **Name** field type in a domain (authoritative domain used in **Section 5.1**) i.e. avaya.com
- Set **Type** to **sip**

Click **Commit** to save changes.

AVAYA
Aura® System Manager 6.3

Last Logged on at June 2, 2014 8:27 AM
Help | About | Change Password | Log off
admin

Home Routing x

Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item Filter: Enable

Name	Type	Notes
*avaya.com	sip	

Commit Cancel

6.2. Add Location

Navigate to **Home → Elements → Routing → Location**, click on **New** button (not shown) and configure as follows:

Under **General**:

- Type in a descriptive **Name**

Under **Location Pattern** click on **New** (not shown):

- Type in an **IP Address Pattern**, e.g. 10.64.10.*

Click **Commit** to save changes. Screen shot shown on next page.

The screenshot displays the Avaya Element Manager web interface for configuring a new Location. The breadcrumb trail at the top reads "Home / Elements / Routing / Locations". The left sidebar shows a tree view with "Routing" expanded, containing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Location Details" and includes "Commit" and "Cancel" buttons. The configuration is organized into several sections:

- General:** Includes a required field for "Name" (set to "Test Room 1") and a "Notes" field.
- Dial Plan Transparency in Survivable Mode:** Features an "Enabled" checkbox (unchecked), a "Listed Directory Number" field, and a dropdown for "Associated CM SIP Entity".
- Overall Managed Bandwidth:** Includes a "Managed Bandwidth Units" dropdown (set to "Kbit/sec"), "Total Bandwidth" and "Multimedia Bandwidth" fields, and a checked checkbox for "Audio Calls Can Take Multimedia Bandwidth".
- Per-Call Bandwidth Parameters:** Includes fields for "Maximum Multimedia Bandwidth (Intra-Location)" (1000 Kbit/Sec), "Maximum Multimedia Bandwidth (Inter-Location)" (1000 Kbit/Sec), "* Minimum Multimedia Bandwidth" (64 Kbit/Sec), and "* Default Audio Bandwidth" (80 Kbit/sec).
- Alarm Threshold:** Includes "Overall Alarm Threshold" and "Multimedia Alarm Threshold" (both set to 80 %), and latency fields for "Latency before Overall Alarm Trigger" and "Latency before Multimedia Alarm Trigger" (both set to 5 Minutes).
- Location Pattern:** Includes "Add" and "Remove" buttons, a table with 2 items, and a "Filter: Enable" button. The table lists IP Address Patterns: "10.64.10.*" and "10.64.101.*".

At the bottom of the Location Pattern section, it says "Select : All, None".

6.3. Add SIP Entity – Communication Manager

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities**, click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has been already configured.

SIP Entity Details

General

* Name:	<input type="text" value="cm-tr1"/>
* FQDN or IP Address:	<input type="text" value="10.64.10.67"/>
Type:	<input type="text" value="CM"/>
Notes:	<input type="text" value="Avaya Aura® Communication M."/>
Adaptation:	<input type="text" value="cm-tr1"/>
Location:	<input type="text" value="Test Room 1"/>
Time Zone:	<input type="text" value="America/Denver"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text"/>
Call Detail Recording:	<input type="text" value="both"/>

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:	<input type="text" value="Use Session Manager Configuration"/>
Supports Call Admission Control:	<input type="checkbox"/>
Shared Bandwidth Manager:	<input type="checkbox"/>
Primary Session Manager Bandwidth Association:	<input type="text"/>
Backup Session Manager Bandwidth Association:	<input type="text"/>

6.4. Add Entity Link – Communication Manager

Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.3**

Click **Commit** to save changes.

Entity Links Commit Cancel

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM	* SM_Public	TLS	* 5061	* Communication Manager	* 5061	Trusted	

6.5. Add SIP Entity – DuVoice

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities**, click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of DuVoice DV2000 in **FQDN or IP Address** field.
- Set **Type** to **SIP Trunk**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has been already configured.

SIP Entity Details

[Commit](#) [Cancel](#)

General

* Name:	<input type="text" value="dv2000-tr1"/>
* FQDN or IP Address:	<input type="text" value="10.64.10.245"/>
Type:	<input type="text" value="SIP Trunk"/>
Notes:	<input type="text" value="DuVoice DV2000"/>
Adaptation:	<input type="text" value="dv2000-tr1"/>
Location:	<input type="text" value="Test Room 1"/>
Time Zone:	<input type="text" value="America/Denver"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text"/>
Call Detail Recording:	<input type="text" value="egress"/>

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:

6.6. Add Entity Link – DuVoice


Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to DuVoice DV2000 SIP Entity configured in **Section 6.5**
- Set **Protocol** to **UDP**

Click **Commit** to save changes.

Entity Links

Commit Cancel

1 Item 									Filter: Enable	
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connect Policy		
<input type="checkbox"/>	* <input type="text" value="asm-tr1_dv2000-tr"/>	* <input type="text" value="asm-tr1"/> ▼	<input type="text" value="TCP"/> ▼	* <input type="text" value="5060"/>	* <input type="text" value="dv2000-tr1"/> ▼	<input type="checkbox"/>	* <input type="text" value="5060"/>	<input type="text" value="trusted"/>		
<div><div></div></div>										
Select : All, None										

6.7. Add Time Ranges

Navigate to **Home → Elements → Routing → Time Ranges**, click on **New** (now shown) and configure as follows:

- Type in a descriptive name in **Name** field

Click **Commit** to save changes.

Time Ranges

Commit Cancel

1 Item Refresh											Filter: Enable	
Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes		
* TimeRange	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	* 00:00	* 23:59			

6.8. Add Routing Policy – Communication Manager

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
 - Select Communication Manager SIP entity added in **Section 6.3**
- Under **Time of Day**, click on **Add** (not shown):
 - Select time range added in previous step

Click **Commit** to save changes.

Routing Policy Details

CommitCancel

General

* Name:cm-tr1

Disabled:☐

* Retries:0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm-tr1	10.64.10.67	CM	Avaya Aura® Communication Manager - Test Room 1

Time of Day

AddRemoveView Gaps/Overlaps

1 ItemFilter: Enable

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	TimeRange	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select : All, None

6.9. Add Routing Policy – DuVoice

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
 - Select DuVoice DV2000 SIP entity added in **Section 6.5**
- Under **Time of Day**, click on **Add** (not shown):
 - Select time range added in previous step

Click **Commit** to save changes.

Routing Policy Details

CommitCancel

General

* Name: dv2000-tr1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
dv2000-tr1	10.64.10.245	SIP Trunk	DuVoice DV2000

Time of Day

AddRemoveView Gaps/Overlaps

1 ItemFilter: Enable

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	TimeRange	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select : All, None

6.10. Add Dial Patterns – Communication Manager

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General**:

- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number
- Set **Domain** to domain configured on **Section 6.1**

Under **Originating Locations and Routing Policies**:

- Click **Add** and select originating location and Communication Manager routing policy as configured in **Section 6.8**

Click **Commit** to save changes.

Note: For Compliance testing, dialed number of 25xxx were used to route calls to Communication Manager. Thus, pattern, min and max values were all set to 5.

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item							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"/>	-ALL-		cm-tr1		<input type="checkbox"/>	cm-tr1	
Select : All , None							

6.11. Add Dial Patterns – DuVoice

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General**:

- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number
- Set **Domain** to **–All–**

Under **Originating Locations and Routing Policies**:

- Click **Add** and select originating location and DuVoice DV2000 routing policy as configured in **Section 6.9**

Click **Commit** to save changes.

Note: For Compliance testing, dialed number of 25099 was used to route calls to DuVoice. Thus, pattern was set to 25099 and, min and max values were set to 5.

Dial Pattern Details

[Commit](#) [Cancel](#)

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

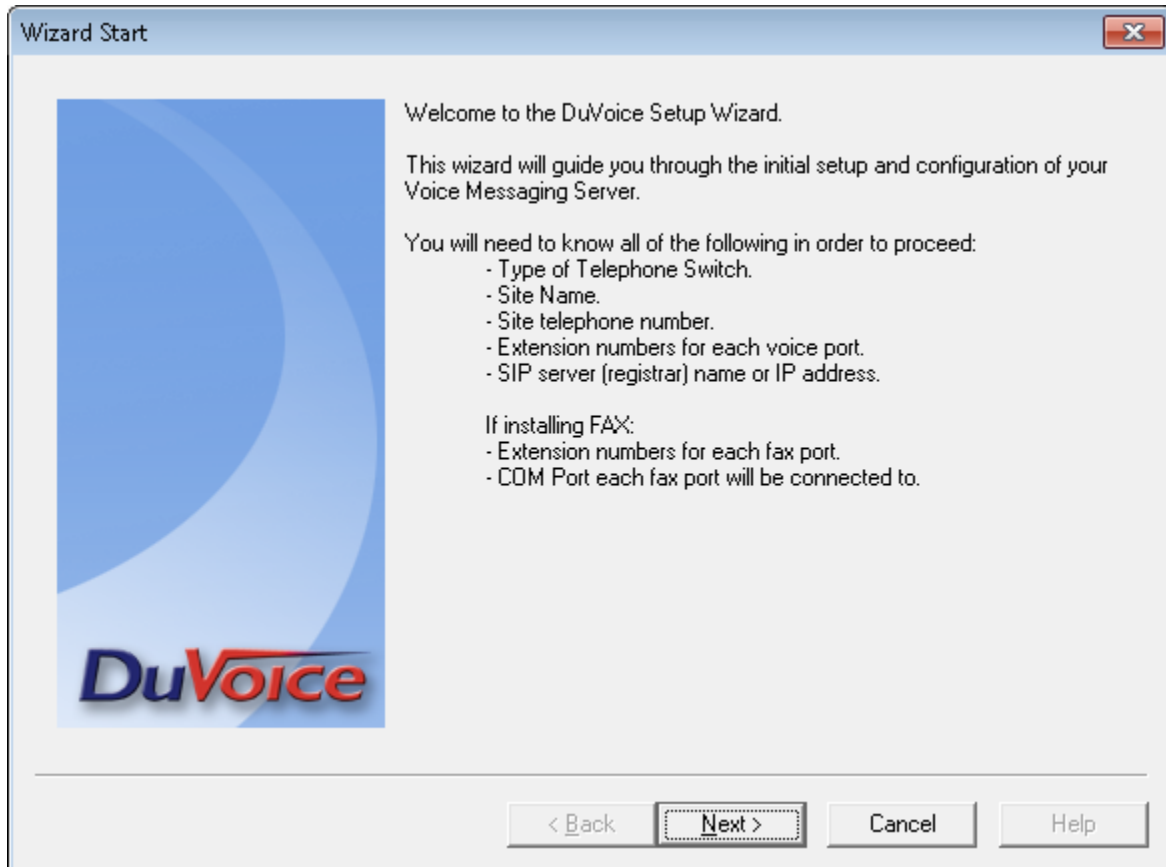
[Add](#) [Remove](#)

3 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"/>	Test Room 1		dv2000-tr1	0	<input type="checkbox"/>	dv2000-tr1	
<input type="checkbox"/>	Test Room 2		dv2000-tr1	0	<input type="checkbox"/>	dv2000-tr1	
<input type="checkbox"/>	Test Room 3		dv2000-tr1	0	<input type="checkbox"/>	dv2000-tr1	
Select : All, None							

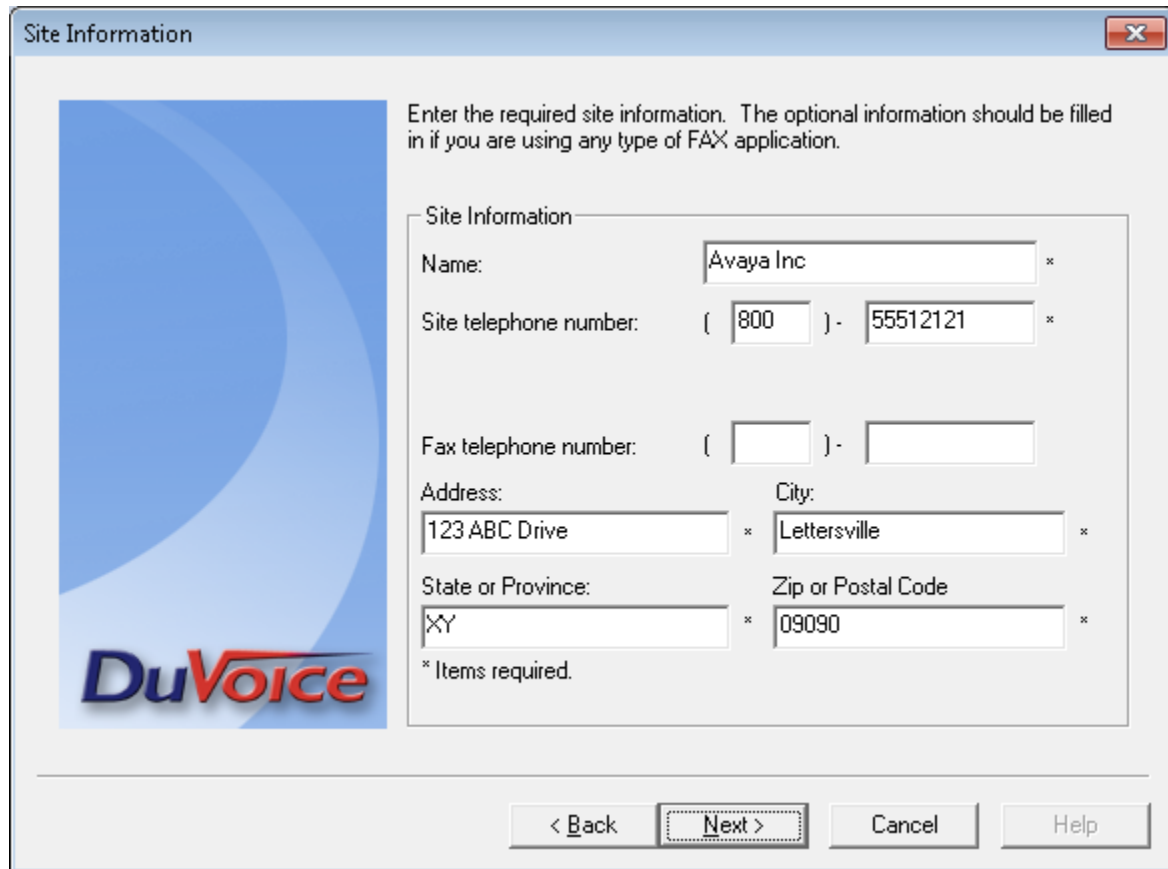
7. Configure DuVoice

During Compliance Testing, DuVoice DV2000 was installed on a Windows 7 Enterprise server. To configure SIP connectivity to Session Manager, locate the SETUP.exe file for DuVoice DV2000 and open it. SETUP.exe can be found in the installation directory for DuVoice.

On the **Wizard Start** window select **Next**



On the **Site Information** window, fill in the fields marked with * and click **Next**.



The screenshot shows a 'Site Information' window with a blue header bar and a close button. On the left is a blue graphic with the 'DuVoice' logo. The main area contains a form with the title 'Site Information' and a subtitle: 'Enter the required site information. The optional information should be filled in if you are using any type of FAX application.' The form fields are: 'Name' (Avaya Inc, marked with *), 'Site telephone number' (800-55512121, marked with *), 'Fax telephone number' (empty), 'Address' (123 ABC Drive, marked with *), 'City' (Lettersville, marked with *), 'State or Province' (XY, marked with *), and 'Zip or Postal Code' (09090, marked with *). A note '* Items required.' is at the bottom of the form. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Site Information

Enter the required site information. The optional information should be filled in if you are using any type of FAX application.

Site Information

Name: Avaya Inc *

Site telephone number: (800) - 55512121 *

Fax telephone number: () -

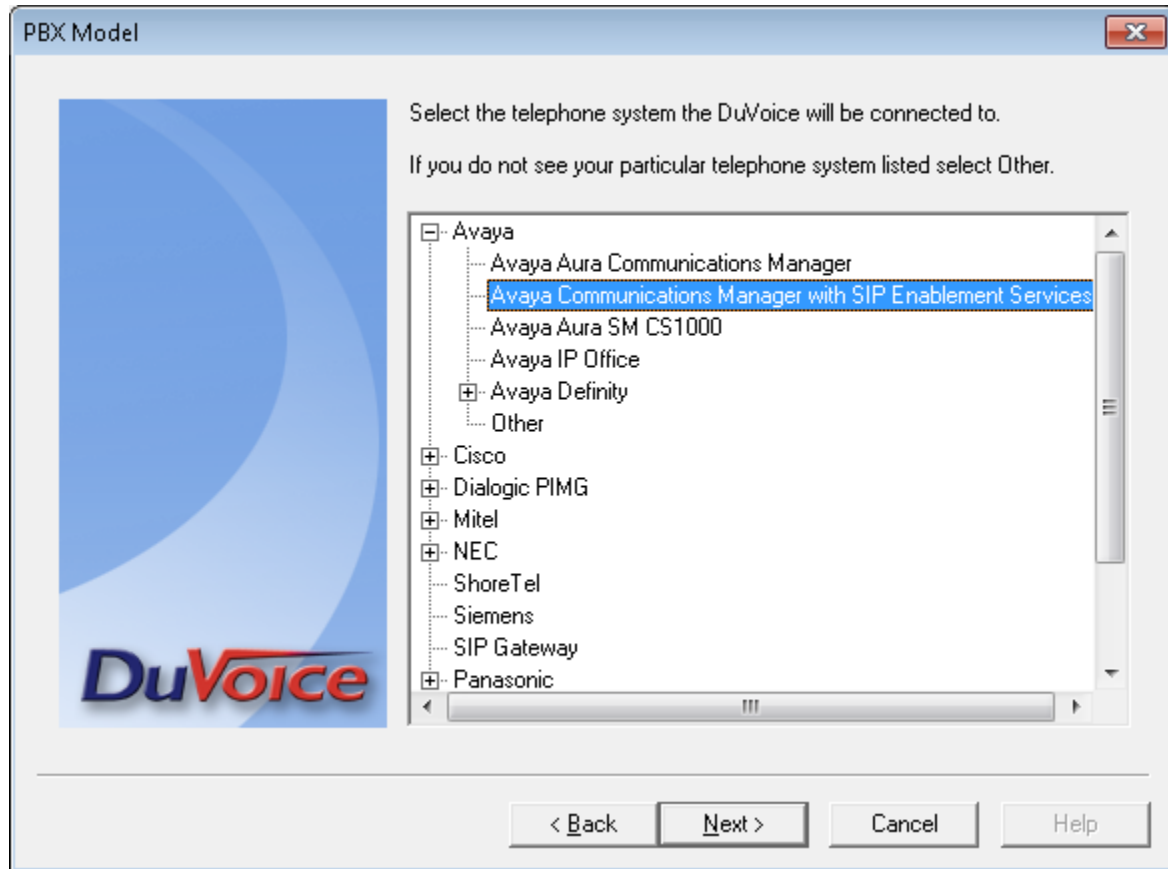
Address: 123 ABC Drive * City: Lettersville *

State or Province: XY * Zip or Postal Code: 09090 *

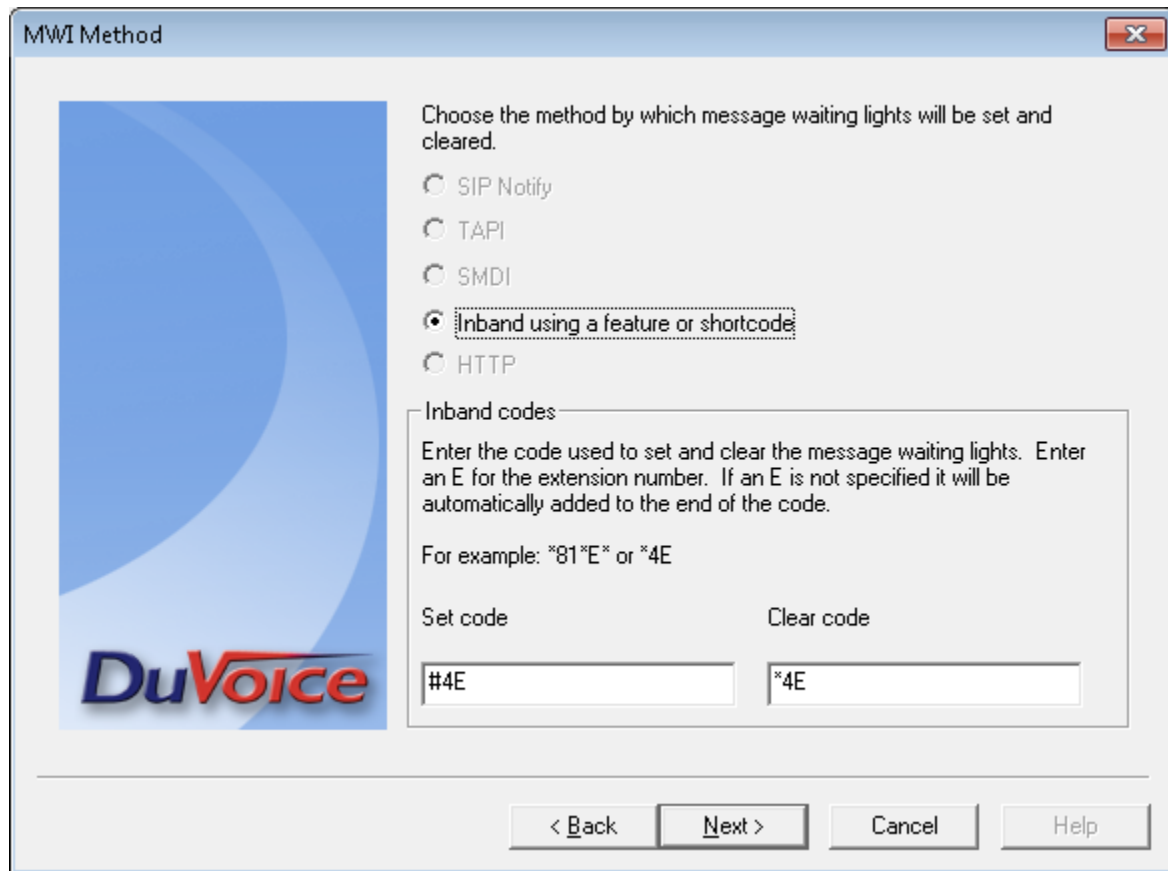
* Items required.

< Back Next > Cancel Help

On the **PBX Model** window, select **Avaya → Avaya Communication Manager with SIP Enablement Services** and click **Next**.



On the **MWI Method** window, accept the default values and click **Next**. Please note that MWI method will be changed to SIP in a later section.



The image shows a Windows-style dialog box titled "MWI Method". On the left is a blue graphic with the "DuVoice" logo. The main area contains a list of radio buttons for selecting the MWI method: "SIP Notify", "TAPI", "SMDI", "Inband using a feature or shortcode" (which is selected), and "HTTP". Below this is a section titled "Inband codes" with instructions: "Enter the code used to set and clear the message waiting lights. Enter an E for the extension number. If an E is not specified it will be automatically added to the end of the code. For example: *81*E* or *4E". There are two input fields: "Set code" containing "#4E" and "Clear code" containing "*4E". At the bottom are four buttons: "< Back", "Next >", "Cancel", and "Help".

MWI Method

Choose the method by which message waiting lights will be set and cleared.

- ☐ SIP Notify
- ☐ TAPI
- ☐ SMDI
- ☒ Inband using a feature or shortcode
- ☐ HTTP

Inband codes

Enter the code used to set and clear the message waiting lights. Enter an E for the extension number. If an E is not specified it will be automatically added to the end of the code.

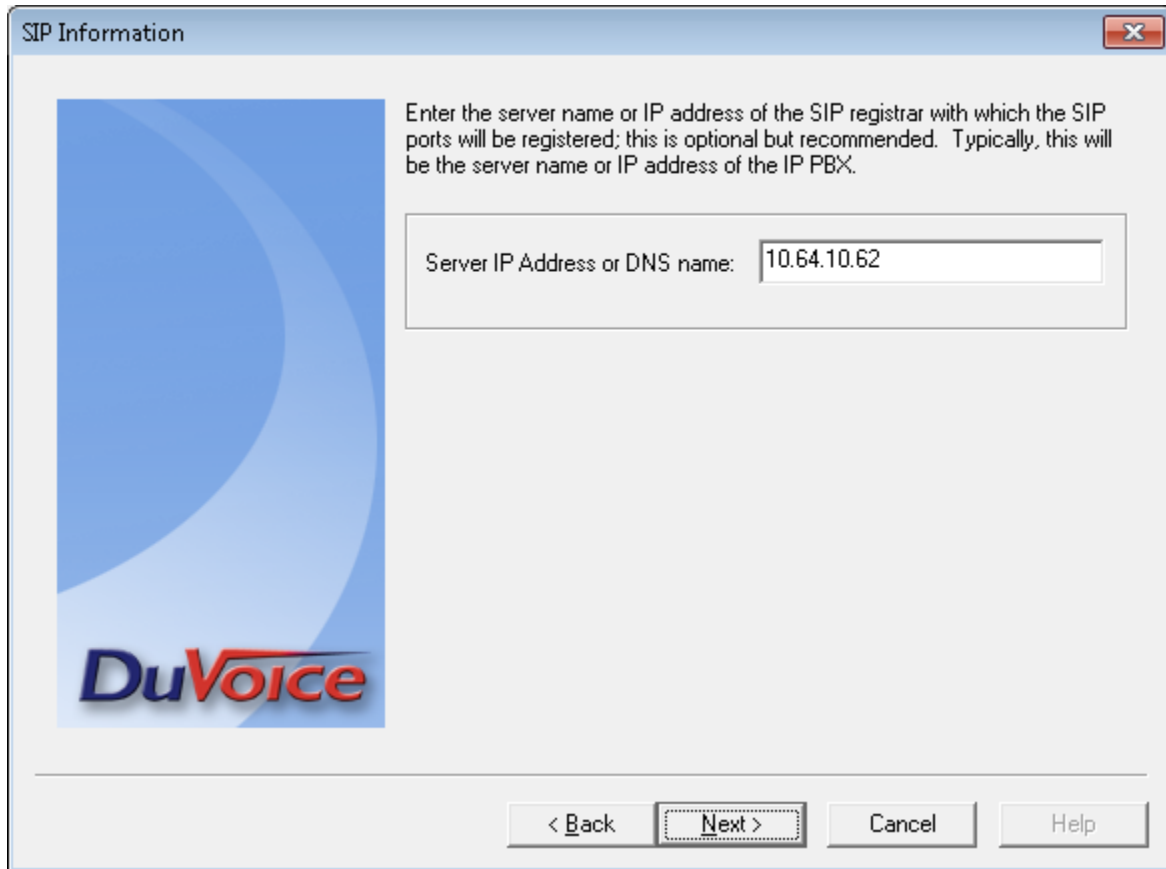
For example: *81*E* or *4E

Set code Clear code

#4E *4E

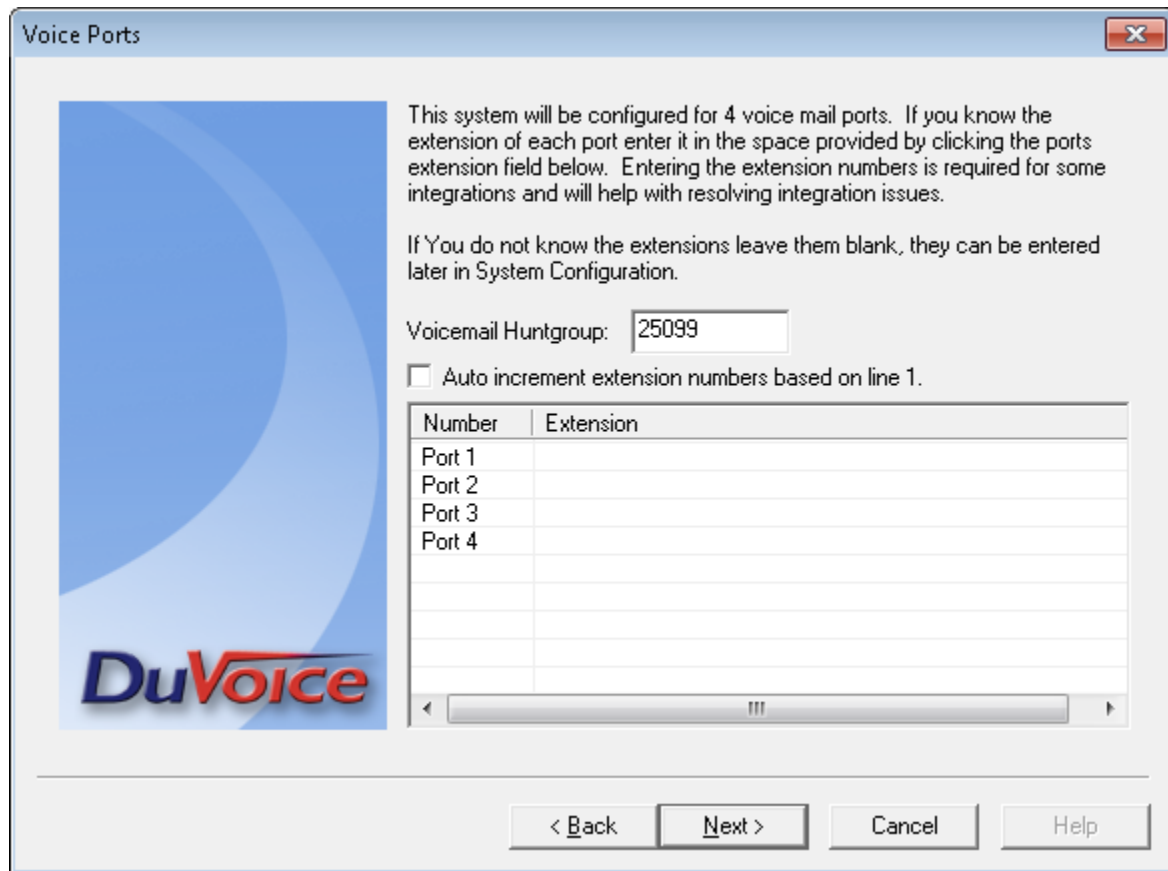
< Back Next > Cancel Help

On the **SIP Information** window, type in the Session Manager IP Address in **Server IP Address or DNS Name** field and click **Next**.



The screenshot shows a window titled "SIP Information" with a close button in the top right corner. On the left side, there is a blue graphic with the "DuVoice" logo. The main area contains instructional text: "Enter the server name or IP address of the SIP registrar with which the SIP ports will be registered; this is optional but recommended. Typically, this will be the server name or IP address of the IP PBX." Below this text is a text input field labeled "Server IP Address or DNS name:" containing the IP address "10.64.10.62". At the bottom of the window, there are four buttons: "< Back", "Next >", "Cancel", and "Help". The "Next >" button is highlighted with a dashed border.

On the **Voice Ports** window, type in the Hunt Group that was configured in Communication Manager in **Voicemail Huntgroup** field and click **Next**.



The 'Voice Ports' window features a blue header bar with the title 'Voice Ports' and a close button. On the left is a blue graphic with the 'DuVoice' logo. The main area contains instructional text about configuring 4 voice mail ports and a 'Voicemail Huntgroup' text box containing '25099'. Below this is a checkbox for 'Auto increment extension numbers based on line 1.' and a table with columns 'Number' and 'Extension' for ports 1 through 4. At the bottom are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

This system will be configured for 4 voice mail ports. If you know the extension of each port enter it in the space provided by clicking the ports extension field below. Entering the extension numbers is required for some integrations and will help with resolving integration issues.

If You do not know the extensions leave them blank, they can be entered later in System Configuration.

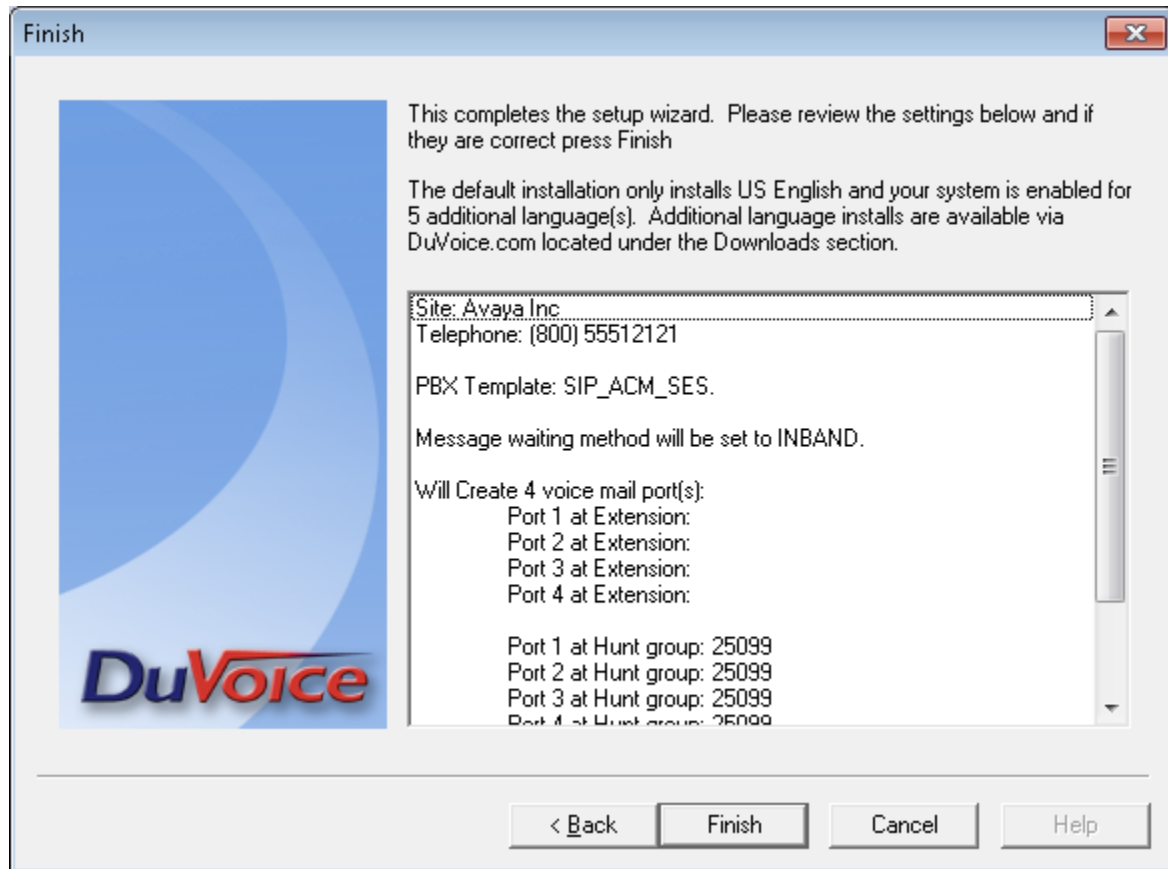
Voicemail Huntgroup:

☐ Auto increment extension numbers based on line 1.

Number	Extension
Port 1	
Port 2	
Port 3	
Port 4	

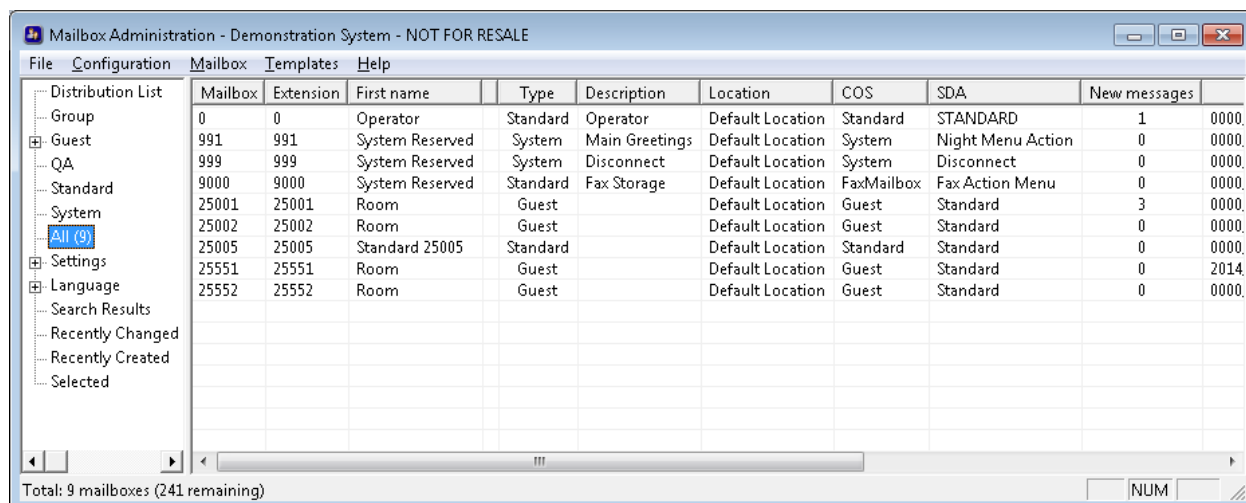
< Back Next > Cancel Help

The final screen shows the configuration, click **Finish**.

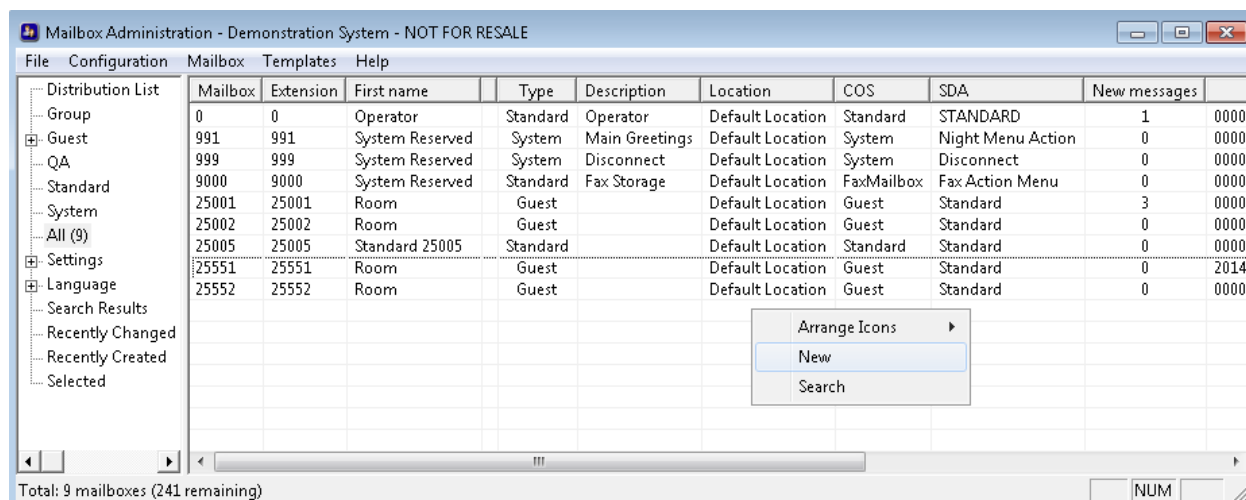


7.1. Configure MailBox

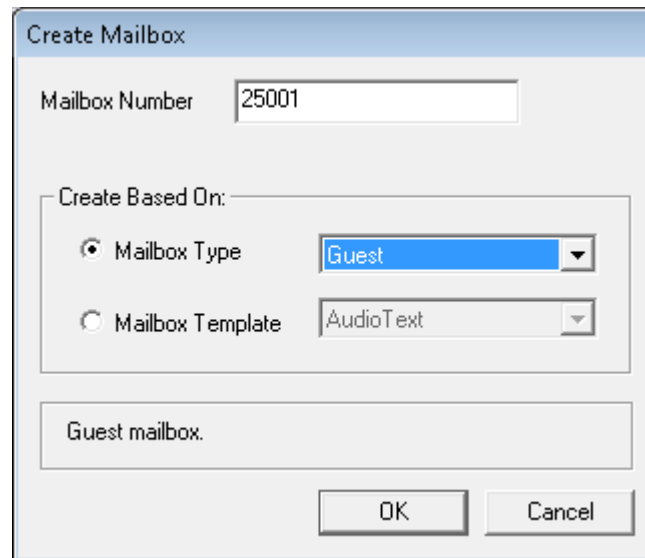
To configure mail boxes for guests, open **Mailbox Administration**, and select **All** in the left pane. A shortcut icon for **Mailbox Administration** can be found on Desktop of the server.



To add a mail box, right click on the right pane and select **New**.

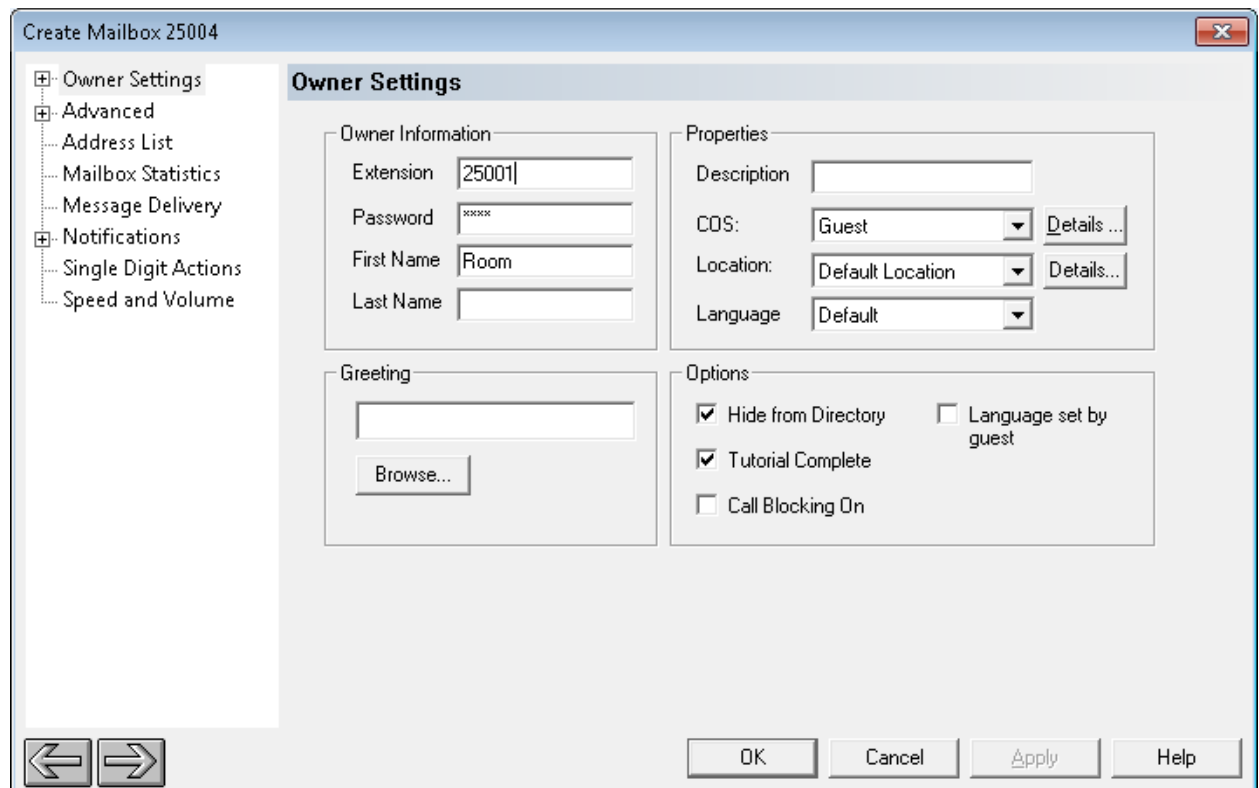


On the **Create Mailbox** window, enter the station extension and select **Guest** for **Mailbox Type**, and click **OK**.



The 'Create Mailbox' dialog box is shown. It has a title bar 'Create Mailbox'. Inside, there is a 'Mailbox Number' field with the value '25001'. Below this is a section 'Create Based On:' with two radio buttons. The first radio button is selected and labeled 'Mailbox Type', with a dropdown menu showing 'Guest'. The second radio button is labeled 'Mailbox Template' with a dropdown menu showing 'AudioText'. Below these is a text field containing 'Guest mailbox.'. At the bottom are 'OK' and 'Cancel' buttons.

On the next window, accept default values and click **OK**.



The 'Create Mailbox 25004' window is shown. It has a title bar 'Create Mailbox 25004'. On the left is a tree view with the following items: Owner Settings (selected), Advanced, Address List, Mailbox Statistics, Message Delivery, Notifications, Single Digit Actions, and Speed and Volume. The main area is titled 'Owner Settings' and contains several sections: 'Owner Information' with fields for Extension (25001), Password (xxxxx), First Name (Room), and Last Name; 'Properties' with fields for Description, COS (Guest), Location (Default Location), and Language (Default), each with a 'Details...' button; 'Greeting' with a text field and a 'Browse...' button; and 'Options' with checkboxes for 'Hide from Directory' (checked), 'Tutorial Complete' (checked), 'Call Blocking On' (unchecked), and 'Language set by guest' (unchecked). At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons. There are also left and right arrow buttons on the bottom left.

8.

Verification Steps

This section describes verification steps that may be used to verify SIP connectivity between DuVoice DV2000 and Session Manager.

8.1. Avaya Aura® Session Manager

On the System Manager, navigate to **Home → Element → Session Manager → System Station → SIP Entity Monitoring** (not shown).

Verify the **Conn. Status** and **Reason Code** are **Up** and **200 OK**.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: dv2000-tr1

Status Details for the selected Session Manager:

Summary View

[illegible]

9. Conclusion

DuVoice DV2000 passed compliance testing. These Application Notes describe the procedures required to configure DuVoice DV2000 to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support the network shown in **Figure 1**.

10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager, Release 6.0, 03-300509 Issue 6.3, June 2014*
- [2] *Administering Avaya Aura® Session Manager, June 2014, Release 6.3.*

Product documentation for DuVoice DV2000 may be directly obtained from DuVoice.

©2014 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.