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.

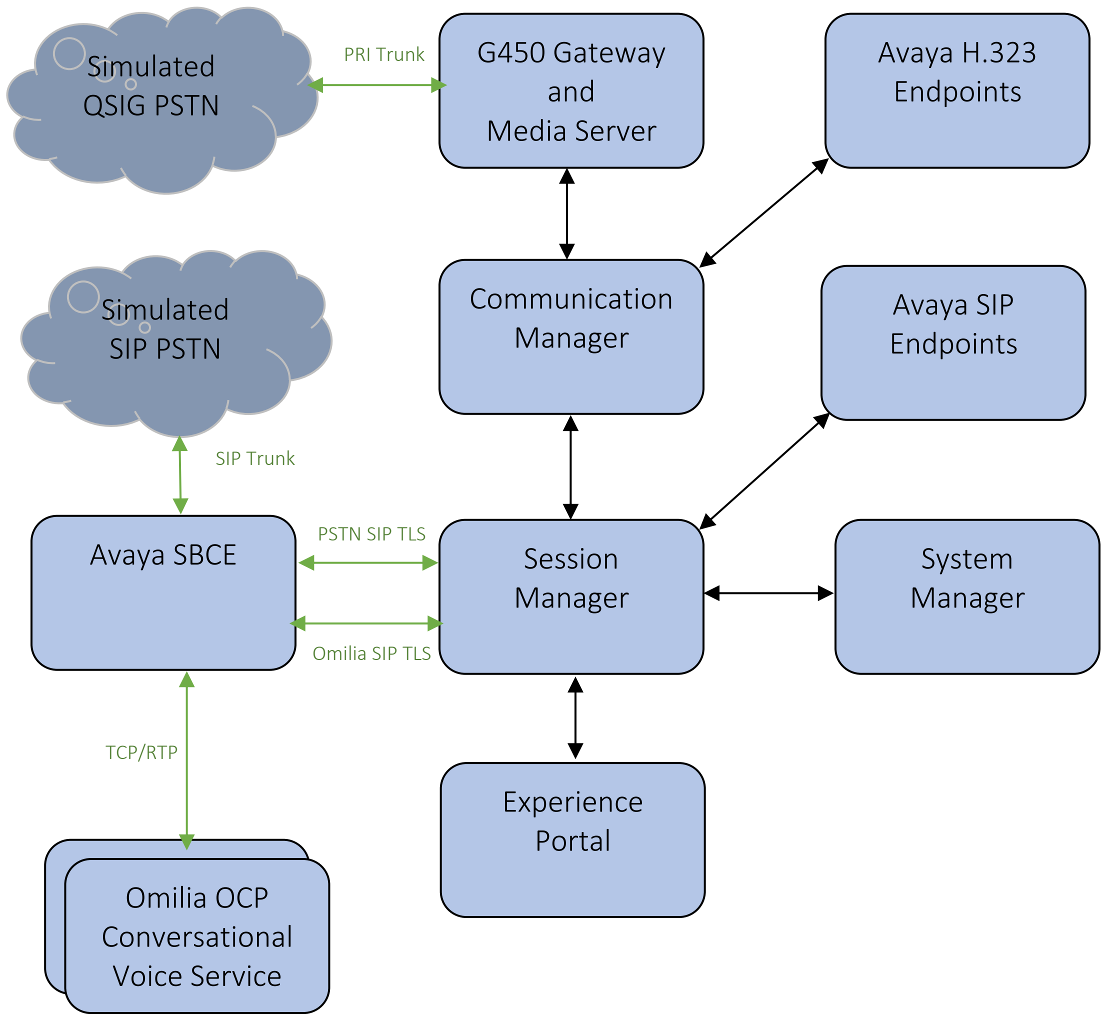


Figure 1: Test Configuration for Omilia OCP Conversational Voice Service and Avaya Aura® Environment.

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 • 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

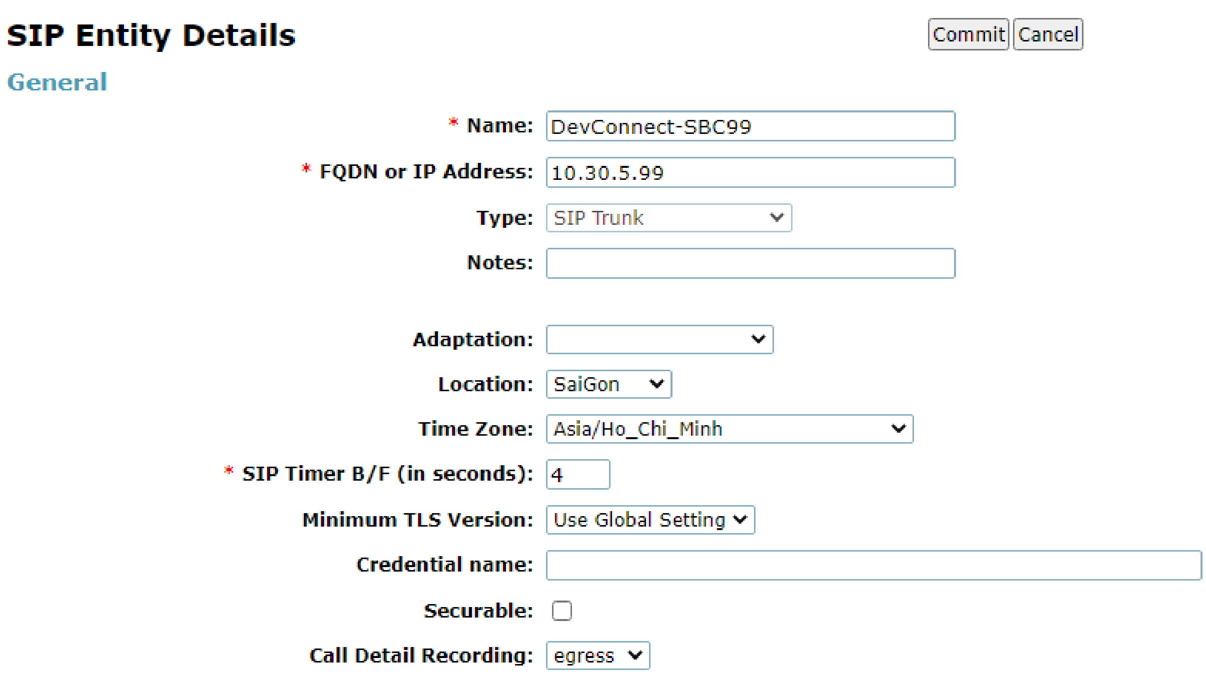
All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL. A SIP trunk and routing needs to be configured for Communication Manager and Avaya SBCE.

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.

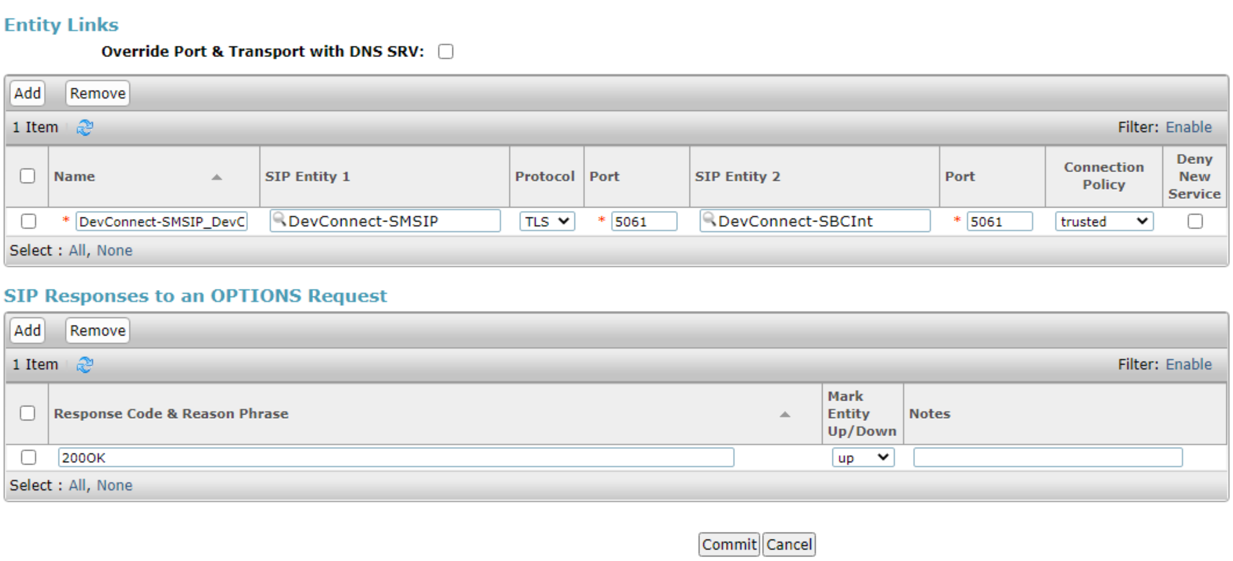
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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.



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"



6.2. Configure Routing Policies

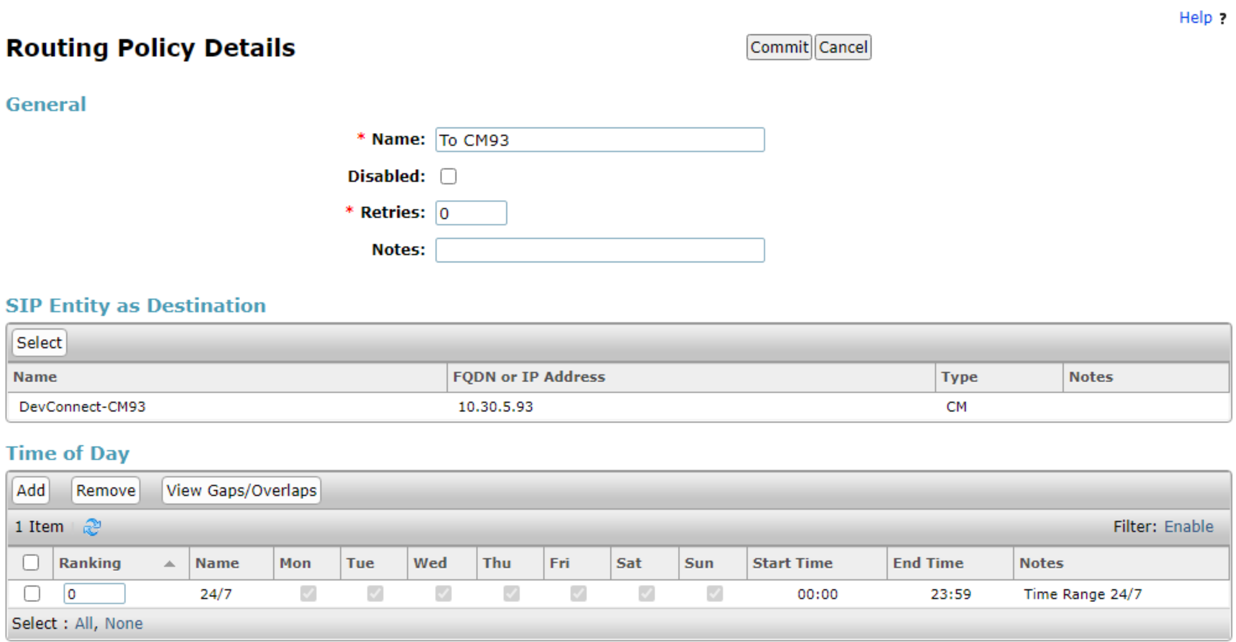
Add a new routing policy for routing calls to Communication Manager and Avaya SBCE.

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.

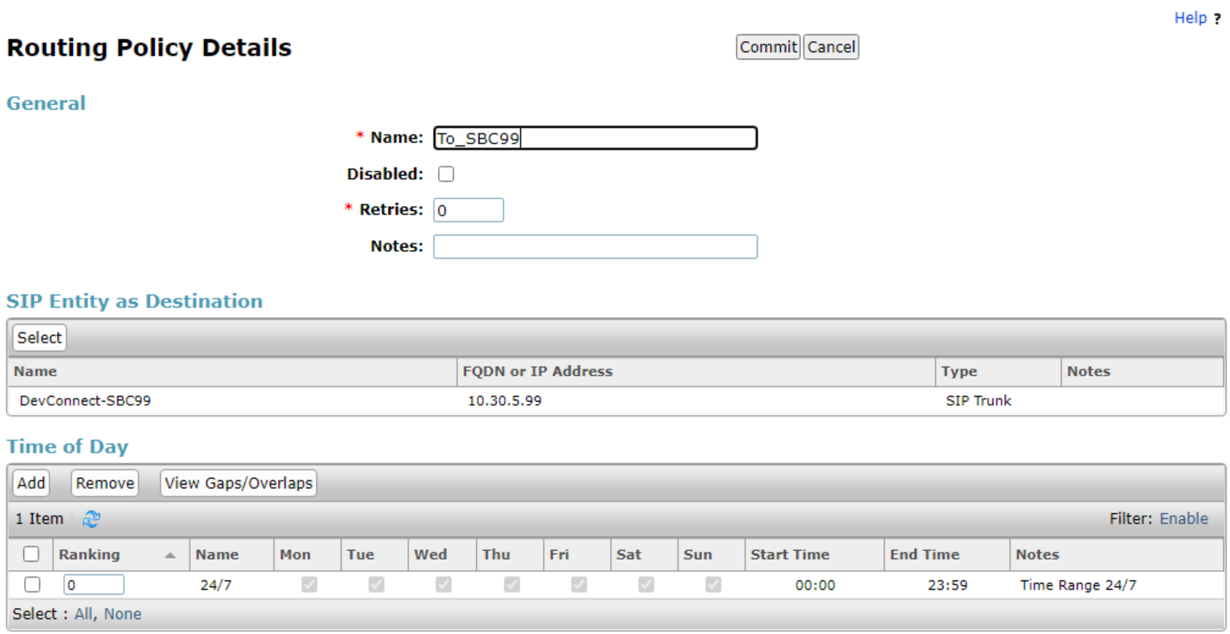


6.2.2. Routing Policy for Avaya SBCE

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.



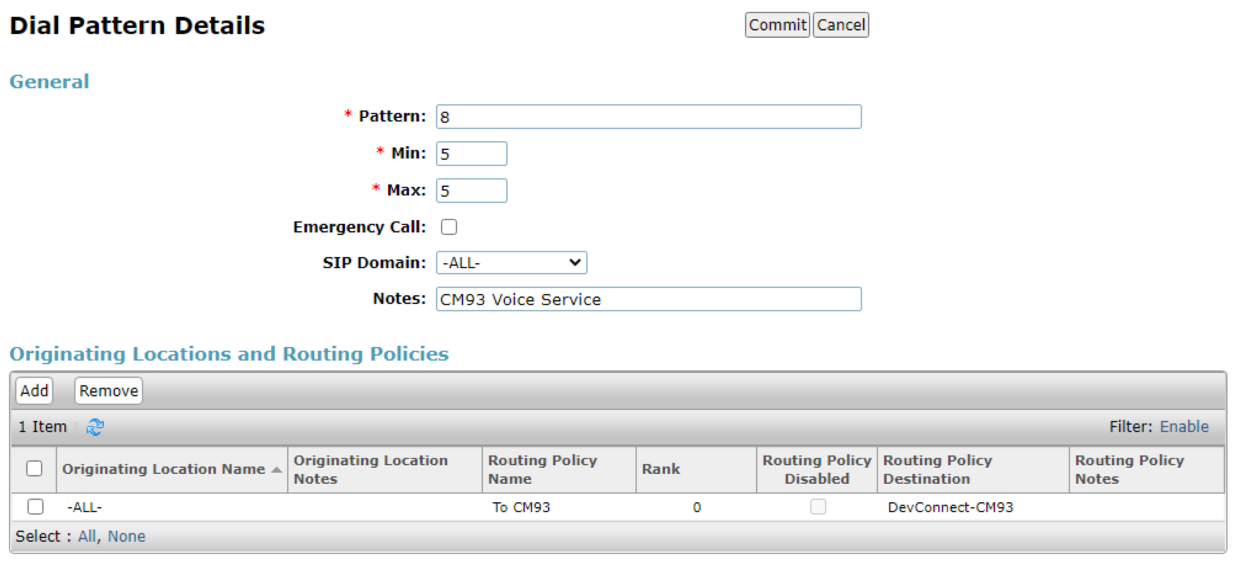
6.3. Configure Dial Patterns

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.

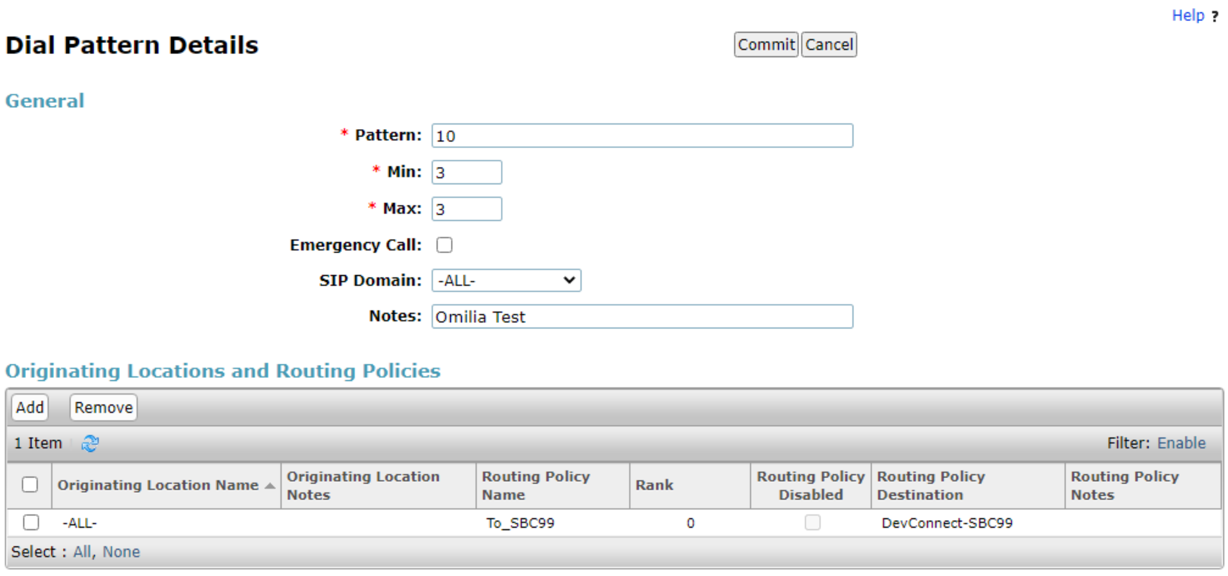
In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous **Section 6.2.1** (not shown). The configuration below shows calls to **8xxxx** were routed to Communication Manager.



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 Polices** created in previous **Section 6.2.2** (not shown). The configuration below shows calls to **10x** were routed to Avaya SBCE.



7. Configure Avaya Session Border Controller for Enterprise

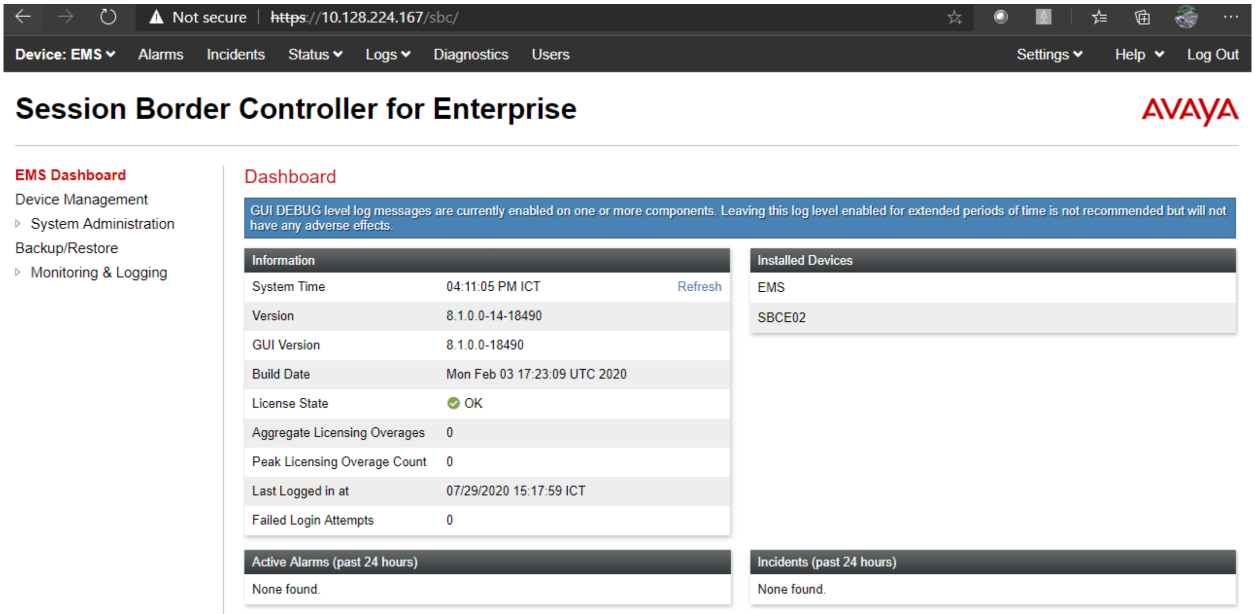
This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides SIP connectivity to VoIP Service Provider, Omilia OCP Conversational Voice Service and Session Manager.

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.

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.

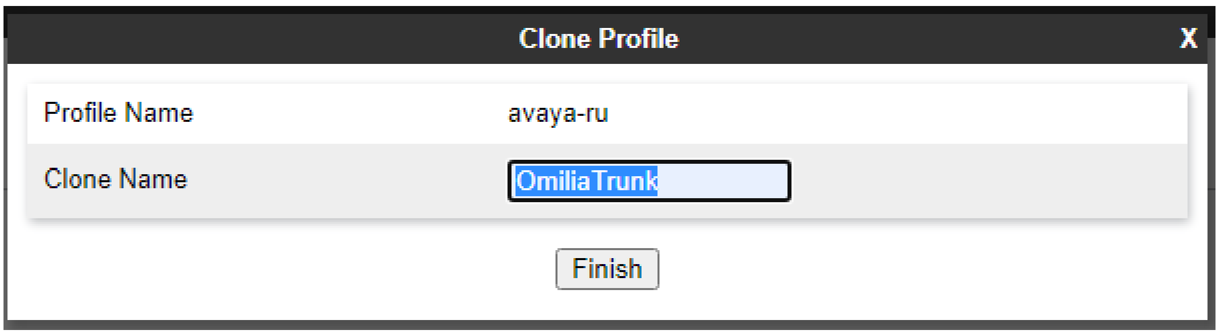


7.2. Define Server Interworking

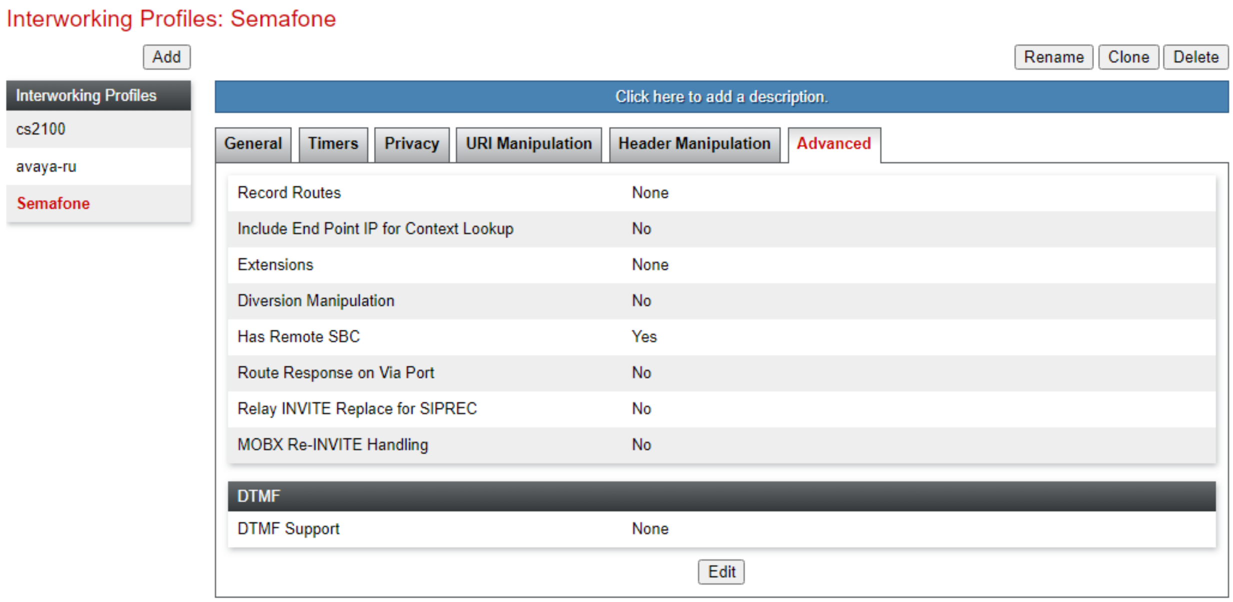
An interworking profile is needed for supported SIP functionality for a SIP server. During Compliance Testing, a pre-configured profile was used for Session Manager and VoIP Service Provider, but the screen captures for those are shown in this section. Add Interworking profile for Omilia OCP Conversational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

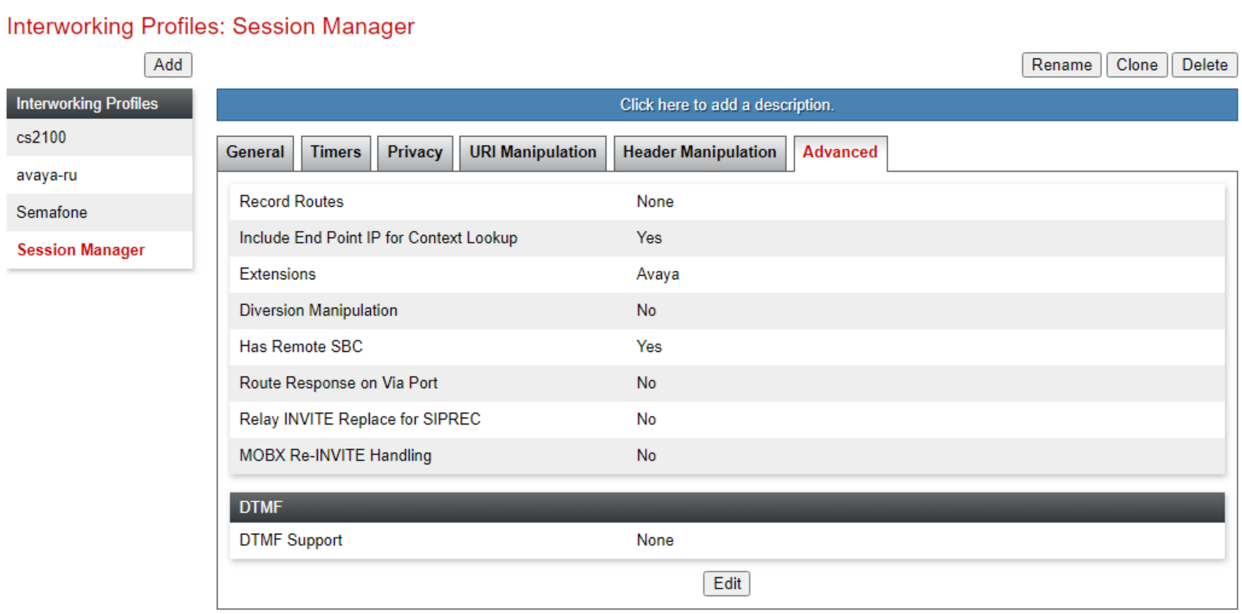


Select the **Advanced** tab and configure the fields as the screen capture below. Note that the **Record Routes** is set to **None.**



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:



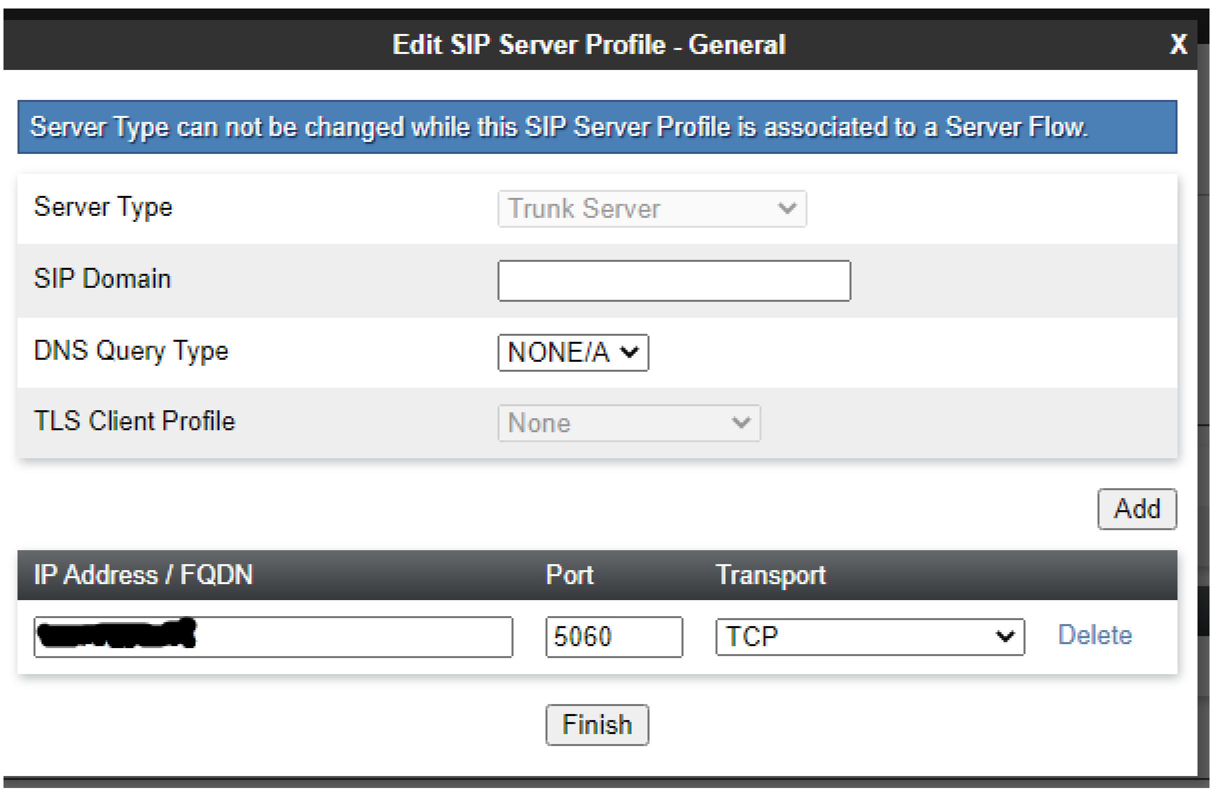
7.3. Define SIP Servers

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.

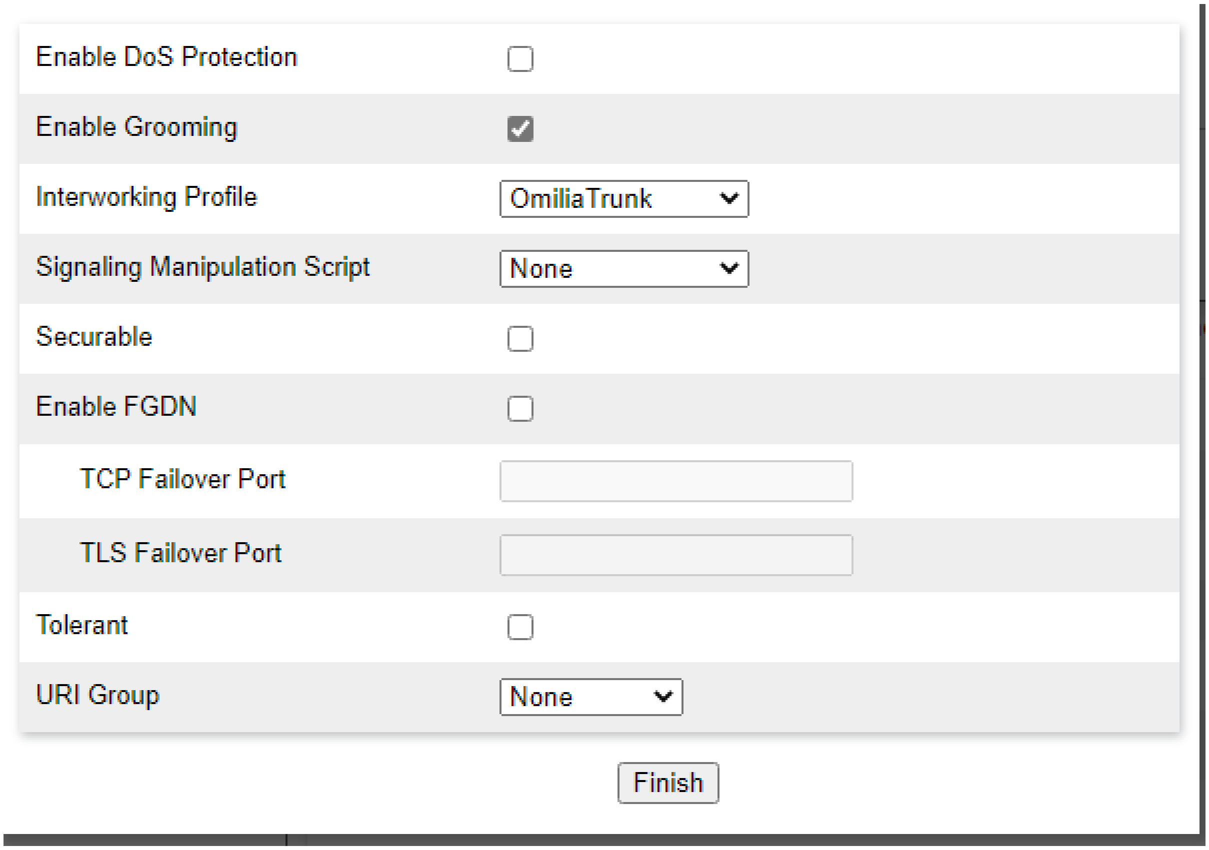
7.3.1. SIP Server for Omilia

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**

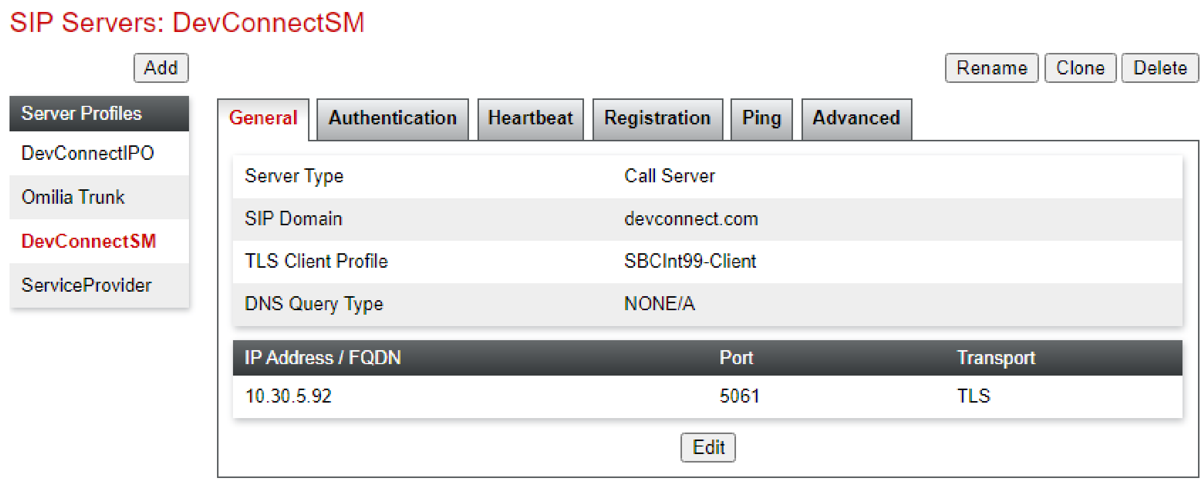


Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for Omilia from **Section 7.2.1** and select **Finish.**

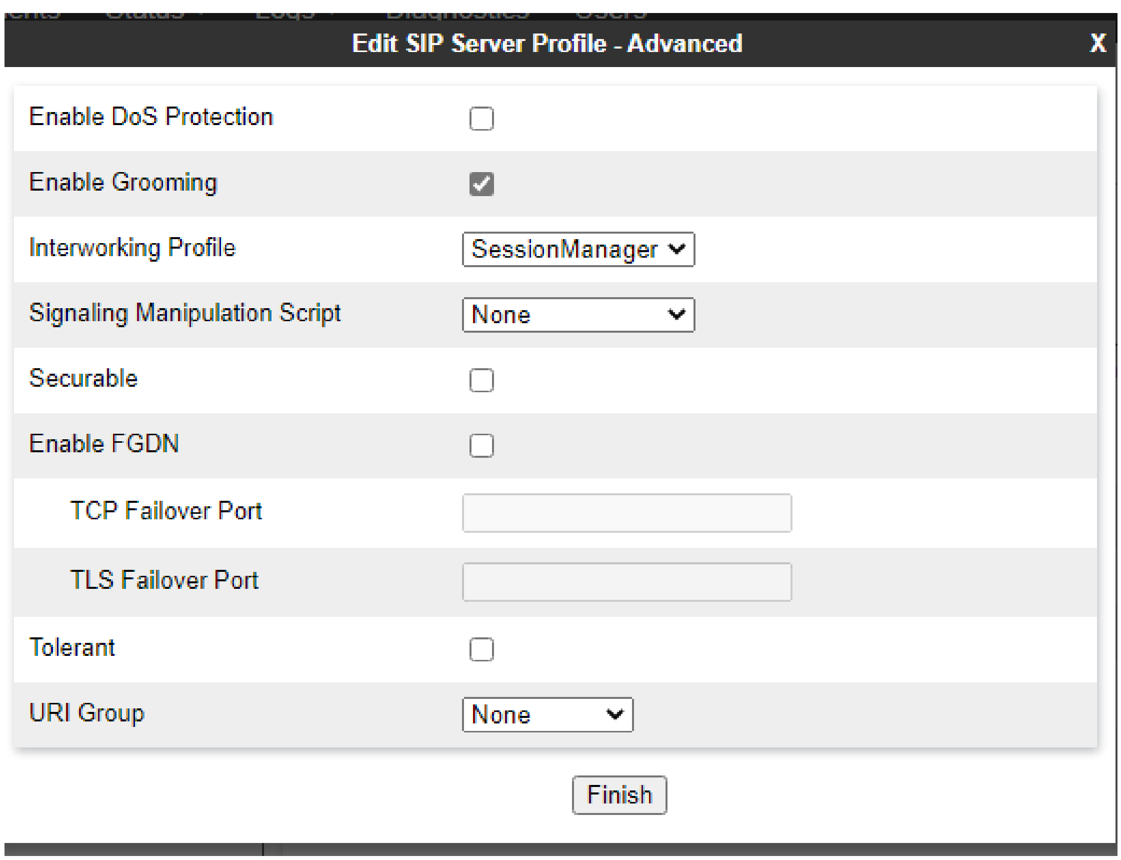


7.3.2. SIP Server for Session Manager

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



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.

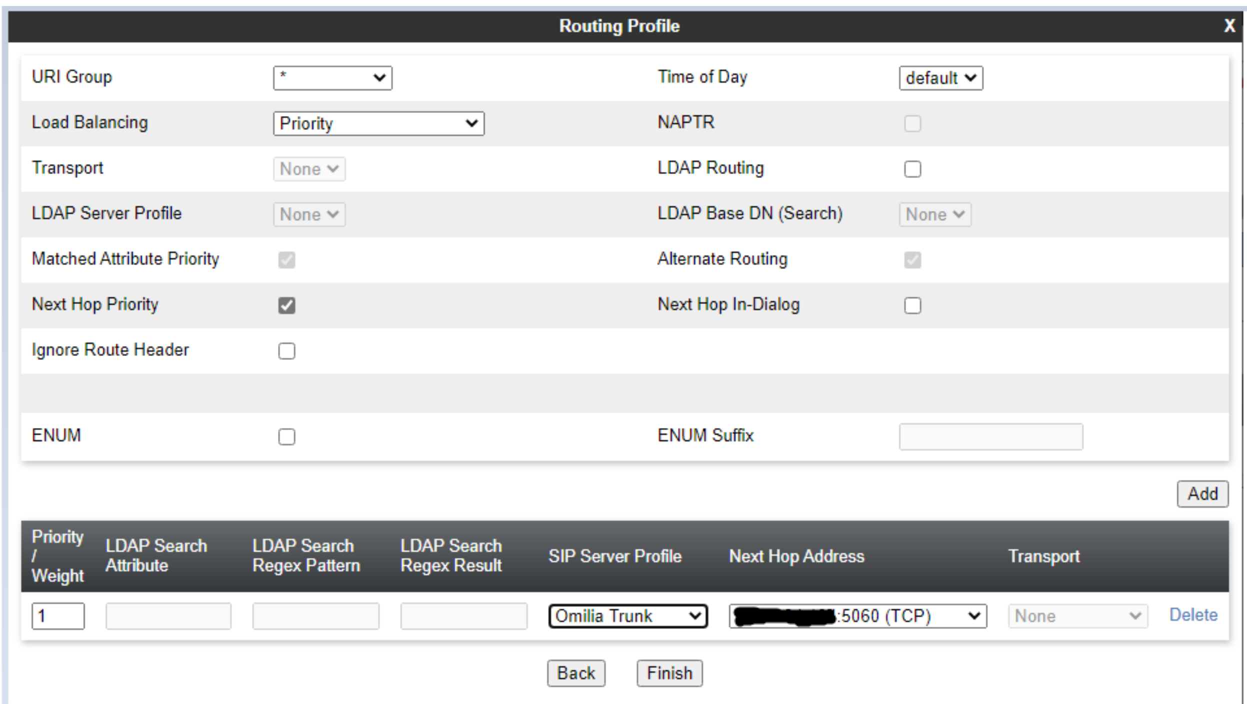


7.4. Define Routing

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.

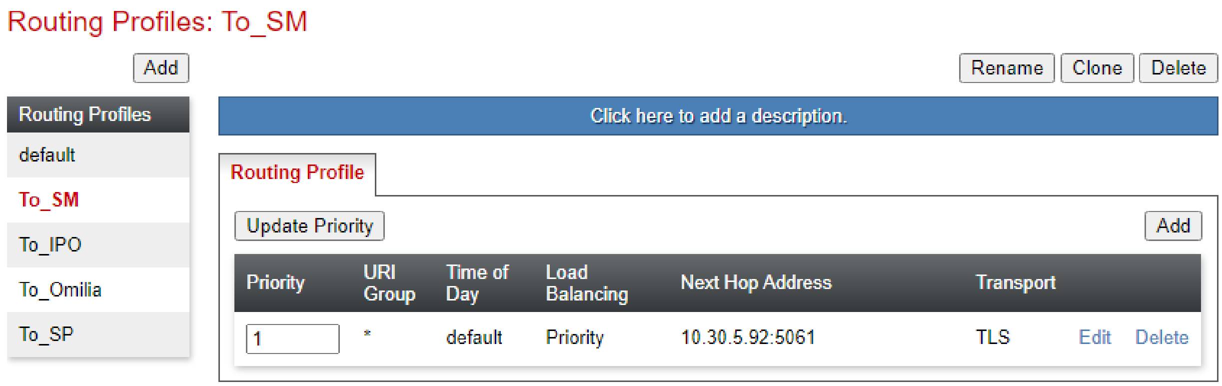
7.4.1. Routing Profile for Omilia OCP Conversational Voice Service

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.



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.



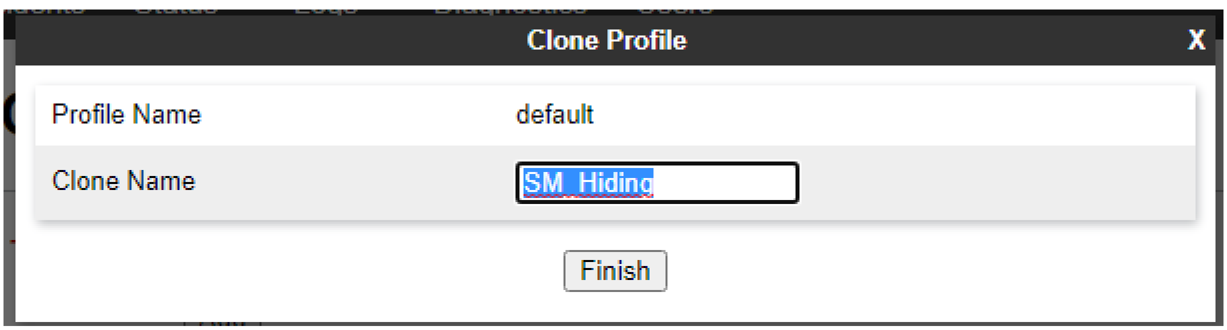
7.5. Topology Hiding

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

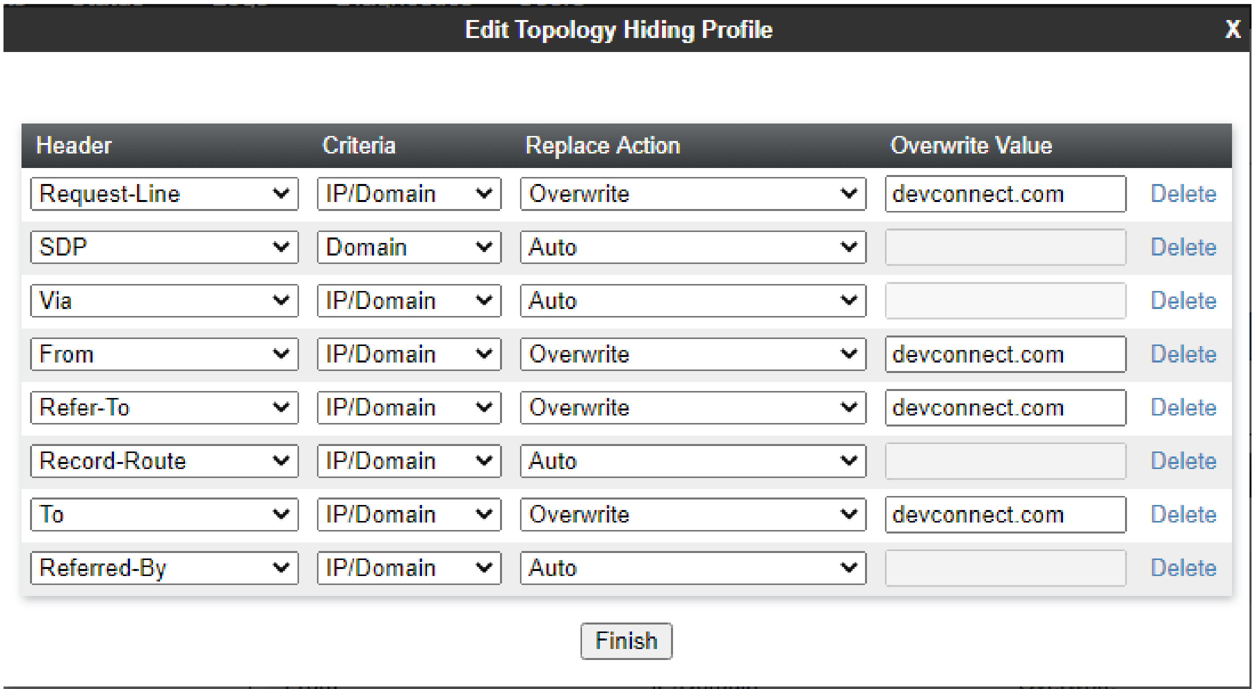
To add the Topology Hiding Profile in the enterprise direction, select Topology Hiding from the Configuration Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown).

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



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

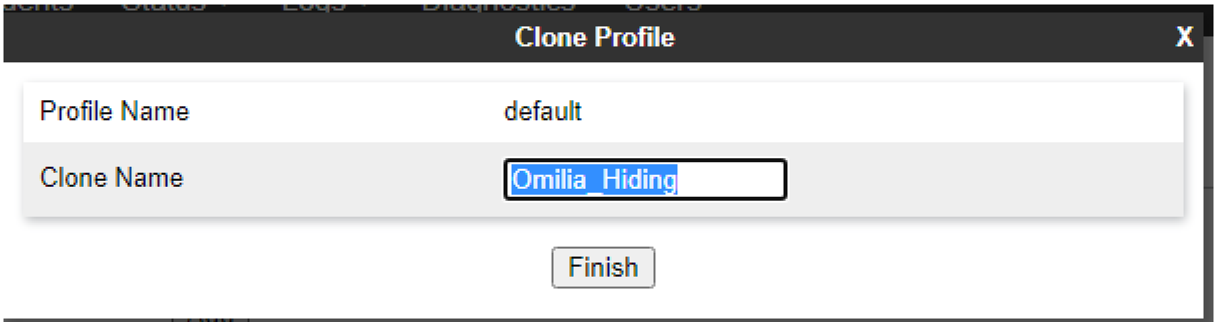
- For the, **From**, **To, Refer-To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **devconnect.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager.
- Default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

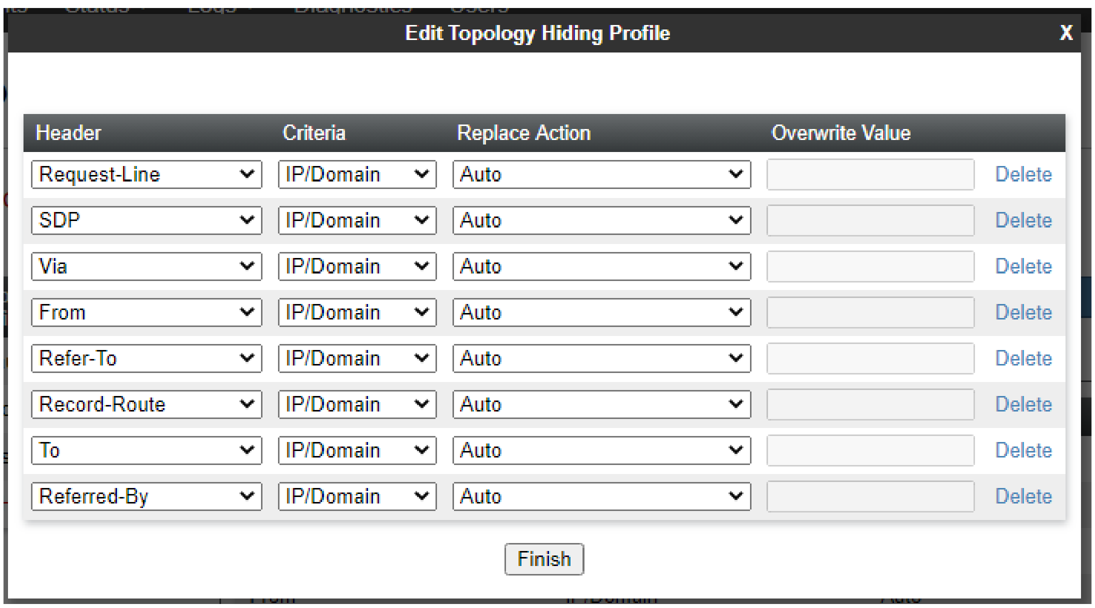

Edit Topology Hiding Profile
X
Header
Criteria
Replace Action
Overwrite Value
Request-Line
IP/Domain
Overwrite
devconnect.com
Delete
SDP
Domain
Auto
Delete
Via
IP/Domain
Auto
Delete
From
IP/Domain
Overwrite
devconnect.com
Delete
Refer-To
IP/Domain
Overwrite
devconnect.com
Delete
Record-Route
IP/Domain
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**.

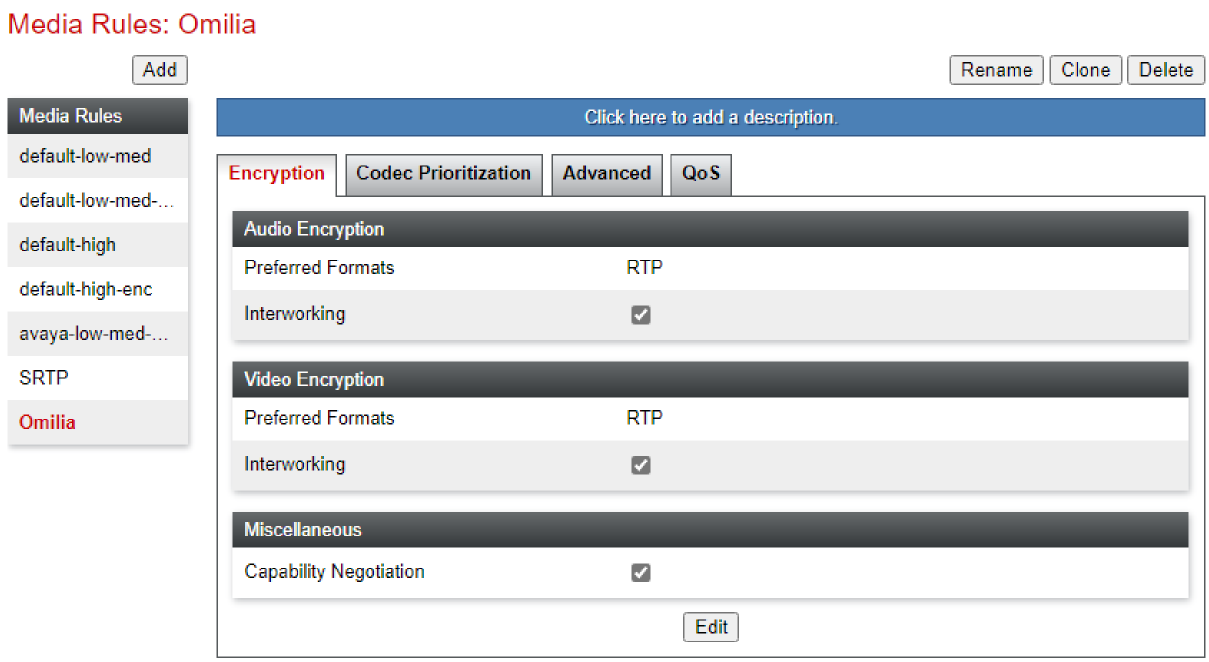




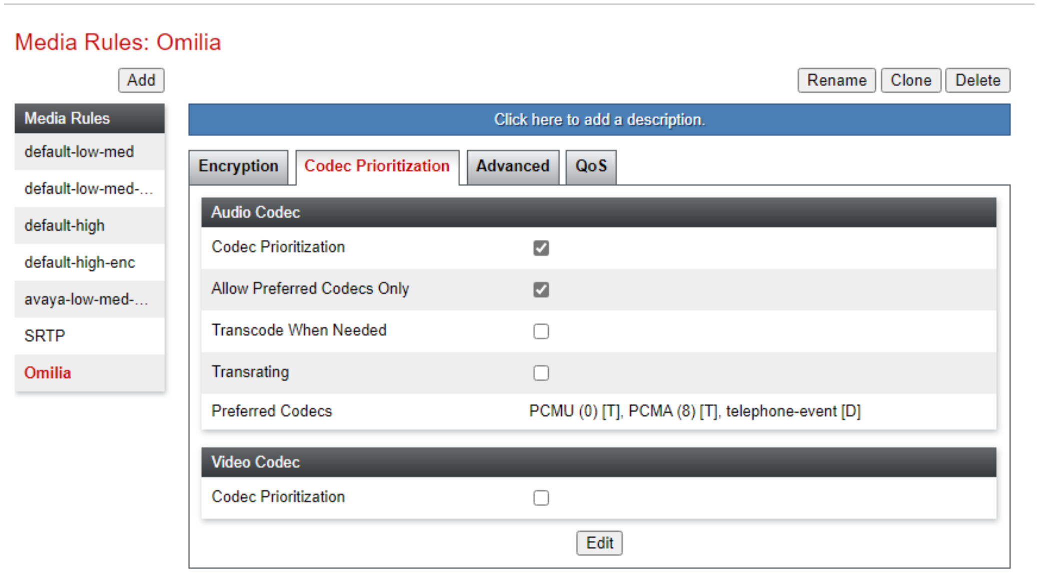
7.6. Define Media Rules

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:



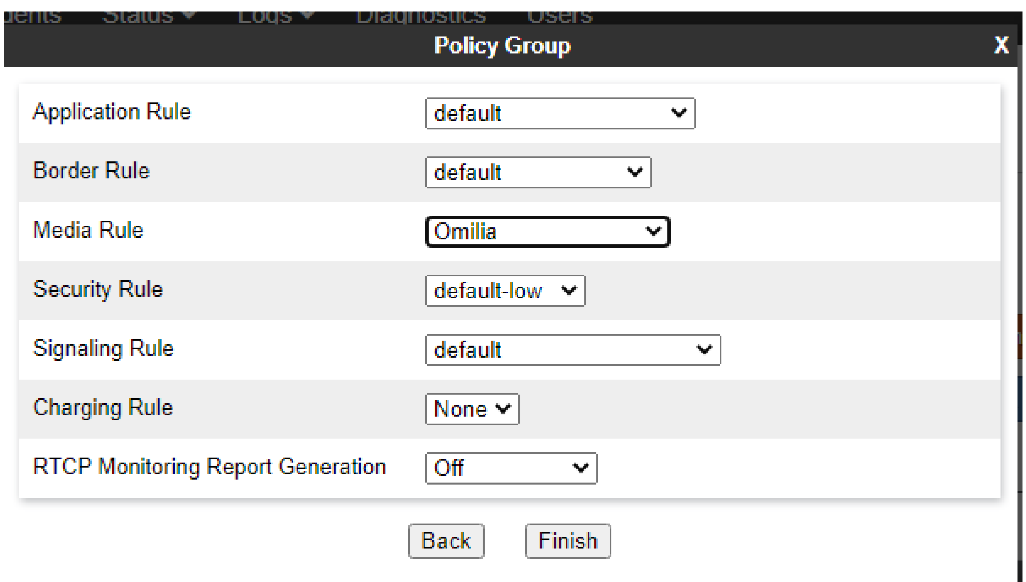
Select the **Codec Prioritization** tab and **Edit.** Configure as shown in the screen capture below:



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.



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 thatTCP was used for Omilia OCP Conversational Voice Service connectivity during the Compliance testing.

Signaling Interface

Signaling Interface

Add

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	SBCExt249	Edit	Delete
B1-Ext247-17	10.30.8.247 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCExt17	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	SBCExt195	Edit	Delete
SP-ExtSignal248	10.30.8.248 B1-Ext (B1, VLAN 0)	5060	---	5061	SBCExt248	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

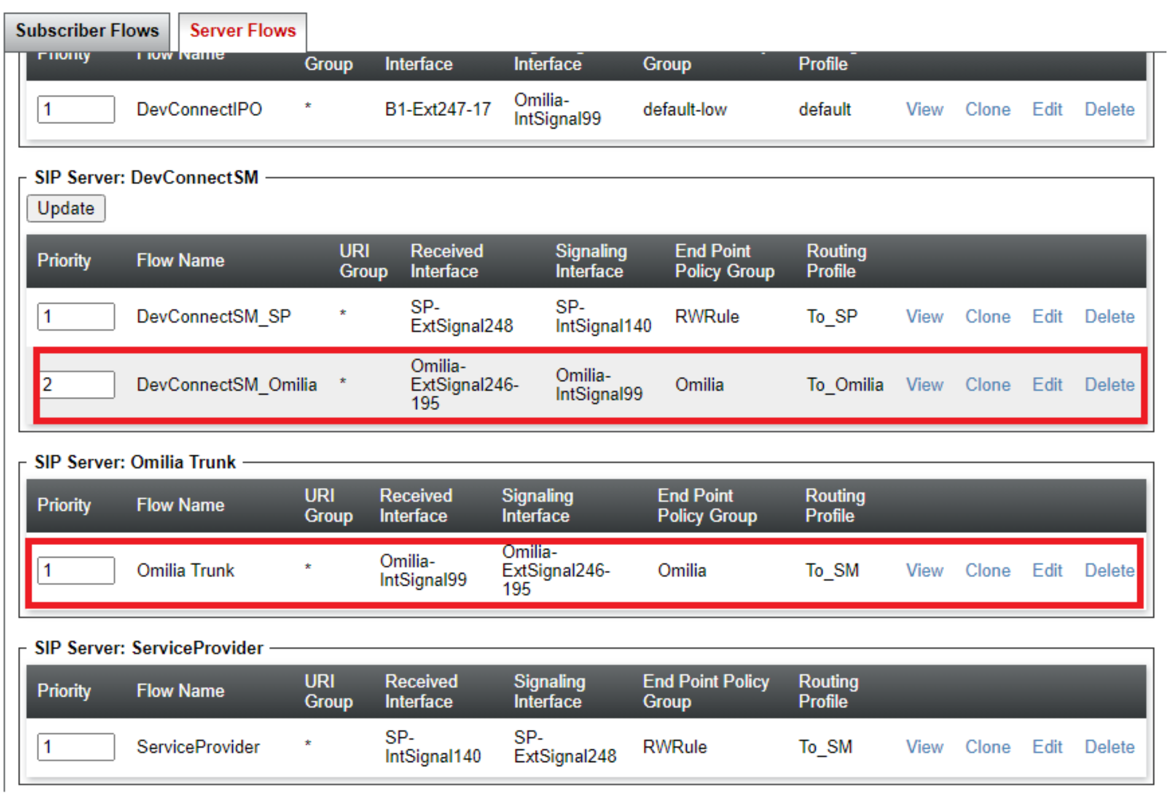
7.10. Server Flows

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 show 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



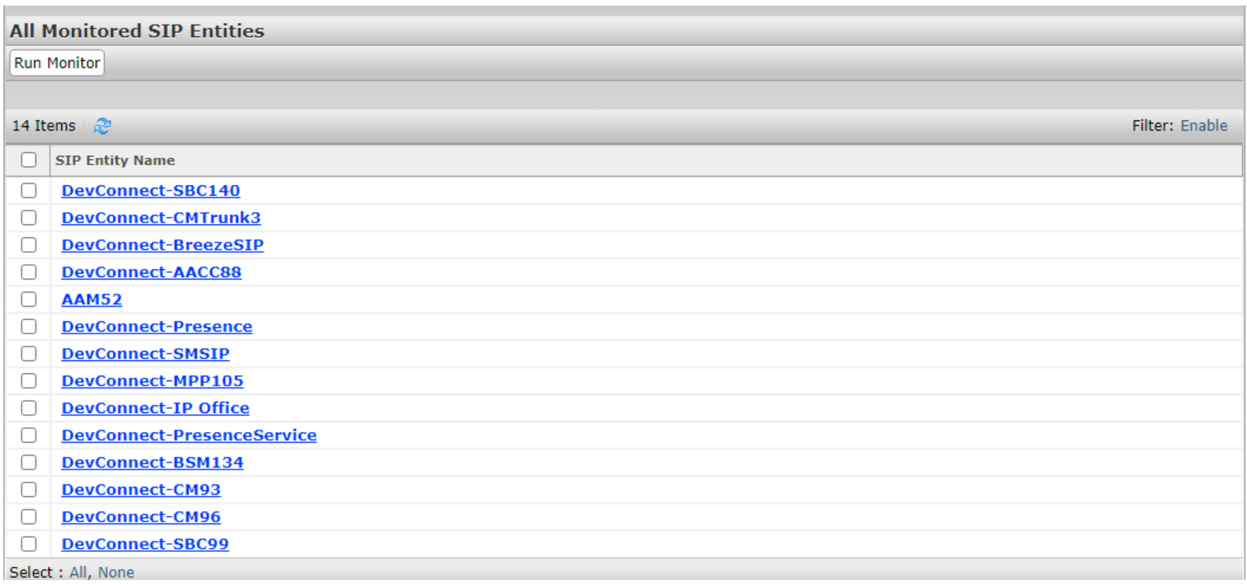
8. Configure Omilia OCP Conversational Voice Service

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

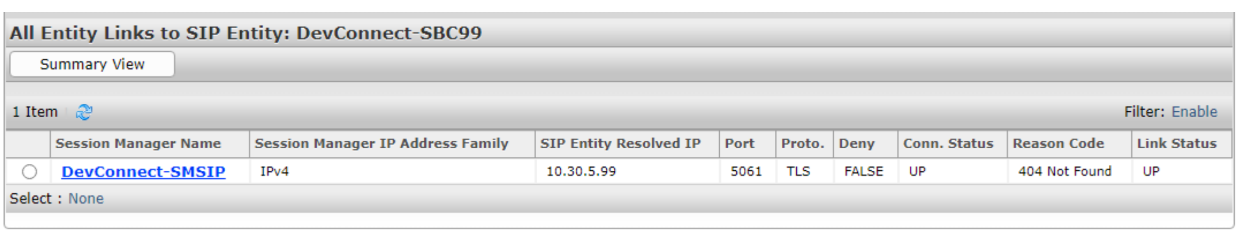
9. Verification Steps

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.

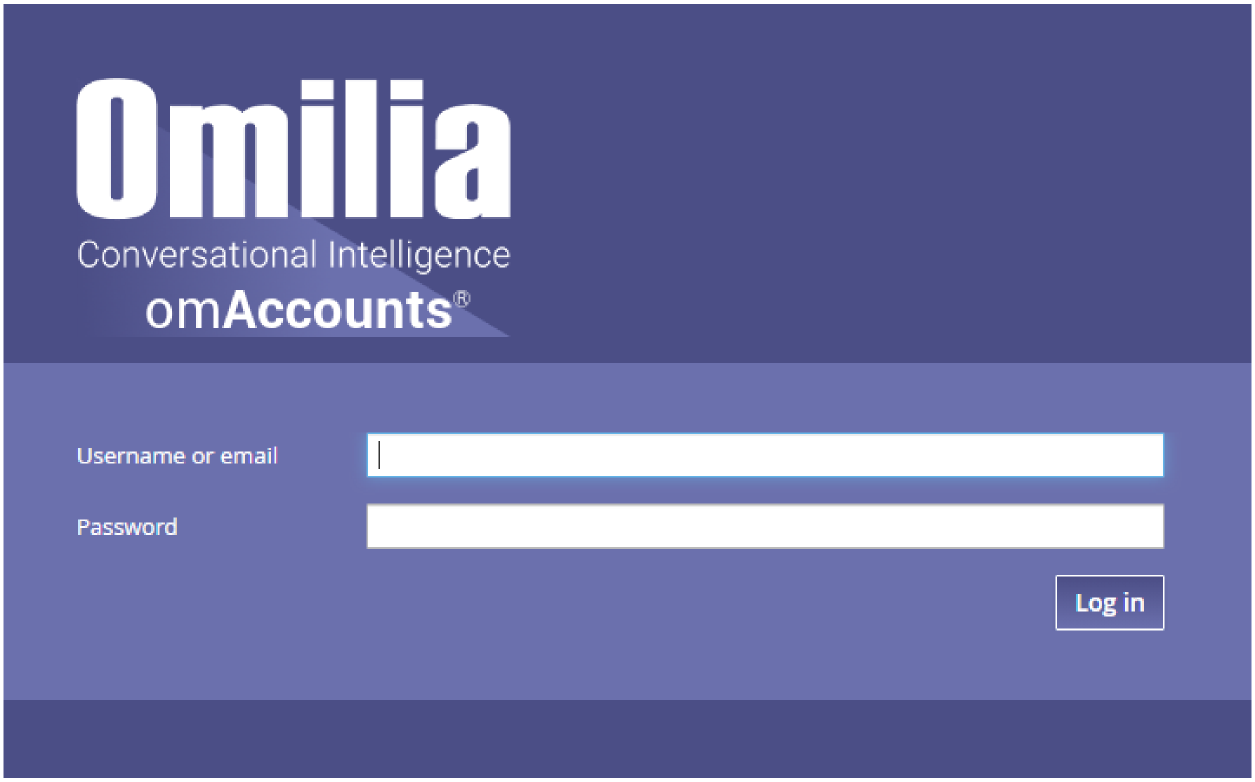


Verify **Conn. Status** is **UP.**

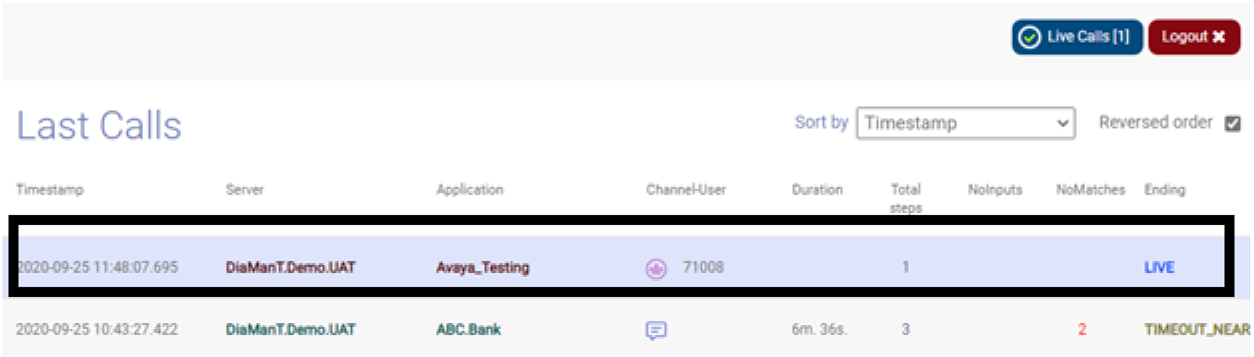


9.2. Verify Call Routing,

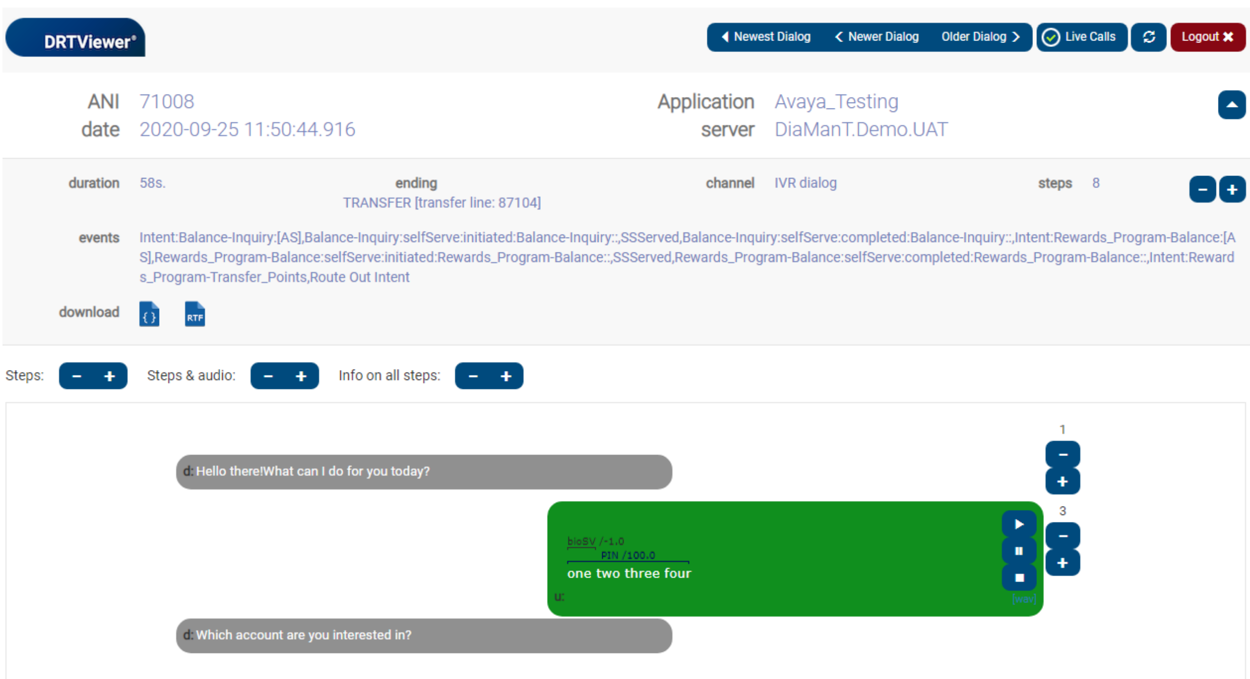
Place a call from the Avaya Endpoints/PSTN to Omilia OCP Conversational Voice Service, ensure the call can be answered by virtual assistants. When the virtual assistant receives a call, login Omilia omAccounts page provided by Omilia. Enter credentials to login.



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



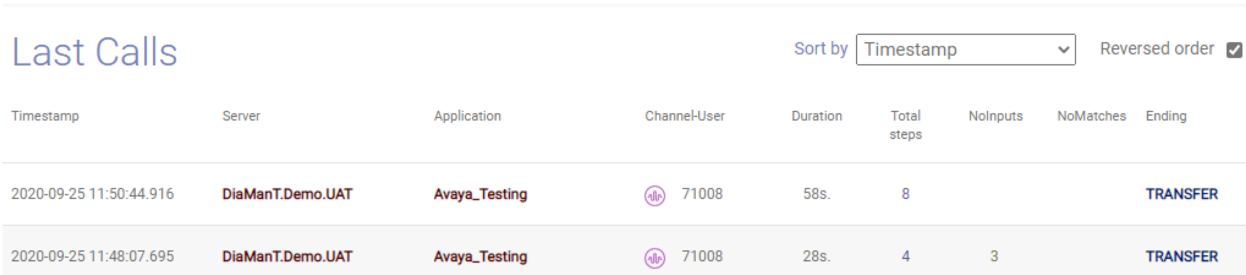
The conversation between virtual assistant and user is show as below:



Solution & Interoperability Test Lab Application Notes

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

Sort by Timestamp Reversed order

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/

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.