



Avaya Solution & Interoperability Test Lab

Application Notes for Vocantas Utilities OnCall with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Vocantas Utilities OnCall to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

Vocantas Utilities OnCall is a voice response solution designed for the requirements of utilities companies. In the compliance testing, Vocantas Utilities OnCall used SIP trunks to Avaya Aura® Session Manager for connections with the PSTN and for transfer of incoming calls to agents on Avaya Aura® Communication Manager.

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 Vocantas Utilities OnCall to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

Vocantas Utilities OnCall is a voice response solution designed for the requirements of utilities companies. In the compliance testing, Vocantas Utilities OnCall used SIP trunks to Avaya Aura® Session Manager for connections with the PSTN and for transfer of incoming calls to agents on Avaya Aura® Communication Manager.

Incoming trunk calls destined for Vocantas Utilities OnCall are delivered by Avaya Aura® Communication Manager to Avaya Aura® Session Manager, and by Avaya Aura® Session Manager to Vocantas Utilities OnCall via SIP trunks. Vocantas Utilities OnCall answers the incoming call and plays the appropriate greeting, and uses DTMF tones from the calling party to determine the service to provide.

When requested by the calling party, Vocantas Utilities OnCall can perform blind transfer of the call to agents on Avaya Aura® Communication Manager. Vocantas Utilities OnCall can also initiate outbound calls to the PSTN, to notify customers with pertinent account information.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established between PSTN users and Utilities OnCall. Call controls were performed from the PSTN users to verify the various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to Utilities OnCall.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, G.711, G.729, codec negotiation, media shuffling, drop, DTMF, blind transfer to internal agents for assistance, outbound to PSTN users for customer account notification, simultaneous calls, and reporting.

The serviceability testing focused on verifying the ability of Utilities OnCall to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Utilities OnCall.

2.2. Test Results

All test cases were executed and verified.

2.3. Support

Technical support on Utilities OnCall can be obtained through the following:

- **Phone:** (877) 271-8853
- **Email:** info@vocantas.com

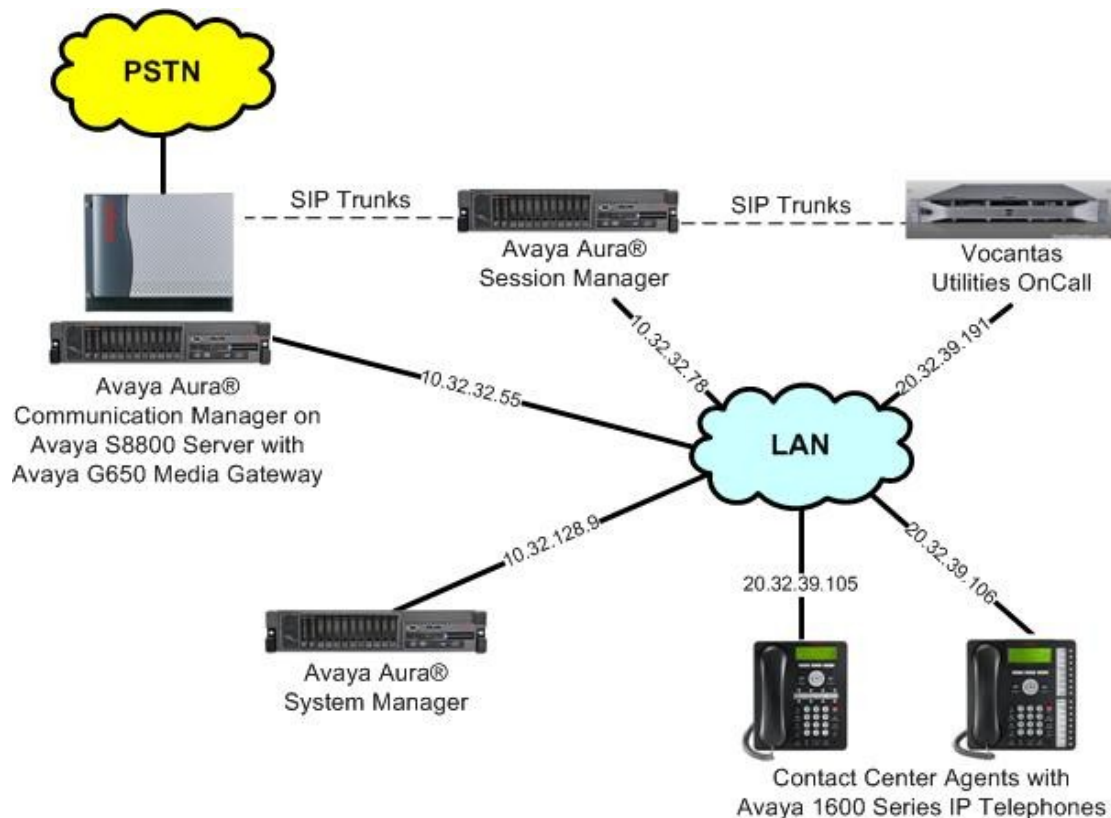
3. Reference Configuration

As shown in the test configuration below, SIP trunks are used between Utilities OnCall and Session Manager, to connect to users on the PSTN and to transfer to agents on Communication Manager. The Utilities OnCall server used the Dialogic Host Media Processing card for SIP messaging exchanges with Session Manager.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing. In the compliance testing, extensions of “61xxx” were associated with Utilities OnCall, and extensions of “62xxx-69xxx” were associated with resources on Communication Manager.

The detailed administration of basic connectivity between Communication Manager and Session Manager, and of contact center devices are not the focus of these Application Notes and will not be described.

The contact center devices used in the compliance testing consists of a skill group with extension “65555”, and two agent extensions “65001-2”.



4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP5.01 (R016x.00.1.510.1-19303)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW040 HW20 FW122
Avaya Aura® Session Manager	6.1 SP5
Avaya Aura® System Manager	6.1 SP5
Avaya 1600 Series IP Telephones (H.323)	1.3
Vocantas Utilities OnCall <ul style="list-style-type: none">Dialogic Host Media Processing	2.0 3.0 Service Update 307

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, the existing SIP trunk group for communication with Session Manager and the associated signaling group, network region, and codec set were used for integration with Vocantas.

5.1. Verify License

Log in to 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.

change system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	7
Maximum Concurrently Registered IP Stations:		18000	2
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:		18000	1
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	20
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0

5.2. Administer SIP Trunk Group

Use the “change trunk-group n” command, where “n” is the existing SIP trunk group number used to reach Session Manager, in this case “5”.

For **Group Name**, update as desired to reflect the same trunk group used to reach Session Manager and Vocantas. For **Number of Members**, enter sufficient number for simultaneous calls with Session Manager and Vocantas. Make a note of the **Signaling Group** number.

change trunk-group 5		Page 1 of 21	
TRUNK GROUP			
Group Number: 5	Group Type: sip	CDR Reports: y	
Group Name: SIP Trunk to SM/Vocantas	COR: 1	TN: 1	TAC: 1005
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 5	
		Number of Members: 10	

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

change trunk-group 5		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	

5.3. Administer SIP Signaling Group

Use the “change signaling-group n” command, where “n” is the existing SIP signaling group number used by the SIP trunk group from **Section 5.2**.

For **DTMF over IP**, enter “rtp-payload”. For **Direct IP-IP Audio Connections**, enter “y”. Make a note of the **Far-end Network Region** number, and the **Far-end Domain** value. Note that **Transport Method** is set to “tcp” for troubleshooting purposes, also note the values of **Near-end Listen Port** and **Far-end Listen Port**, which will be used later.

```
change signaling-group 5                               Page 1 of 1
                                     SIGNALING GROUP

Group Number: 5                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
Q-SIP? n                            SIP Enabled LSP? n
IP Video? n                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: Clan-1           Far-end Node Name: S8800-SM-SIG
Near-end Listen Port: 5060           Far-end Listen Port: 5060
                                     Far-end Network Region: 1
                                     Far-end Secondary Node Name:
Far-end Domain: br110.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload           RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3   IP Audio Hairpinning? n
Enable Layer 3 Test? y               Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

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 5.3**.

For **Name**, update as desired to reflect the same network region used to reach Vocantas. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. In the compliance testing, the same network region was used for all Avaya users. Make a note of the **Codec Set** number.

```
change ip-network-region 1                          Page 1 of 20
                                     IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: br110.com
Name: Main/Vocantas
MEDIA PARAMETERS
Codec Set: 1      Intra-region IP-IP Direct Audio: yes
                  Inter-region IP-IP Direct Audio: yes
                  IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
```

5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the existing codec set number used by the IP network region from **Section 5.4**. Update the audio codec types in the **Audio Codec** fields as desired. The screenshot below shows the settings used in the compliance testing.

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.729	n	2	20
2:	G.711MU	n	2	20
3:				
4:				
5:				
6:				
7:				

5.6. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is the existing route pattern number to reach Session Manager, in this case “5”. For **Pattern Name**, update as desired to reflect the same route pattern used to reach Session Manager and Vocantas. For **Secure SIP**, make certain the value is “n”.

change route-pattern 5														Page		1 of 3									
Pattern Number: 5														Pattern Name: To SM/Vocantas											
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												n	user										
2:														n	user										
3:														n	user										
4:														n	user										
5:														n	user										
6:														n	user										
														BCC VALUE		TSC	CA-TSC	ITC BCIE		Service/Feature		PARM	No.	Numbering	LAR
														0	1	2	M	4	W	Request				Dgts Format	
																						Subaddress			
1:	y	y	y	y	y	n	n	rest								none									

5.7. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Vocantas. Add an entry for the trunk group defined in **Section 5.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 5 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	6	5		5	Total Administered: 1 Maximum Entries: 540

5.8. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 61xxx to Vocantas. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 61xxx, as shown below.

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Node Net Conv Num	
61	5	0		aar n	

5.9. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to route calls to 61xxx. In the example shown below, calls with digits 61xxx will be routed using route pattern “5” from **Section 5.6**. Set the **Call Type** to “unku”, to prevent “+” being added as a prefix.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					Percent Full: 2
Location: all					
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num ANI Req'd
61	5	5	5	unku	n

5.10. Administer ISDN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing ISDN trunk group number used to reach the PSTN, in this case “10”. Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from Vocantas to be modified.

change trunk-group 10			Page 3 of 21	
TRUNK FEATURES				
ACA Assignment? n		Measured: none	Wideband Support? n	
		Internal Alert? n	Maintenance Tests? y	
		Data Restriction? n	NCA-TSC Trunk Member:	
		Send Name: y	Send Calling Number: y	
Used for DCS? n			Send EMU Visitor CPN? n	
Suppress # Outpulsing? n		Format: public		
Outgoing Channel ID Encoding: preferred		UII IE Treatment: service-provider		
		Replace Restricted Numbers? n		
		Replace Unavailable Numbers? n		
		Send Connected Number: n		
Network Call Redirection: none		Hold/Unhold Notifications? n		
Send UII IE? y		Modify Tandem Calling Number: tandem-cpn-form		
Send UCID? n				
Send Codeset 6/7 LAI IE? y		Dsl Echo Cancellation? n		
Apply Local Ringback? n		US NI Delayed Calling Name Update? n		
Show ANSWERED BY on Display? y				
		Network (Japan) Needs Connect Before Disconnect? n		
DSN Term? n				

5.11. Administer Tandem Calling Party Number

Use the “change tandem-calling-party-num” command, to define the calling party number to send to the PSTN for tandem calls from Vocantas.

In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 10 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

change tandem-calling-party-num					Page	1 of	8
CALLING PARTY NUMBER CONVERSION							
FOR TANDEM CALLS							
CPN		Trk		Number			
Len	Prefix	Grp(s)	Delete	Insert	Format		
5	6	10		90884	pub-unk		

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 locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

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 the System Manager server. Log in using the appropriate credentials.

The screenshot shows the Avaya Aura® System Manager 6.1 login interface. At the top, the Avaya logo is on the left and the title "Avaya Aura® System Manager 6.1" is on the right. Below the title bar is a red navigation bar with the text "Home / Log On". The main heading is "Log On". On the left side, there is a box containing the text: "Recommended access to System Manager is via FQDN." followed by a link "Go to central login for Single Sign-On". Below this, it says "If IP address access is your only option, then note that authentication will fail in the following cases:" followed by a bulleted list: "• First time login with 'admin' account" and "• Expired/Reset passwords". On the right side, there are two input fields labeled "User ID:" and "Password:". At the bottom right, there are two buttons: "Log On" and "Cancel". Below the "Cancel" button is a link "Change Password".

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements > Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing > Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Vocantas.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing - Introduction to Network Routing Policy Help ?

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Locations - Location Details Help ?

Location Details

General

* Name: Vocantas-Loc

Notes: Vocantas Location

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
20.32.29.191	Utilities OnCall

6.3. Administer Adaptations

Select **Routing > Adaptations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new adaptation for Vocantas.

The **Adaptation Details** screen is displayed. In the **General** sub-section, enter a descriptive **Adaptation name**. For **Module name**, select “DigitConversionAdapter”.

For **Module parameter**, enter “odstd=20.32.39.191”, where “20.32.39.191” is the IP address of Vocantas. This will set the destination domain for outgoing calls from Session Manager to the IP address of Vocantas, as required by Vocantas.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help | About | Change Password | Log off admin". A breadcrumb trail shows "Home / Elements / Routing / Adaptations - Adaptation Details". The left sidebar contains a menu with "Routing" selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Adaptation Details" and includes "Commit" and "Cancel" buttons. The "General" section contains the following fields: "Adaptation name" (Vocantas-Adaptation), "Module name" (DigitConversionAdapter), "Module parameter" (odstd=20.32.39.191), "Egress URI Parameters" (empty), and "Notes" (empty). Below this, there are two sections for digit conversion: "Digit Conversion for Incoming Calls to SM" and "Digit Conversion for Outgoing Calls from SM". Each section has "Add" and "Remove" buttons, a "0 Items Refresh" status, a "Filter: Enable" link, and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, and Notes.

6.4. Administer SIP Entities

Select **Routing > SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Vocantas.

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 Vocantas.
- **Type:** “Other”
- **Adaptation:** Select the Vocantas adaptation name from **Section 6.3**.
- **Location:** Select the Vocantas location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Name:** Vocantas

* **FQDN or IP Address:** 20.32.39.191

Type: Other

Notes:

Adaptation: Vocantas-Adaptation

Location: Vocantas-Loc

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

Select **Routing > Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for Vocantas.

The **Entity Links** screen is displayed. 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 “BR110-SM”.
- **Protocol:** The signaling group transport method from **Section 5.3**.
- **Port:** The signaling group listen port number from **Section 5.3**.
- **SIP Entity 2:** The Vocantas entity name from **Section 6.4**.
- **Port:** The signaling group listen port number from **Section 5.3**.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a breadcrumb trail: Home / Elements / Routing / Entity Links - Entity Links. Below the title is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row contains the following values: Name: BR110-SM2Vocantas, SIP Entity 1: BR110-SM, Protocol: TCP, Port: 5060, SIP Entity 2: Vocantas, Port: 5060, Connection Policy: Trusted, and Notes: (empty). Below the table, there is a message '* Input Required' and buttons for 'Commit' and 'Cancel'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* BR110-SM2Vocantas	* BR110-SM	TCP	* 5060	* Vocantas	* 5060	Trusted	

6.6. Administer Routing Policies

Select **Routing > Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for Vocantas.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Vocantas entity name from **Section 6.4** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) × [Home](#)

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details [Help ?](#) [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
Vocantas	20.32.39.191	Other	

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Ranking ¹	Name ²	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<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	Time Range 24/7

Select : All, None

6.7. Administer Dial Patterns

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 Vocantas.

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.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** The signaling group domain name from **Section 5.3**.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching Vocantas. In the compliance testing, the policy allowed for call origination from all locations, as shown below. Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

[Home / Elements / Routing / Dial Patterns - Dial Pattern Details](#)

Dial Pattern Details [Help ?](#) [Commit](#) [Cancel](#)

General

* **Pattern:** 61

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

SIP Domain: br110.com

Notes: Vocantas

Originating Locations and Routing Policies

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

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To-Vocantas	0	<input type="checkbox"/>	Vocantas	

Select : All, None

Denied Originating Locations

7. Configure Vocantas Utilities OnCall

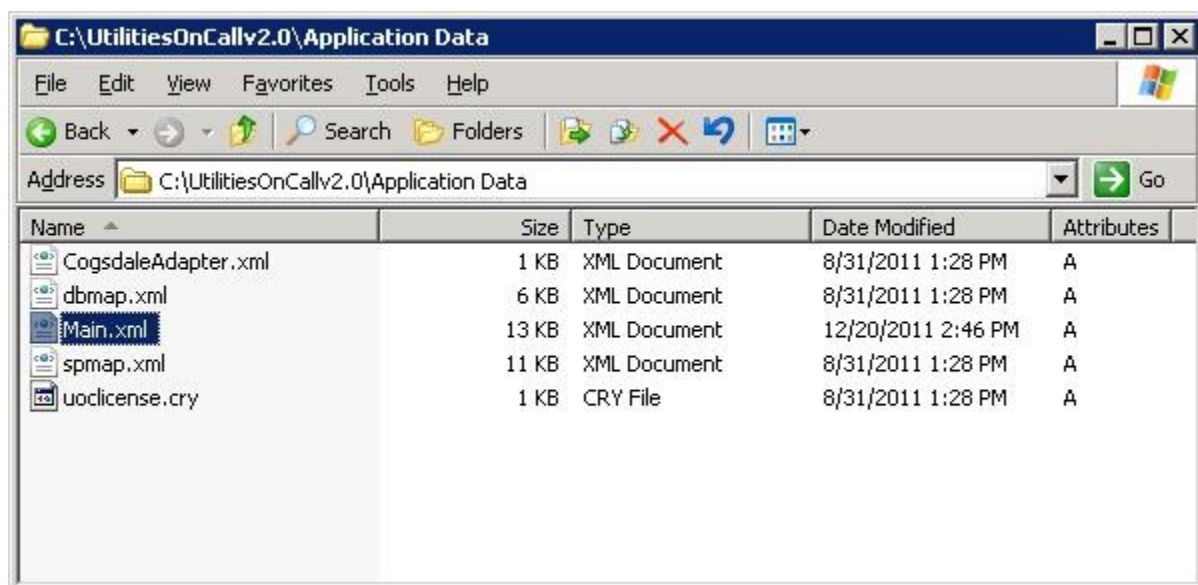
This section provides the procedures for configuring Utilities OnCall. The procedures include the following areas:

- Administer Main.xml
- Administer VBVoice

The configuration of Utilities OnCall is typically performed by Vocantas support engineers. The procedural steps are presented in these Application Notes for informational purposes.

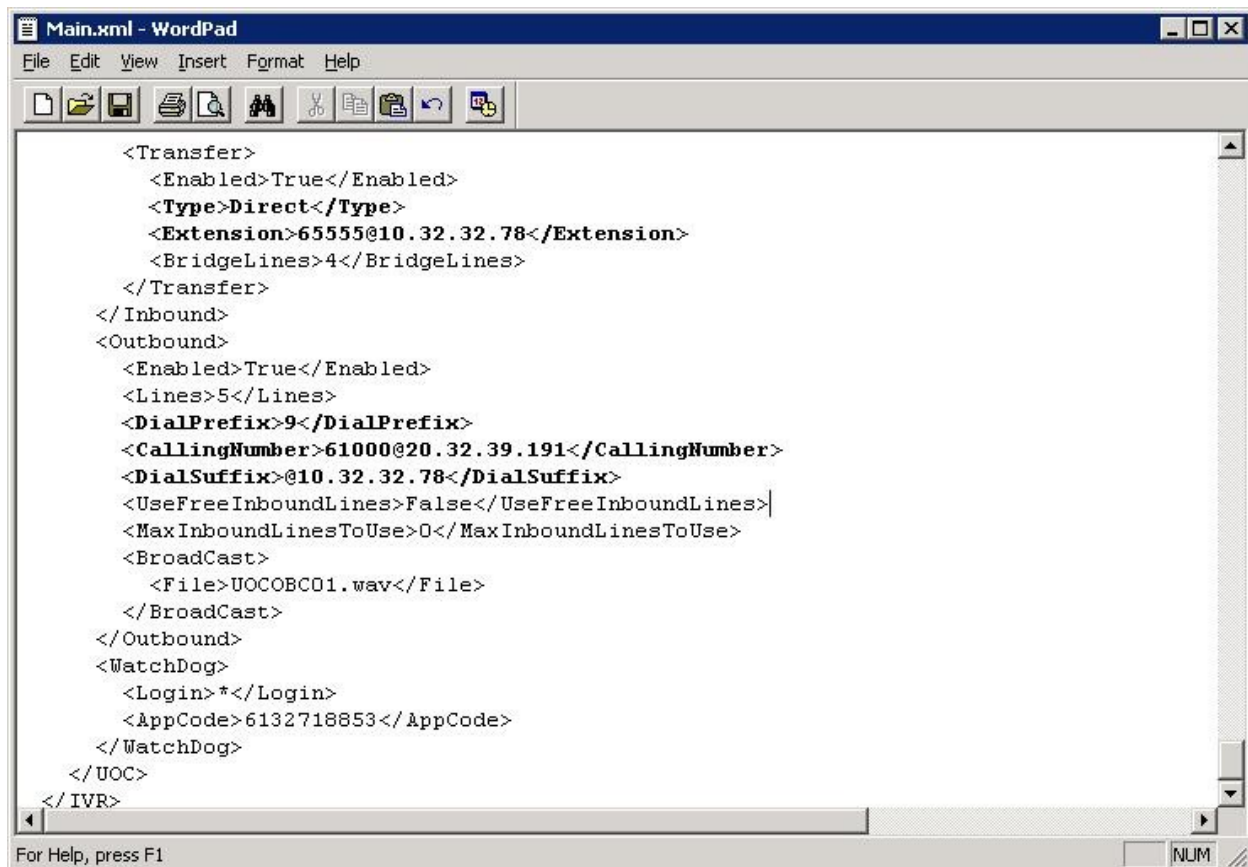
7.1. Administer Main.xml

From the Utilities OnCall server, navigate to the **C:\UtilitiesOnCallv2.0\Application Data** directory to locate the **Main.xml** file shown below.



Open the **Main.xml** file with the WordPad application. Scroll down to the bottom of the file. For transfer **Type**, enter “Direct”. For transfer **Extension**, enter “x@y” where “x” is the skill group extension from **Section 3**, and “y” is the IP address of Session Manager.

For outbound **DialPrefix**, enter the applicable ARS/AAR dialing prefix, in this case “9”. For outbound **CallingNumber**, enter “x@y” where “x” is an available extension assigned to Utilities OnCall, and “y” is the IP address of the Utilities OnCall server. For outbound **DialSuffix**, enter “@y” where “y” is the IP address of Session Manager.

A screenshot of the WordPad application window titled "Main.xml - WordPad". The window shows an XML configuration file with the following content:

```
<Transfer>
  <Enabled>True</Enabled>
  <Type>Direct</Type>
  <Extension>65555@10.32.32.78</Extension>
  <BridgeLines>4</BridgeLines>
</Transfer>
</Inbound>
<Outbound>
  <Enabled>True</Enabled>
  <Lines>5</Lines>
  <DialPrefix>9</DialPrefix>
  <CallingNumber>61000@20.32.39.191</CallingNumber>
  <DialSuffix>@10.32.32.78</DialSuffix>
  <UseFreeInboundLines>False</UseFreeInboundLines>
  <MaxInboundLinesToUse>0</MaxInboundLinesToUse>
  <BroadCast>
    <File>UOCBC01.wav</File>
  </BroadCast>
</Outbound>
<WatchDog>
  <Login>*</Login>
  <AppCode>6132718853</AppCode>
</WatchDog>
</UOC>
</IVR>
```

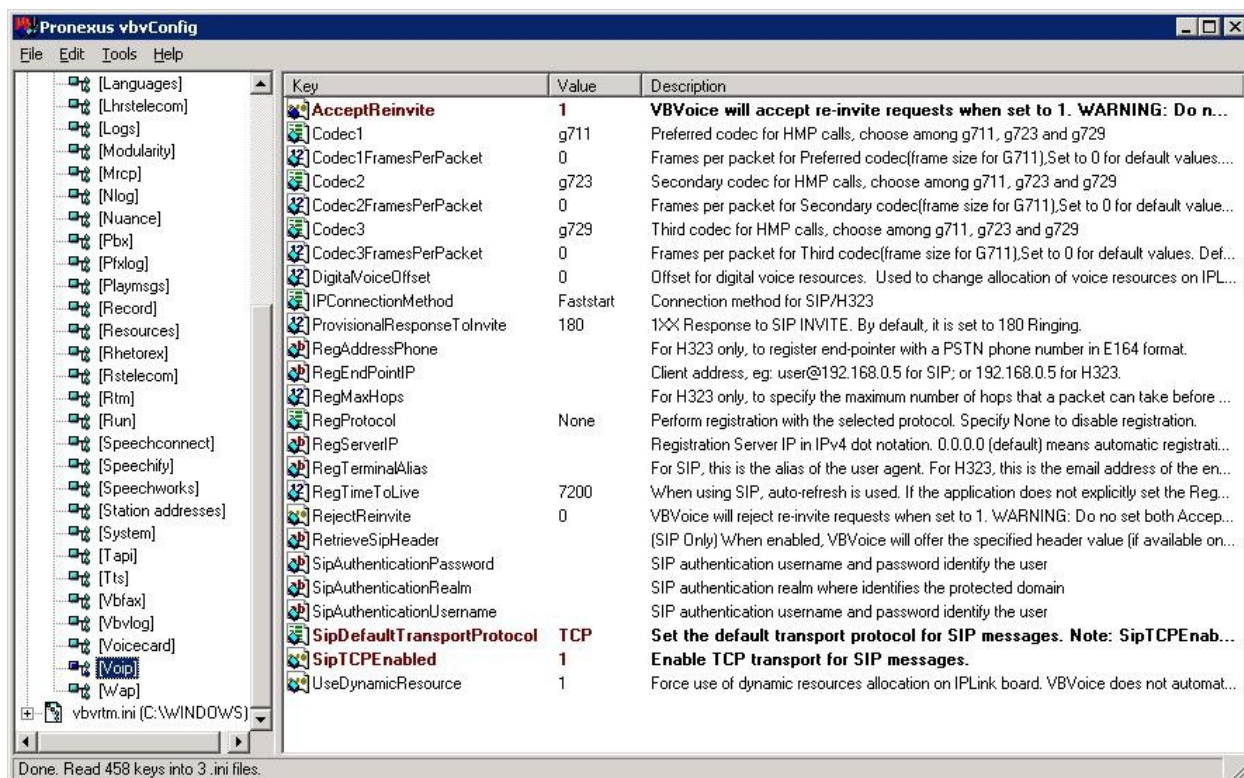
The WordPad interface includes a menu bar (File, Edit, View, Insert, Format, Help) and a toolbar with various icons. The status bar at the bottom indicates "For Help, press F1" and "NUM".

7.2. Administer VBVoice

Select **All Program > Pronexus > VBVConfig > Configure VBVoice**, to display the **Pronexus vbvConfig** screen below. Select **vbvoice.ini > Voip** in the left pane, to display a list of parameters in the right pane.

Right click on **AcceptReinvite**, and enable the parameter in the subsequent screen (not shown). Use similar procedure to enable **SipTCPEEnabled**, and set **SipDefaultTransportProtocol** to “TCP”. Retain the default values in the remaining fields.

The screenshot below shows the parameter settings used in the compliance testing.



8. Verification Steps

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

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 5.2**. 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
0005/001	T00083	in-service/idle	no
0005/002	T00084	in-service/idle	no
0005/003	T00085	in-service/idle	no
0005/004	T00086	in-service/idle	no
0005/005	T00087	in-service/idle	no
0005/006	T00045	in-service/idle	no
0005/007	T00046	in-service/idle	no
0005/008	T00047	in-service/idle	no
0005/009	T00048	in-service/idle	no
0005/010	T00049	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 5.3**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 5
```

STATUS SIGNALING GROUP	
Group ID:	5
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 below. Click on the Vocantas entity name from **Section 6.4**.

The screenshot displays the Avaya Aura® System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". A secondary bar shows "Session Manager" and "Home" buttons. The left sidebar contains a tree view with categories like "Session Manager", "Network Configuration", "Device and Location Configuration", "Application Configuration", "System Status", "Managed Bandwidth Usage", "Security Module Status", "Registration Summary", "User Registrations", and "SIP Performance". The "SIP Entity Monitoring" link under "System Status" is selected.

The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a sub-header "Entity Link Status for All Session Manager Instances". Below this is a "Run Monitor" button and a table with 3 items. The table has columns for "Session Manager Name", "Entity Links Down/Total", "Entity Links Partially Down", "SIP Entities - Monitoring Not Started", and "SIP Entities - Not Monitored". The rows are for "BR110-SM", "devcon-asm", and "Dev4 SM".

Below the table is a "Select : All, None" dropdown. Further down is the "All Monitored SIP Entities" section, which includes another "Run Monitor" button and a table with 21 items. The table has columns for "SIP Entity Name". The rows are for "sp3-cm", "sp3-cm-2", and "Vocantas", which is circled in red.

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
BR110-SM	5/7	0	0	0
devcon-asm	1/12	0	0	0
Dev4 SM	---	---	---	---

SIP Entity Name
sp3-cm
sp3-cm-2
Vocantas

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

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a breadcrumb trail: Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring. 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." and "All Entity Links to SIP Entity: Vocantas". A "Summary View" button is present. A table displays the connection status for one item, BR110-SM, with columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The Conn. Status and Link Status are both "Up".

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	BR110-SM	20.32.39.191	5060	TCP	Up	486 Busy Here	Up

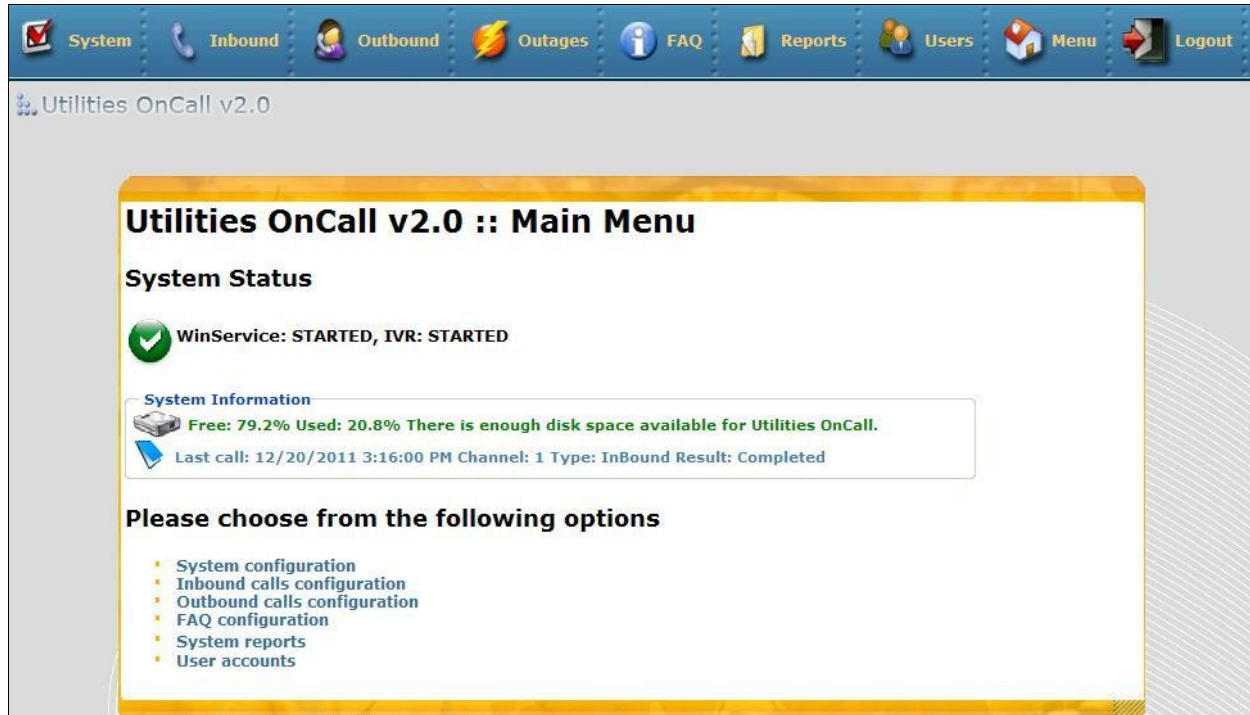
8.3. Verify Vocantas Utilities OnCall

Make and complete an incoming trunk call from the PSTN to Utilities OnCall.

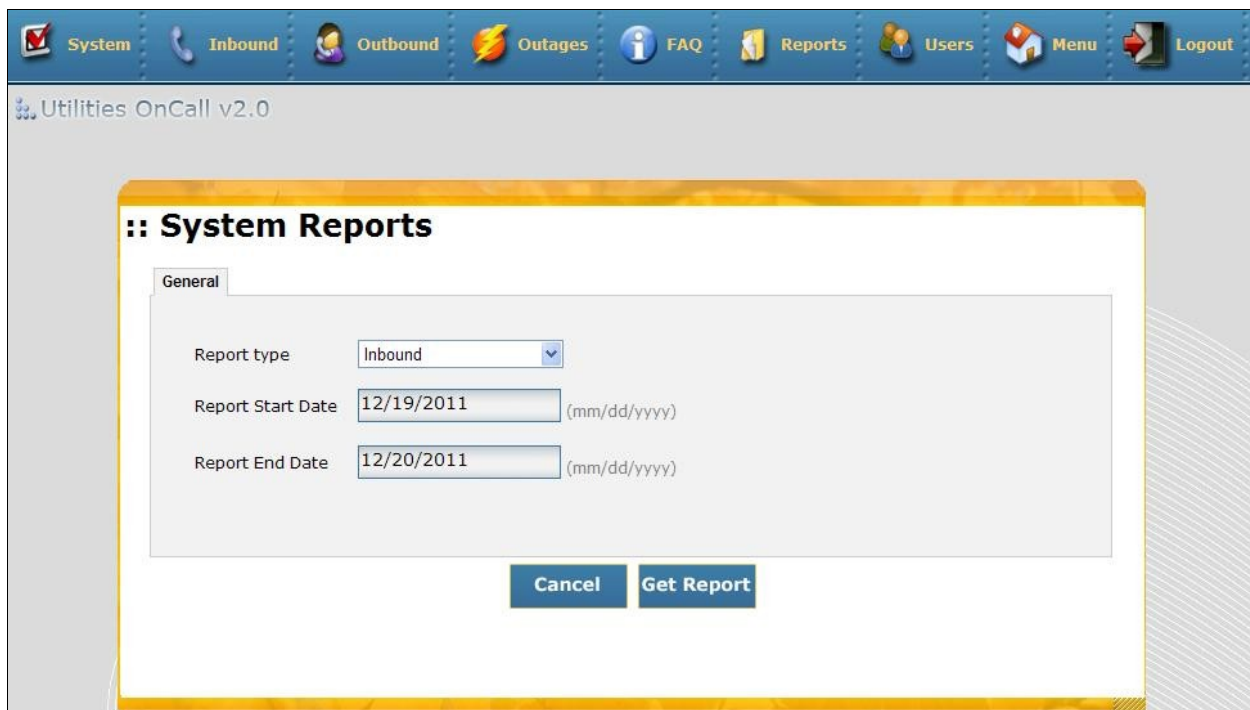
Access the Utilities OnCall web-based interface by using the URL “http://ip-address/uocgui/webgui” in an Internet browser window, where “ip-address” is the IP address of the Utilities OnCall server. The **Welcome to Utilities OnCall v2.0** screen is displayed. Log in using the appropriate credentials.

The screenshot shows the "Welcome to Utilities OnCall v2.0" login screen. It features a blue background with a white login form. The form includes fields for "Username" and "Password", a "Login" button, and a "Please login." prompt. At the bottom, it displays "Avaya DevConnect 1.800.000.0000 Ottawa".

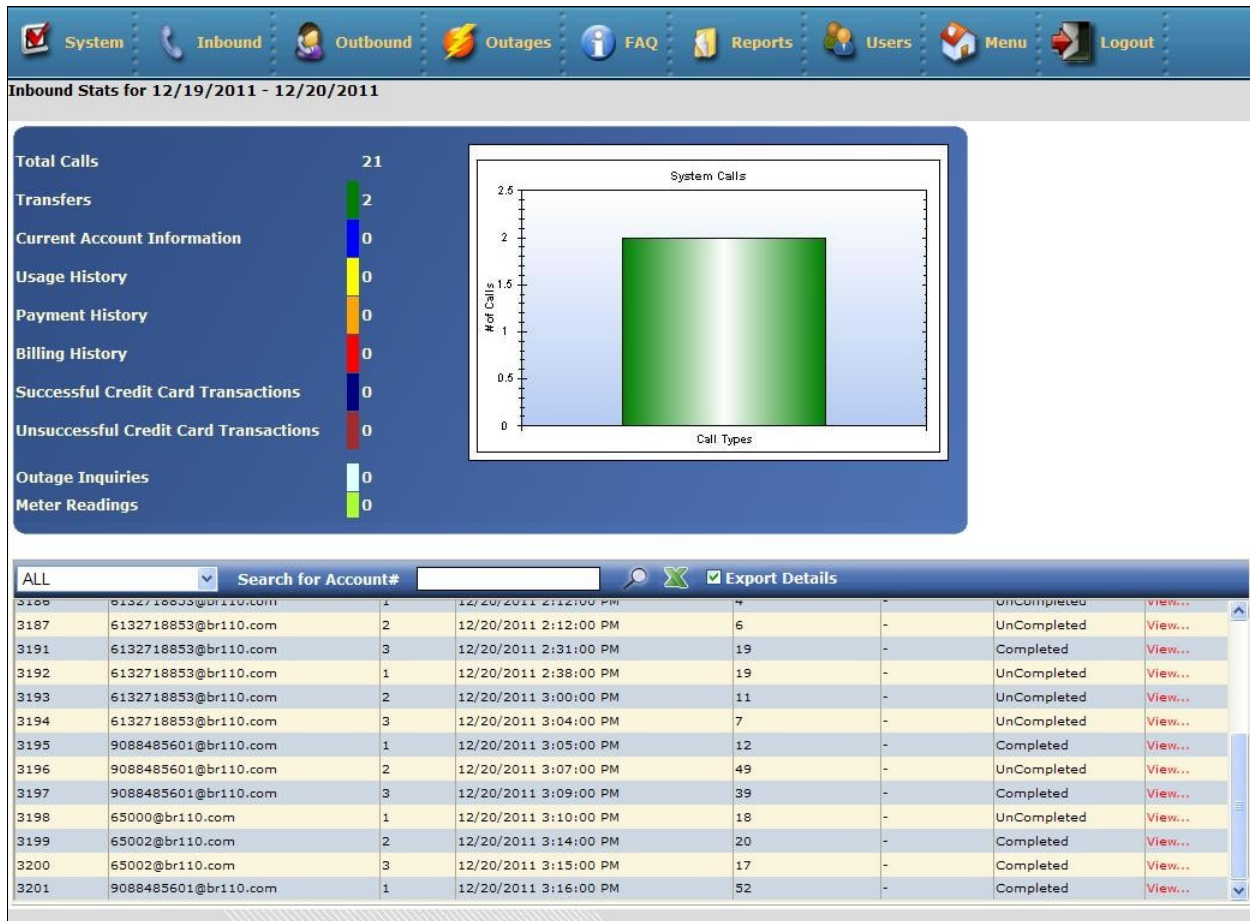
The **Utilities OnCall v2.0 Main Menu** screen is displayed. Select **Reports** from the top menu.



The **System Reports** screen is displayed next. Retain all default values and click **Get Report**.



The **Inbound Stats** report is displayed. Verify that there is an entry reflecting the last call, with proper values in the relevant fields, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Vocantas Utilities OnCall to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Session Manager. All feature and serviceability test cases were completed.

10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Administering Avaya Aura™ Session Manager*, Document Number 03-603324, Issue 3, Release 6.0, August 2010, available at <http://support.avaya.com>.
3. *Vocantas Utilities OnCall Administrator and User Guide*, 2011, available upon request to Vocantas Support.

©2012 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.