



Avaya Solution & Interoperability Test Lab

Application Notes for Omilia OCP Conversational Voice Service Cloud Solution 1.0 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Environment 8.1.2 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Omilia OCP Conversational Voice Service Cloud Solution 1.0 to interoperate with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Environment 8.1.2.

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

Omilia OCP Conversational Voice Service Cloud Solution provides a full stack of building blocks for conversational IVR virtual assistants. Omilia OCP Conversational Voice Service Cloud Solution IVR virtual assistants can engage in true end-to-end conversations in natural language - customers can speak freely and there is no predetermined flow or structure.

Omilia OCP Conversational Voice Service Cloud Solution Main components:

- DiaManT, a dialog management tool which drives conversational interactions with users from start to finish.
- deepASR & deep NLU, Automated Speech Recognition and Natural Language Understanding Engines.
- xPert Packs, providing out-of-the-box recognition and understanding for specific verticals (Banking, Telecoms, Insurance, Healthcare, etc.,) in various languages.

These Application Notes describe the configuration steps for OCP Conversational Voice Service to interoperate with Avaya Session Border Controller for Enterprise (Avaya SBCE) and Avaya Aura® environment 8.1.2.

2. General Test Approach and Test Results

The general test approach was to configure the Omilia OCP Conversational Voice Service Cloud Solution to communicate with the Avaya SBCE and Avaya Aura® environment. Interoperability testing contained functional tests done manually mentioned in **Section 2.1**. The serviceability test cases were performed manually by disconnecting/reconnecting the sip trunk connectivity to Omilia OCP Conversational Voice Service Cloud Solution.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Omilia OCP Conversational Voice Service Cloud Solution did not include use of any specific encryption features as requested by Omilia.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The Interoperability Compliance Test included feature and serviceability testing. Feature testing included the validation of the following:

- Inbound calls from Avaya Aura® environment to Omilia OCP Conversational Voice Service
- Transfer calls from Omilia OCP Conversational Voice Service to Avaya Endpoints
- Proper transmissions of DTMF to Omilia OCP Conversational Voice Service
- Codec negotiations between Avaya SBCE and Omilia OCP Conversational Voice Service
- Routing of RTP from Avaya SBCE to Omilia OCP Conversational Voice Service
- Calls for scenarios involving internal, external, IVR, mute, hold, reconnect, and transfer

The serviceability testing focused on verifying the ability of Omilia OCP Conversational Voice Service to recover from adverse conditions such as disconnecting/reconnecting the connection to Omilia OCP Conversational Voice Service.

2.2. Test Results

All test cases passed successfully.

2.3. Support

Support is available via <https://omilia.com>

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and Omilia OCP Conversational Voice Service. The Avaya SBCE connect with Session Manager via two SIP Trunks: PSTN SIP trunk for routing call from/to VoIP Service Provider and Omilia SIP trunk for routing call from/to Omilia OCP Conversational Voice Service.

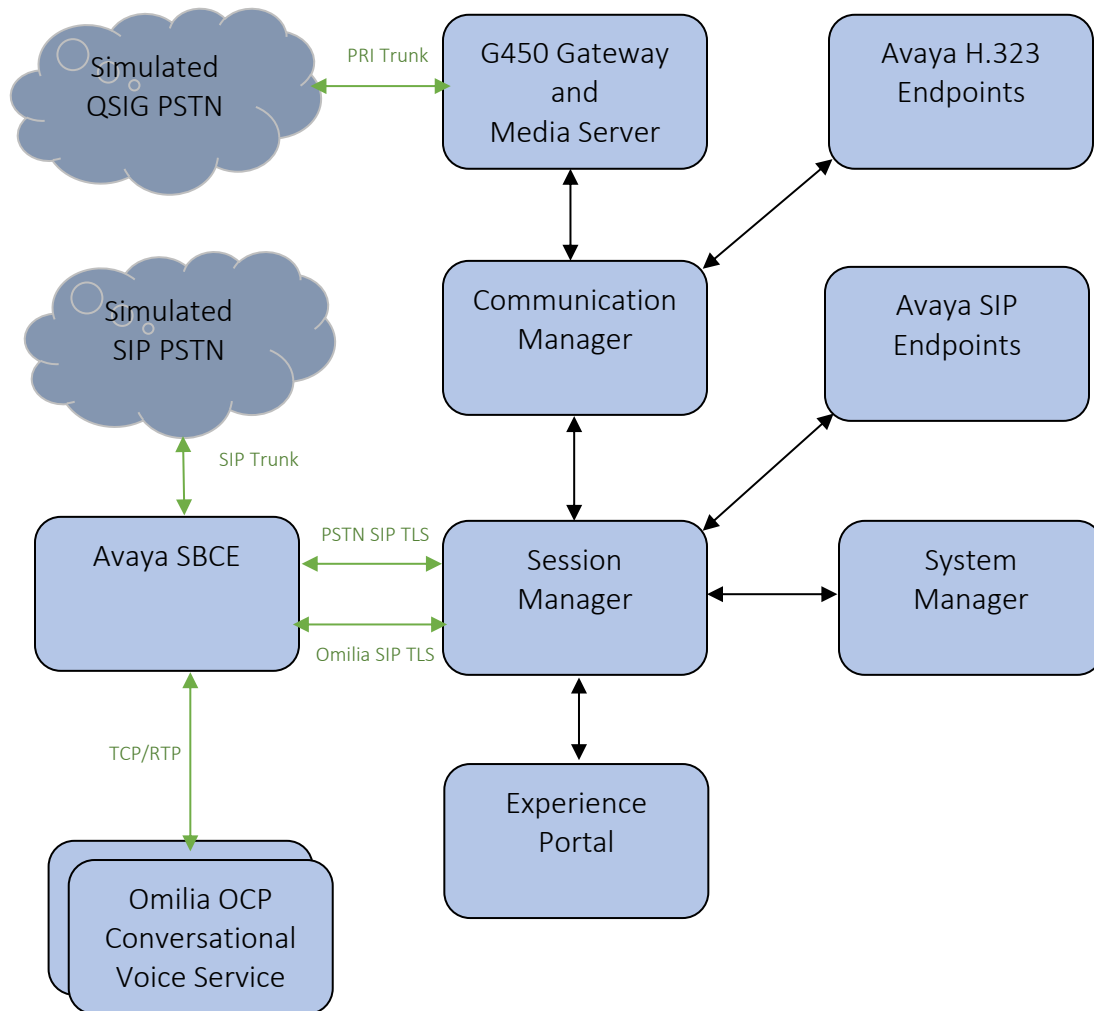


Figure 1: Test Configuration for Omilia OCP Conversational Voice Service and Avaya Aura[®] Environment.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.2
Avaya Aura® Session Manager in Virtual Environment	8.1.2
Avaya Aura® Communication Manager in Virtual Environment	8.1.2
Avaya G450 Media Gateway <ul style="list-style-type: none">• MGP	41.16.30
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.0.0-14-18490
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya Workplace Client	3.8.4.10.2
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.9
Omilia OCP Conversational Voice Service	1.0

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure Omilia OCP Conversational Voice Service successfully with Communication Manager.

It is assumed that the general installation and configuration of Avaya Aura® environment and simulated PSTN SIP Trunk have been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screen captures will show the use of the change command instead of the add command, since the configuration used for the testing was previously added.

5.1. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to **none**.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? all
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? nsmsip92
```

5.2. Outbound Routing to Omilia

This section describes the steps required to configure outbound calls via the Session Manager SIP trunk to the Omilia OCP Conversational Voice Service. The Uniform Dial plan (UDP) and Automatic Alternate Routing (AAR) are used to route outbound calls to the Omilia OCP Conversational Voice Service

5.2.1.Administer Uniform Dial plan

Use the **change uniform-dialplan n** command to administer the uniform dialplan. In this configuration extension 101 is configured as aar to send calls via the aar analysis table.

change uniform-dialplan 1						Page 1 of 2	
UNIFORM DIAL PLAN TABLE							
						Percent Full: 0	
Matching			Insert		Node		
Pattern	Len	Del	Digits	Net	Conv	Num	
101	3	0		aar	n		
4	10	0		aar	n		
5	4	0		aar	n		
6	5	0		aar	n		

5.2.2.Administer AAR

Use the **change aar analysis n** command to specify which route pattern to use based upon the number dialed. In this example, **Route Pattern 1** is used for **Dialed String 101**.

change aar analysis 1						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 2			
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
101		3	3	1	lev0		n
4		10	10	1	lev0		n
5		4	4	1	lev0		n
6		5	5	1	lev0		n

5.2.3.Save Translations

Configuration of Communication Manager is complete. Use the save translation command to save these changes.

6. Configure Avaya Aura® Session Manager

All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL. A SIP trunk and routing needs to be configured for Communication Manager and Avaya SBCE.

6.1. Configure SIP Entity for Avaya SBCE

Add new SIP entity for Avaya SBCE. Select **Routing** → **SIP Entities** from the left pane and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya SBCE.

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, example “DevConnect-SBC99”
- **FQDN or IP Address:** The internal SIP IP address of Avaya SBCE.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.

SIP Entity Details

General

* Name:	<input type="text" value="DevConnect-SBC99"/>
* FQDN or IP Address:	<input type="text" value="10.30.5.99"/>
Type:	<input type="text" value="SIP Trunk"/>
Notes:	<input type="text"/>
Adaptation:	<input type="text"/>
Location:	<input type="text" value="SaiGon"/>
Time Zone:	<input type="text" value="Asia/Ho_Chi_Minh"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Minimum TLS Version:	<input type="text" value="Use Global Setting"/>
Credential name:	<input type="text"/>
Securable:	<input type="checkbox"/>
Call Detail Recording:	<input type="text" value="egress"/>

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 “DevConnect-SMSIP”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Avaya SBCE entity name from this section, in this case “DevConnect-SBCInt”
- **Port:** “5061”
- **Connection Policy:** “trusted”

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"/>	* DevConnect-SMSIP_DevC	DevConnect-SMSIP	TLS	* 5061	DevConnect-SBCInt	* 5061	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove		
1 Item Filter: Enable		
<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down
<input type="checkbox"/>	200OK	up

Select : All, None

Commit Cancel

6.2. Configure Routing Policies

Add a new routing policy for routing calls to Communication Manager and Avaya SBCE.

6.2.1. Routing Policy for 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 to Communication Manager.

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name.

Routing Policy Details

CommitCancel

Help ?

General

* Name: To CM93

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevConnect-CM93	10.30.5.93	CM	

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	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

6.2.2. Routing Policy for Avaya SBCE

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the Avaya SBCE entity name.

Routing Policy DetailsCommitCancel[Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DevConnect-SBC99	10.30.5.99	SIP Trunk	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	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

6.3. Configure Dial Patterns

Dial patterns needs to be configured for Session Manager to know where to route the calls.

6.3.1. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Policies** created in previous **Section 6.2.1** (not shown). The configuration below shows calls to **8xxxx** were routed to Communication Manager.

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

<input type="button" value="Add"/> <input type="button" value="Remove"/>							
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-		To CM93	0	<input type="checkbox"/>	DevConnect-CM93	
Select : All, None							

6.3.2.Dial Pattern for Avaya SBCE

Select **Routing → Dial Patterns** from the left pane and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Policies** created in previous **Section 6.2.2** (not shown). The configuration below shows calls to **10x** were routed to Avaya SBCE.

Dial Pattern DetailsCommitCancelHelp ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

AddRemove

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-		To_SBC99	0	<input type="checkbox"/>	DevConnect-SBC99	

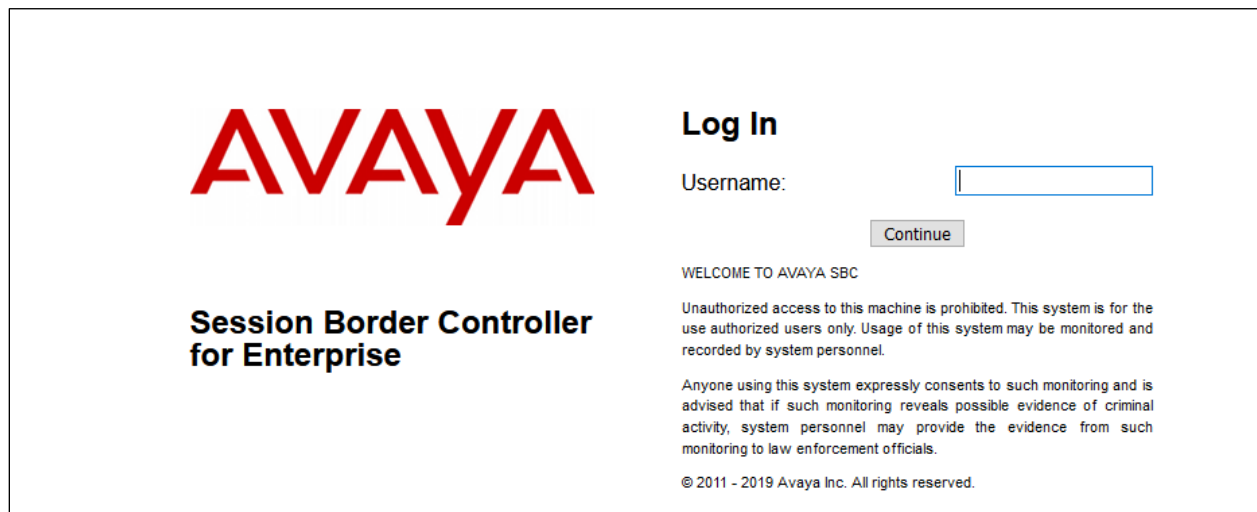
Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides SIP connectivity to VoIP Service Provider, Omilia OCP Conversational Voice Service and Session Manager.

Note: The Staging and Production Omilia OCP Conversational Voice Service IP Addresses and ports for the relevant region will be shared with the Avaya customer during the integration phase. Capacity numbers used for the inbound and outbound routes will also be defined at the same time.

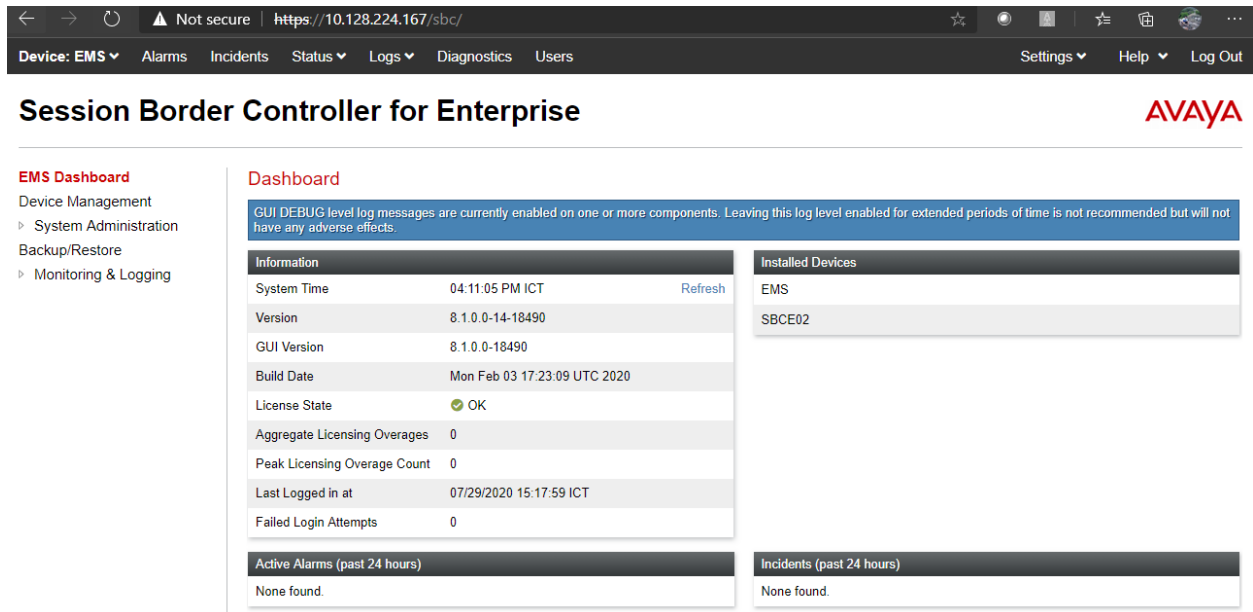
Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A login screen is presented. Log in using the appropriate username and password.



The image shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, a welcome message reads "WELCOME TO AVAYA SBC". Below that is a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." This is followed by a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2019 Avaya Inc. All rights reserved." is visible.

7.1. Access Avaya Session Border Controller for Enterprise

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



Browser address bar: <https://10.128.224.167/sbc/>

Top navigation bar: Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, Log Out

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
 - System Administration
- Backup/Restore
- Monitoring & Logging

Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

Information	
System Time	04:11:05 PM ICT Refresh
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/29/2020 15:17:59 ICT
Failed Login Attempts	0

Installed Devices
EMS
SBCE02

Active Alarms (past 24 hours)
None found.

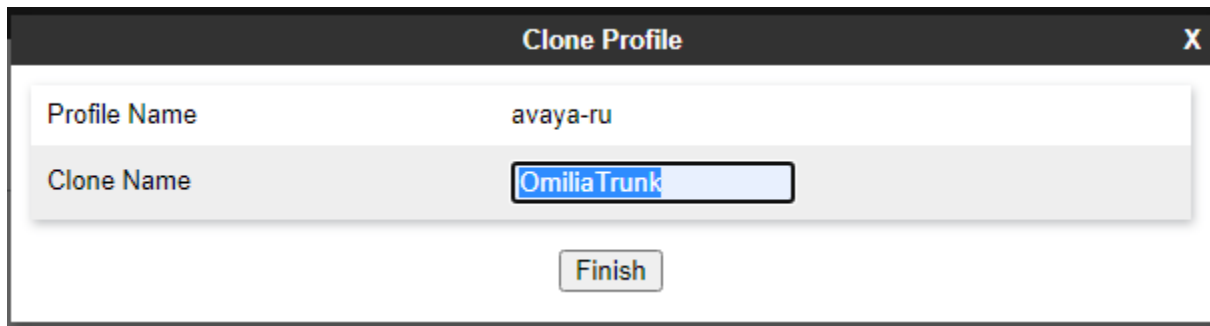
Incidents (past 24 hours)
None found.

7.2. Define Server Interworking

An interworking profile is needed for supported SIP functionality for a SIP server. During Compliance Testing, a pre-configured profile was used for Session Manager and VoIP Service Provider, but the screen captures for those are shown in this section. Add Interworking profile for Omilia OCP Conversational Voice Service and Session Manager.

7.2.1. Server Interworking profile for Omilia

To add a Server Interworking profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. Screen captures for the profile are shown below. Select the **avaya-ru** profile and select **Clone**. Type in a **Clone Name** for Omilia profile. Select **Finish** once done.



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog has two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'OmiliaTrunk'. Below these fields is a 'Finish' button.

Select the **Advanced** tab and configure the fields as the screen capture below. Note that the **Record Routes** is set to **None**.

Interworking Profiles: Semafone

Add

Rename

Clone

Delete

Interworking Profiles

cs2100

avaya-ru

Semafone

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

Record Routes

None

Include End Point IP for Context Lookup

No

Extensions

None

Diversion Manipulation

No

Has Remote SBC

Yes

Route Response on Via Port

No

Relay INVITE Replace for SIPREC

No

MOBX Re-INVITE Handling

No

DTMF

DTMF Support

None

Edit

7.2.2. Server Interworking profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. The **Advanced** tab screen capture is shown below:

Interworking Profiles: Session Manager

Add

Rename

Clone

Delete

Interworking Profiles

cs2100

avaya-ru

Semafone

Session Manager

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

Record Routes

None

Include End Point IP for Context Lookup

Yes

Extensions

Avaya

Diversion Manipulation

No

Has Remote SBC

Yes

Route Response on Via Port

No

Relay INVITE Replace for SIPREC

No

MOBX Re-INVITE Handling

No

DTMF

DTMF Support

None

Edit

7.3. Define SIP Servers

A SIP server definition is required for each server connected to the Avaya SBCE. Add SIP Servers for Omilia OCP Conversational Voice Service and Session Manager.

7.3.1. SIP Server for Omilia

To define a server, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up screen (not shown) and select **Next**. Note that for security purposes, Public IP Addresses have been changed to Private.

- **Server Type:** **Trunk Server**
- **TLS Client Profile:** Select a TLS profile for authentication
- **IP Address / FQDN** SIP IP Address of Omilia OCP Conversational Voice Service
- **Port:** SIP Port of Omilia OCP Conversational Voice Service
- **Transport:** **TCP**

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
[REDACTED]	5060	TCP

Delete

Finish

Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for Omilia from **Section 7.2.1** and select **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	OmiliaTrunk ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

7.3.2.SIP Server for Session Manager

Session Manager SIP Server was preconfigured. The screen capture below shows the **General** tab:

SIP Servers: DevConnectSM

Add

Server Profiles

DevConnectIPO

Omilia Trunk

DevConnectSM

ServiceProvider

Rename

Clone

Delete

General

Authentication

Heartbeat

Registration

Ping

Advanced

Server Type

Call Server

SIP Domain

devconnect.com

TLS Client Profile

SBCInt99-Client

DNS Query Type

NONE/A

IP Address / FQDN

Port

Transport

10.30.5.92

5061

TLS

Edit

All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile from **Section 7.2.2.** was configured.

Edit SIP Server Profile - Advanced X

Enable DoS Protection

☐

Enable Grooming

☒

Interworking Profile

SessionManager ▾

Signaling Manipulation Script

None ▾

Securable

☐

Enable FGDN

☐

TCP Failover Port

TLS Failover Port

Tolerant

☐

URI Group

None ▾

Finish

7.4. Define Routing

Routing information is required for routing calls to all configured SIP Servers. The IP addresses and ports defined here will be used as the destination addresses for signaling.

7.4.1. Routing Profile for Omilia OCP Conversational Voice Service

To define Routing profile for, navigate to **Configuration Profiles → Routing** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown). Add entry for Omilia OCP Conversational Voice **SIP Server Profile**. The Next Hop Address field will be populated with the IP address, port and protocol defined for the Omilia OCP Conversational Voice. Note the **Priority / Weight** value; lower the value, higher the priority. If calls to higher priority SIP Server fail, calls are routed to the next highest priority SIP Server. Select **Finish** once done.

Routing Profile

URI Group

*

▼

Time of Day

default

▼

Load Balancing

Priority

▼

NAPTR

☐

Transport

None

▼

LDAP Routing

☐

LDAP Server Profile

None

▼

LDAP Base DN (Search)

None

▼

Matched Attribute Priority

☒

Alternate Routing

☒

Next Hop Priority

☒

Next Hop In-Dialog

☐

Ignore Route Header

☐

ENUM

☐

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Omilia Trunk

██████████.5060 (TCP)

None

Delete

Back

Finish

7.4.2. Routing Profile for Session Manager

Routing Profile for Session Manager was preconfigured. Screen capture below shows the configured Routing Profile for Session Manager.

Routing Profiles: To_SM

Add

Routing Profiles

default

To_SM

To_IPO

To_Omilia

To_SP

Rename

Clone

Delete

Click here to add a description.

Routing Profile

Update Priority

Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
<input type="text" value="1"/>	*	default	Priority	10.30.5.92:5061	TLS

EditDelete

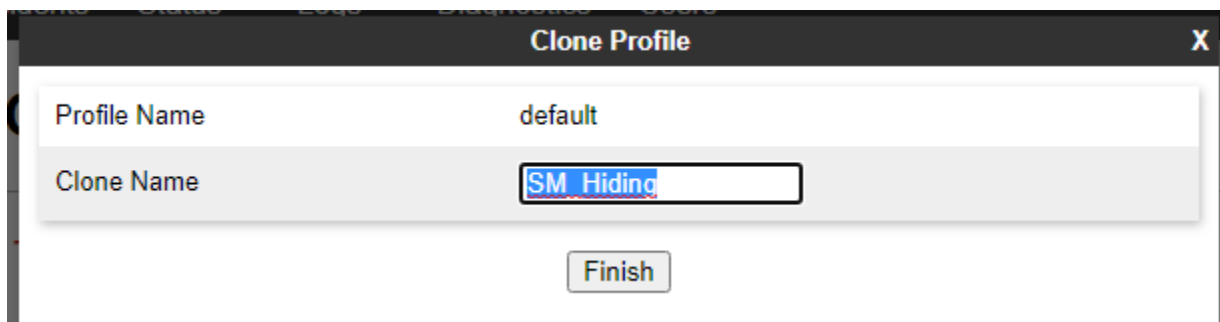
7.5. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network. Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.5.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select Topology Hiding from the Configuration Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown).

- Enter a Clone Name such as the one shown below.
- Click **Finish**.



The screenshot shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The dialog has two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'SM_Hiding'. Below these fields is a 'Finish' button.

On the newly cloned **SM_Hiding** profile screen, click the Edit button (not shown).

- For the, **From**, **To**, **Refer-To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **devconnect.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager.
- Default values were used for all other fields.
- Click **Finish**.

Edit Topology Hiding ProfileX

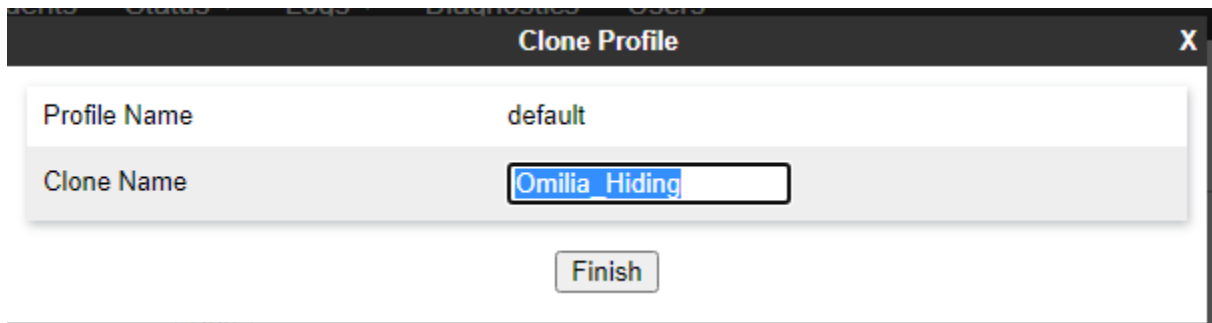
Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Overwrite	devconnect.com	Delete
SDP	Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	devconnect.com	Delete
Refer-To	IP/Domain	Overwrite	devconnect.com	Delete
Record-Route	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	devconnect.com	Delete
Referred-By	IP/Domain	Auto		Delete

Finish

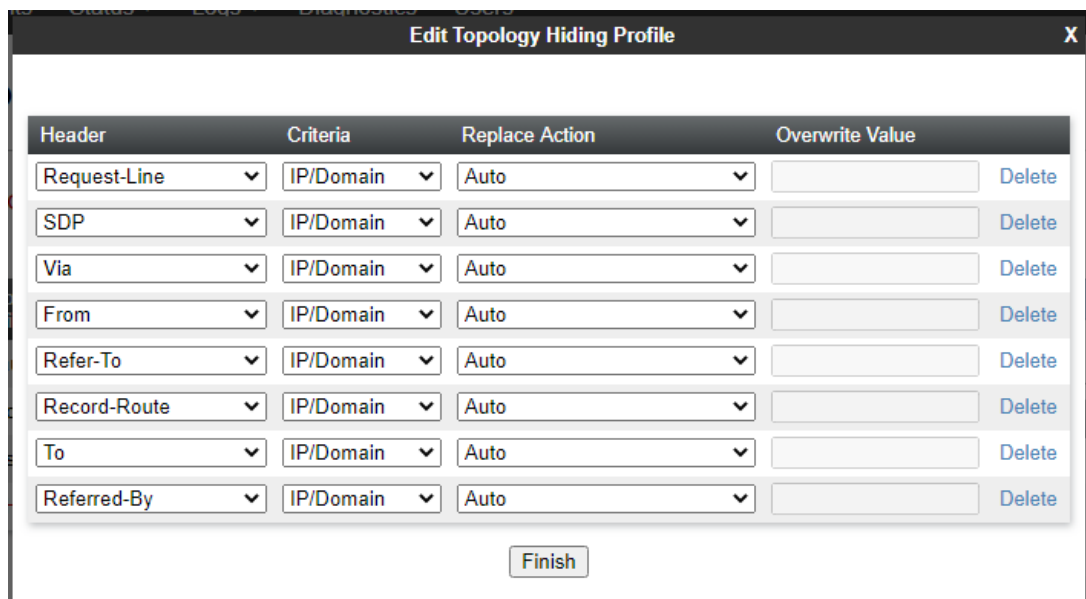
7.5.2. Topology Hiding Profile – Omilia OCP Conversational Voice Service

To add the Topology Hiding Profile in the Omilia OCP Conversational Voice Service direction, select Topology Hiding from the Configuration Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown).

- Enter a Clone Name such as the one shown below.
- Click **Finish**.



The 'Clone Profile' dialog box has a title bar with 'Clone Profile' and a close button 'X'. It contains two input fields: 'Profile Name' with the value 'default' and 'Clone Name' with the value 'Omilia_Hiding'. Below these fields is a 'Finish' button.



The 'Edit Topology Hiding Profile' dialog box has a title bar with 'Edit Topology Hiding Profile' and a close button 'X'. It contains a table with the following data:

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
From	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
To	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete

Below the table is a 'Finish' button.

7.6. Define Media Rules

Media rules are used to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies. Note that during Compliance Testing calls to all the SIP Servers used the same Media Rules.

To define a new Media Rule, navigate to **Domain Policies → Media Rules**. Clone **default-low-med** rule and provide a **Clone Name** for the new Media Rule (not shown). Once added, select the newly added **Media Rule** and Edit the **Encryption** tab, configure as shown in the screen capture below:

Media Rules: Omilia

The screenshot shows the 'Media Rules: Omilia' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med', 'default-low-med-...', 'default-high', 'default-high-enc', 'avaya-low-med-...', 'SRTP', and 'Omilia' (which is highlighted in red). Above this list is an 'Add' button. The main area has a blue header bar with the text 'Click here to add a description.' and three buttons: 'Rename', 'Clone', and 'Delete'. Below the header is a tabbed interface with four tabs: 'Encryption' (selected and highlighted in red), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab contains three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Each section has two rows: 'Preferred Formats' and 'Interworking'. In the 'Audio Encryption' section, 'Preferred Formats' is set to 'RTP' and 'Interworking' has a checked checkbox. The same configuration is shown for the 'Video Encryption' section. In the 'Miscellaneous' section, 'Capability Negotiation' has a checked checkbox. An 'Edit' button is located at the bottom right of the configuration area.

Audio Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input checked="" type="checkbox"/>

Select the **Codec Prioritization** tab and **Edit**. Configure as shown in the screen capture below:

Media Rules: Omilia

Add Rename Clone Delete

Media Rules

- default-low-med
- default-low-med-...
- default-high
- default-high-enc
- avaya-low-med-...
- S RTP
- Omilia**

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

Audio Codec

Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Transcode When Needed	<input type="checkbox"/>
Transrating	<input type="checkbox"/>
Preferred Codecs	PCMU (0) [T], PCMA (8) [T], telephone-event [D]

Video Codec

Codec Prioritization	<input type="checkbox"/>
----------------------	--------------------------

Edit

7.7. Define Endpoint Policy Groups

Endpoint policy groups comprise a group of endpoint policy sets, all of which are specifically configured using a number of relevant parameters. Recently added Media Rule is associated with an Endpoint Policy Group.

To add an Endpoint Policy Group, navigate to **Domain Policies → Endpoint Policy Groups**. Clone **default-low** profile and provide a **Clone Name** for the new Endpoint Policy Group (not shown). Once added, **Edit** the newly cloned group and set the **Media Rule** to the Media Rule added in **Section 7.6**. Select **Finish** once done.

Policy Group

Application Rule	default
Border Rule	default
Media Rule	Omilia
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

Back Finish

7.8. Signaling Interface

Signaling Interface needs to be defined for each SIP Server and SIP Remote Workers for SIP signaling. Navigate to **Networks & Flows → Signaling Interface** to define a new Signaling Interface. During the Compliance Testing the following interfaces were defined.

- **Omilia-IntSignal99**: Signaling interface used by Session Manager to send and receive calls.
- **Omilia-ExtSignal246-195**: Signaling interface used by Omilia OCP Conversational Voice Service to send and receive calls.

Note that TCP was used for Omilia OCP Conversational Voice Service connectivity during the Compliance testing.

Signaling Interface

Signaling Interface						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
B1-Ext249	10.30.8.249 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCEExt249	Edit Delete
B1-Ext247-17	10.30.8.247 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCEExt17	Edit Delete
SP-IntSignal140	10.30.5.140 A1-Int1 (A1, VLAN 0)	5060	---	5061	SBCInt140	Edit Delete
Omilia-IntSignal99	10.30.5.99 A1-Int1 (A1, VLAN 0)	5060	---	5061	SBCInt99	Edit Delete
Omilia-ExtSignal246-195	10.30.8.246 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCEExt195	Edit Delete
SP-ExtSignal248	10.30.8.248 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCEExt248	Edit Delete

7.9. Media Interface

Media Interface needs to be defined for each SIP Server and SIP Remote Workers to send and receive media (RTP or SRTP). Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined.

- **Omilia-IntMedia99**: Interface used by Session Manager to send and receive media.
- **Omilia-ExtMedia246-195**: Interface used by Omilia OCP Conversational Voice Service to send and receive media.

Media Interface

Media Interface			Add	
Name	Media IP Network	Port Range		
MediaB1-249	10.30.8.249 B1-Ext (B1, VLAN 0)	35000 - 40000	Edit	Delete
MediaB1-247-17	10.30.8.247 B1-Ext (B1, VLAN 0)	35000 - 40000	Edit	Delete
Omilia-IntMedia99	10.30.5.99 A1-Int1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
SP-IntMedia140	10.30.5.140 A1-Int1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Omilia-ExtMedia246-195	10.30.8.246 B1-Ext (B1, VLAN 0)	35000 - 40000	Edit	Delete
SP-ExtMedia248	10.30.8.248 B1-Ext (B1, VLAN 0)	35000 - 40000	Edit	Delete

7.10. Server Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The call flows for Inbound and Outbound calls are shown as below through the Avaya SBCE and Omilia OCP Conversational Voice Service

- Outbound: Avaya Endpoints/ PSTN → Avaya SM → SBC Internal Interface → SBC External Interface → Omilia OCP Conversational Voice Service
- Inbound: Omilia OCP Conversational Voice Service → SBC External Interface → SBC Internal Interface → Avaya SM → Avaya Endpoints (Agents)

Server Flows combine the previously defined profiles for Omilia OCP Conversational Voice Service and Session Manager. These End Point Server Flows allow calls to be routed to and from Omilia OCP Conversational Voice Service / Session Manager. Navigate to **Network & Flows → End Point Flows → Server Flows**. The screen capture below displays the configured Server Flows. The screen capture below displays the Server flows used during the Compliance test.

End Point Flows

Subscriber Flows		Server Flows					
Priority	Flow Name	Group	Interface	Interface	Group	Profile	
1	DevConnectIPO	*	B1-Ext247-17	Omilia-IntSignal99	default-low	default	View Clone Edit Delete

SIP Server: DevConnectSM
[Update](#)

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	DevConnectSM_SP	*	SP-ExtSignal248	SP-IntSignal140	RWRule	To_SP	View Clone Edit Delete
2	DevConnectSM_Omilia	*	Omilia-ExtSignal246-195	Omilia-IntSignal99	Omilia	To_Omilia	View Clone Edit Delete

SIP Server: Omilia Trunk

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Omilia Trunk	*	Omilia-IntSignal99	Omilia-ExtSignal246-195	Omilia	To_SM	View Clone Edit Delete

SIP Server: ServiceProvider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ServiceProvider	*	SP-IntSignal140	SP-ExtSignal248	RWRule	To_SM	View Clone Edit Delete

8. Configure Omilia OCP Conversational Voice Service

All configuration related to Omilia OCP Conversational Voice Service is performed by Omilia engineers and thus, is not documented.

9. Verification Steps


9.1. Verify Entity Link to Avaya Session Border Controller for Enterprise and Entity Link to Avaya Aura Communication manager

To verify SIP connectivity to Avaya SBCE, via System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. Under the **All Monitored SIP Entities**, select the Avaya SBCE Entity.

All Monitored SIP Entities

Run Monitor

14 Items



Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	DevConnect-SBC140
<input type="checkbox"/>	DevConnect-CMTrunk3
<input type="checkbox"/>	DevConnect-BreezeSIP
<input type="checkbox"/>	DevConnect-AACC88
<input type="checkbox"/>	AAM52
<input type="checkbox"/>	DevConnect-Presence
<input type="checkbox"/>	DevConnect-SMSIP
<input type="checkbox"/>	DevConnect-MPP105
<input type="checkbox"/>	DevConnect-IP Office
<input type="checkbox"/>	DevConnect-PresenceService
<input type="checkbox"/>	DevConnect-BSM134
<input type="checkbox"/>	DevConnect-CM93
<input type="checkbox"/>	DevConnect-CM96
<input type="checkbox"/>	DevConnect-SBC99

Select : All, None

Verify **Conn. Status** is **UP**.

All Entity Links to SIP Entity: DevConnect-SBC99

Summary View

1 Item

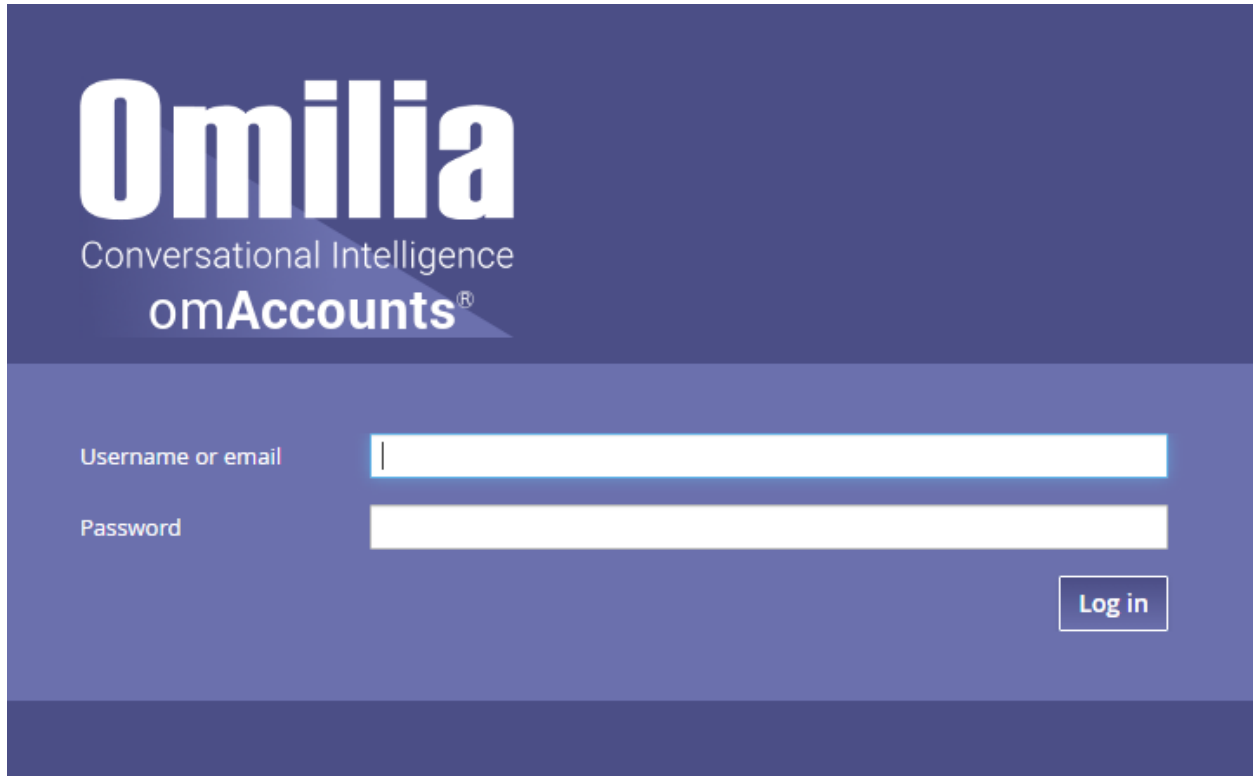
Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	DevConnect-SMSIP	IPv4	10.30.5.99	5061	TLS	FALSE	UP	404 Not Found	UP

Select : None

9.2. Verify Call Routing,

Place a call from the Avaya Endpoints/PSTN to Omilia OCP Conversational Voice Service, ensure the call can be answered by virtual assistants. When the virtual assistant receives a call, login Omilia omAccounts page provided by Omilia. Enter credentials to login.

The image shows the Omilia omAccounts login page. At the top, the Omilia logo is displayed in white on a dark blue background, with the tagline 'Conversational Intelligence' and 'omAccounts®' below it. The main body of the page is a lighter blue. It features two input fields: 'Username or email' and 'Password'. To the right of the password field is a 'Log in' button. The page has a clean, modern design with a dark blue header and footer area.

Omilia
Conversational Intelligence
omAccounts®

Username or email

Password

Log in

Verify Omilia can show the call as below. Click on the **Live** call.

Last Calls									
Sort by Timestamp Reversed order									
Timestamp	Server	Application	Channel-User	Duration	Total steps	NoInputs	NoMatches	Ending	
2020-09-25 11:48:07.695	DiaManT.Demo.UAT	Avaya_Testing	71008		1			LIVE	
2020-09-25 10:43:27.422	DiaManT.Demo.UAT	ABC.Bank		6m. 36s.	3		2	TIMEOUT_NEAR	

The conversation between virtual assistant and user is show as below:

DRTViewer*

Newest Dialog < Newer Dialog Older Dialog > Live Calls Logout

ANI 71008

date 2020-09-25 11:50:44.916

Application Avaya_Testing

server DiaManT.Demo.UAT

duration 58s.

ending TRANSFER [transfer line: 87104]

channel IVR dialog

steps 8

events Intent:Balance-Inquiry:[AS],Balance-Inquiry:selfServe:initiated:Balance-Inquiry::SSServed,Balance-Inquiry:selfServe:completed:Balance-Inquiry::Intent:Rewards_Program-Balance:[AS],Rewards_Program-Balance:selfServe:initiated:Rewards_Program-Balance::SSServed,Rewards_Program-Balance:selfServe:completed:Rewards_Program-Balance::Intent:Reward s_Program-Transfer_Points,Route Out Intent

download

Steps: Steps & audio: Info on all steps:

d: Hello there!What can I do for you today?

1

2

3

4



one two three four

[way]

d: Which account are you interested in?

At end of conversation, ask virtual assistant transfers the call to agent. Verify Avaya agent can receive the call transfer from Omilia OCP Conversational Voice Service.

Verify Omilia can show the call ending with **Transfer** state as below:

Last Calls								
Timestamp	Server	Application	Channel-User	Duration	Total steps	NoInputs	NoMatches	Ending
2020-09-25 11:50:44.916	DiaManT.Demo.UAT	Avaya_Testing	 71008	58s.	8			TRANSFER
2020-09-25 11:48:07.695	DiaManT.Demo.UAT	Avaya_Testing	 71008	28s.	4	3		TRANSFER

10. Conclusion

These Application Notes describe the configuration steps for Omilia OCP Conversational Voice Service Cloud Solution 1.0 to interoperate with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Environment 8.1.2, as shown in **Figure 1**. Omilia OCP Conversational Voice Service 1.0 was able to successfully interoperate with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® environment 8.1.

11. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 5, July 2020
- [3] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020

Documentation related to Omilia OCP Conversational Voice Service can be obtained from <https://omilia.com/>

©2020 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.