



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Modular Messaging R5.2 with Orange Open Trade – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Orange Open Trade trading solution to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Modular Messaging. Orange Open Trade trading solution consists of trading turret endpoints attached to a server which communicates with Avaya Aura® Session Manager via a SIP trunk.

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 used to enable Orange Business Services – Trading Solutions Open Trade to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Orange Open Trade trading solution consists of trading turret endpoints attached to proprietary Orange PBX which communicates with Avaya Aura® Session Manager via a SIP trunk.

Orange Business Services - Trading Solutions is a leading provider of convergent voice and electronic trading infrastructure and services for the trading communities. In 2010, Orange Business Services - Trading Solutions launched Open Trade. Open Trade is a complete solution that meets the mandatory high-demanding voice trading communication requirements. It is made of the Open Trade Smart Turrets (the terminal), the Open Trade Communication Manager and Plug-in Units. Open Trade is SIP compliant and interfaces with Avaya Aura® Session Manager via a SIP trunk

The Open Trade endpoints do not register with Session Manager. Calls to Open Trade endpoints from Avaya endpoints are established using appropriate call routing on both Avaya Aura® Communication Manager and Avaya Aura® Session Manager, as described in these application notes with Avaya Modular Messaging providing voicemail.

2. General Test Approach and Test Results

The general test approach was to validate correct operation of a variety of call handling scenarios and recovery from service interruption.

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.

2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of successful execution of the following features and link failure scenarios:

- Basic call incoming/outgoing, calling/called party terminates
- Call forwarding to/from Open Trade/Avaya endpoints
- Call Coverage
- Supervised Transfer/Blind transfer
- Name/number presentation
- Conferencing
- Voicemail related activities and MWI verification
- DTMF recognition
- Barge-In

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP4 build R016x.02.0.823.0-20199
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP3
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Modular Messaging running on S3500 Servers	5.2 Patch 8 MAS - 9.2.150.13
Avaya 9630 IP Deskphone	<ul style="list-style-type: none">• H323 S3.105S• SIP 2.6.8.4
Open Trade Administration	3.0.5.2
Open Trade Everywhere	1.0.4

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using the Communication Manager System Administration Terminal (SAT).

5.1. Dialplan

In order that calls are routed to the extensions configured on the Open Trade solution, the dialplan must be configured accordingly using the **change dialplan analysis command**. In this case a **4** digit **Dialed String** beginning with **4** is routed to the uniform-dialplan (**udp**) table.

change diaplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 1			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	3	fac							
2	10	udp							
3	11	udp							
4	4	udp							
5	4	ext							
6	4	ext							
7	3	dac							
8	4	udp							
9	1	fac							
*	3	fac							

5.2. Call Routing

The Application Notes assume that the relevant digital, SIP and H323 stations are configured and routing to Session Manager and the PSTN is in place. Use the **change uniform-dialplan 0** command and configure as shown below, where a matching patten of **4** with a **Length** of **4** digits is sent to the **aar** table.

change uniform-dialplan 0							Page 1 of 2
UNIFORM DIAL PLAN TABLE							Percent Full: 0
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num	
2	10	0		ars	n		
3	11	0		aar	n		
4	4	0		aar	n		
8	4	0		aar	n		
					n		

Use the **change aar analysis 0** command. Assign values for this command as shown in the following table. In this case the **Dialed String 4** digits in length is routed using **Route Pattern 1** where route pattern 1 is a preconfigured route to Session Manager.

change aar analysis 0							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
3	11	11	1	unku		n	
4	4	4	1	unku		n	
402	4	4	4	aar		n	
5	4	4	1	aar		n	
5999	4	4	1	unku		n	
6000	4	4	1	unku		n	
6001	4	4	1	unku		n	
6002	4	4	1	unku		n	
6003	4	4	1	unku		n	
8000	4	4	1	unku		n	
8897	4	4	1	aar		n	

5.3. Configure Signalling Group

It is assumed the necessary signaling group and trunk configuration has been completed for the interface between Communication Manager and Session Manager. Enter the command **change signaling-group x** where **x** is the signaling group relevant to the trunk between Communication Manager and Session Manager, in this case **1**. Ensure that the items highlighted below are configured accordingly in order that the DTMF and shuffling features work as expected.

change signaling-group 1	Page 1 of 2
SIGNALING GROUP	
Group Number: 1	Group Type: sip
IMS Enabled? n	Transport Method: tcp
Q-SIP? n	
IP Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM
Near-end Node Name: procr	
Near-end Listen Port: 5060	
Far-end Node Name: sm62sigint	
Far-end Listen Port: 5060	
Far-end Network Region: 1	
Far-end Domain:	
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y	IP Audio Hairpinning? y
H.323 Station Outgoing Direct Media? y	Initial IP-IP Direct Media? y
	Alternate Route Timer(sec): 6

6. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Avaya Aura® Session Manager configuration required for interoperating with Open Trade.

Session Manager is managed via Avaya Aura® System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button

AVAYA Avaya Aura® System Manager 6.2

Home / Log On

Log On

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

Log On

[Change Password](#)

6.1. Configure Adaptation

In order for successful interoperation of Open Trade with Session Manager over a SIP trunk, an Adaptation must be configured. Click **Routing → Adaptations → New** enter a **Name** to identify this Adaptation, select **Click to add module** from the drop down box next to **Module Name** and set the **New Module Name** to **DigitConversionAdapter**. Set the **Module Parameter** to **odstd=172.29.187.244 osrcd=10.10.16.148 fromto=true**. For a SIP Entity using this Adaptation, the SIP messaging will be modified so that the destination domain (**odstd**) and source domain (**osrcd**) are changed to 172.29.187.244 and 10.10.16.148, the Open Trade CAB IP address and the Session Manager SIP signalling interface IP address respectively. Click **Commit** when done.

Home / Elements / Routing / Adaptations [Help ?](#)

Adaptation Details Commit Cancel

General

* **Adaptation name:**

New module name:

Module parameter:

Egress URI Parameters:

Notes:

6.2. Configure Etrali Open Trade Entity

A SIP Entity must be created for the Open Trade CAB SIP interface. Click **Routing** → **SIP Entities** → **New** assign an identifying **Name**, the **FQDN or IP Address** for the Open Trade CAB SIP interface, set the **Type** to **SIP Trunk**, choose the Adaptation configured in **Section 6.1** from the drop down box and click **Commit** when done.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: OpenTrade

* FQDN or IP Address: 172.29.187.244

Type: SIP Trunk

Notes:

Adaptation: OTAdaptation

Location:

Commit Cancel

6.3. Configure Entity Link

The configuration of an Entity Link connects the Session Manager SIP Entity with the Open Trade CAB SIP Entity. Click **Routing** → **Entity Links** → **New** assign an identifying **Name** choose the entity assigned to the preconfigured Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TCP**, enter **5060** for the Port, choose the Open Trade CAB SIP entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop down box. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to Open Trade.

Home / Elements / Routing / Entity Links

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ToOpenTrade	* SM62	TCP	* 5060	* OpenTrade	* 5060	Trusted	

Commit Cancel

6.4. Create Routing Policy

Click **Routing** → **Routing Policies** → **New** assign an indentifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select**.

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Choose the Open Trade Entity configured in **Section 6.2** and click **Select**.

Home / Elements / Routing / Routing Policies

SIP Entity List Select Cancel

SIP Entities

13 Items | [Refresh](#) Filter: [Enable](#)

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	CM62	10.10.16.142	CM	
<input type="radio"/>	CMM62	10.10.16.142	CM	
<input type="radio"/>	ExperiencePortal	10.10.16.99	Voice Portal	
<input type="radio"/>	IBM	10.10.16.190	SIP Trunk	
<input type="radio"/>	MM52	10.10.16.26	Modular Messaging	
<input type="radio"/>	OfaxBrookTrout	10.10.16.103	SIP Trunk	
<input type="radio"/>	OfaxDiva	10.10.16.104	SIP Trunk	
<input checked="" type="radio"/>	OpenTrade	172.29.187.244	SIP Trunk	

Review the configuration and click **Commit** when done.

[Home](#) / [Elements](#) / [Routing](#) / [Routing Policies](#)

[Help ?](#)

Routing Policy Details

Commit

Cancel

General

* Name:

ToOpenTrade

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
OpenTrade	172.29.187.244	SIP Trunk	

6.5. Administer Dial Patterns

Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate destination. In **Section 5.2** Communication Manager is configured to route 4 digit strings beginning with 4 to Session Manager. To create a Dial Pattern to route these digits from Session Manager to Open Trade click **Routing → Dial Patterns → New**. Under Pattern enter the numbers presented to Session Manager by Communication Manager in the Patterns box. Set the Min and Max digit string length, and set SIP Domain to ALL. In the **Originating Locations and Routing Policies** section of the web page, click **Add**.

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns](#)

[Help ?](#)

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

General

* Pattern: 40

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

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

0 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
--------------------------	---------------------------	----------------------------	---------------------	------	-------------------------	----------------------------	----------------------

Originating Location and Routing Policy List

[Select](#) [Cancel](#)

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations1 Item | [Refresh](#)Filter: [Enable](#)

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	DevConnectLab	
Select : All , None		

Routing Policies

9 Items | [Refresh](#)Filter: [Enable](#)

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToCM6.2	<input type="checkbox"/>	CM62	
<input type="checkbox"/>	ToCMM62	<input type="checkbox"/>	CMM62	
<input type="checkbox"/>	ToIBM	<input type="checkbox"/>	IBM	
<input type="checkbox"/>	ToMM	<input type="checkbox"/>	MM52	
<input type="checkbox"/>	ToOfaxBrookTrout	<input type="checkbox"/>	OfaxBrookTrout	
<input type="checkbox"/>	ToOfaxDiva	<input type="checkbox"/>	OfaxDiva	
<input checked="" type="checkbox"/>	ToOpenTrade	<input type="checkbox"/>	OpenTrade	

Dial Pattern Details

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

General

* Pattern: * Min: * Max: Emergency Call: ☐Emergency Priority: Emergency Type: SIP Domain: Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)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	Rou Poli Not
<input type="checkbox"/>	-ALL-	Any Locations	ToOpenTrade	0	<input type="checkbox"/>	OpenTrade	

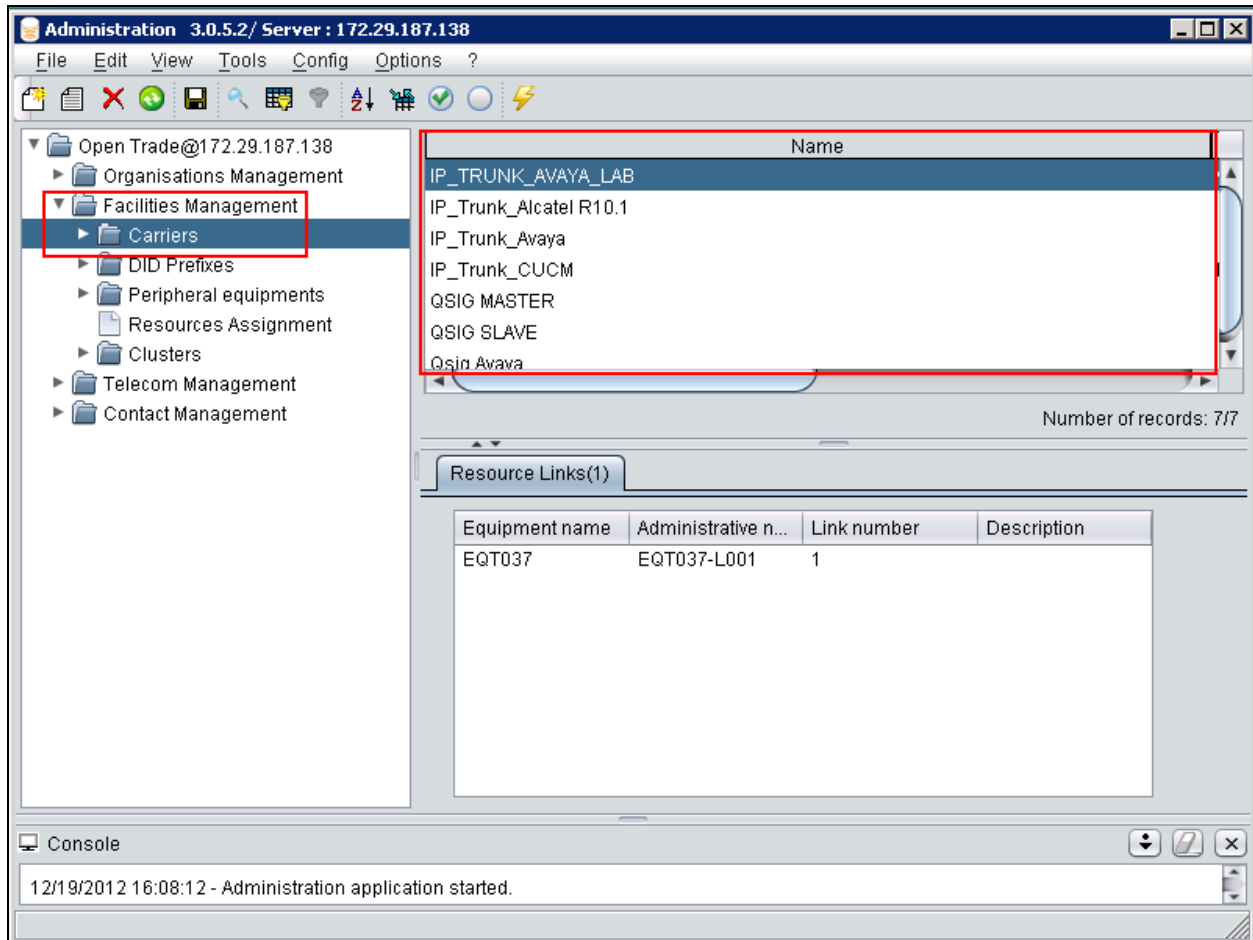
7. Configure Orange Open Trade Server

Start the Open Trade Administration program, and log in with the appropriate credentials.



7.1. Create Carrier

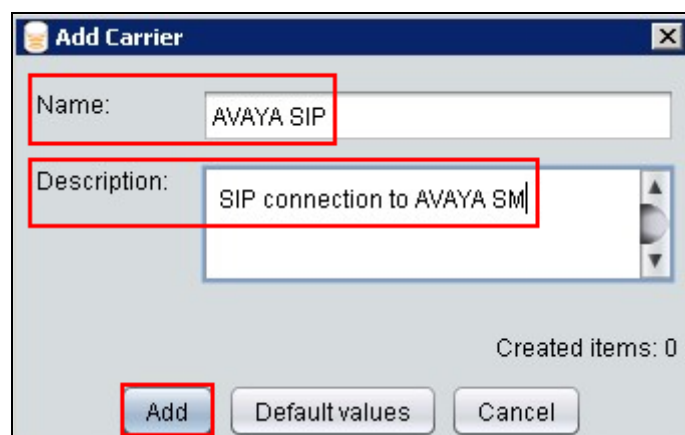
Expand the **Facilities Management** icon and select the **Carriers** menu element. Place the cursor under the **Name** pane header and right-click the mouse.



Select **Create** from the menu which appears.

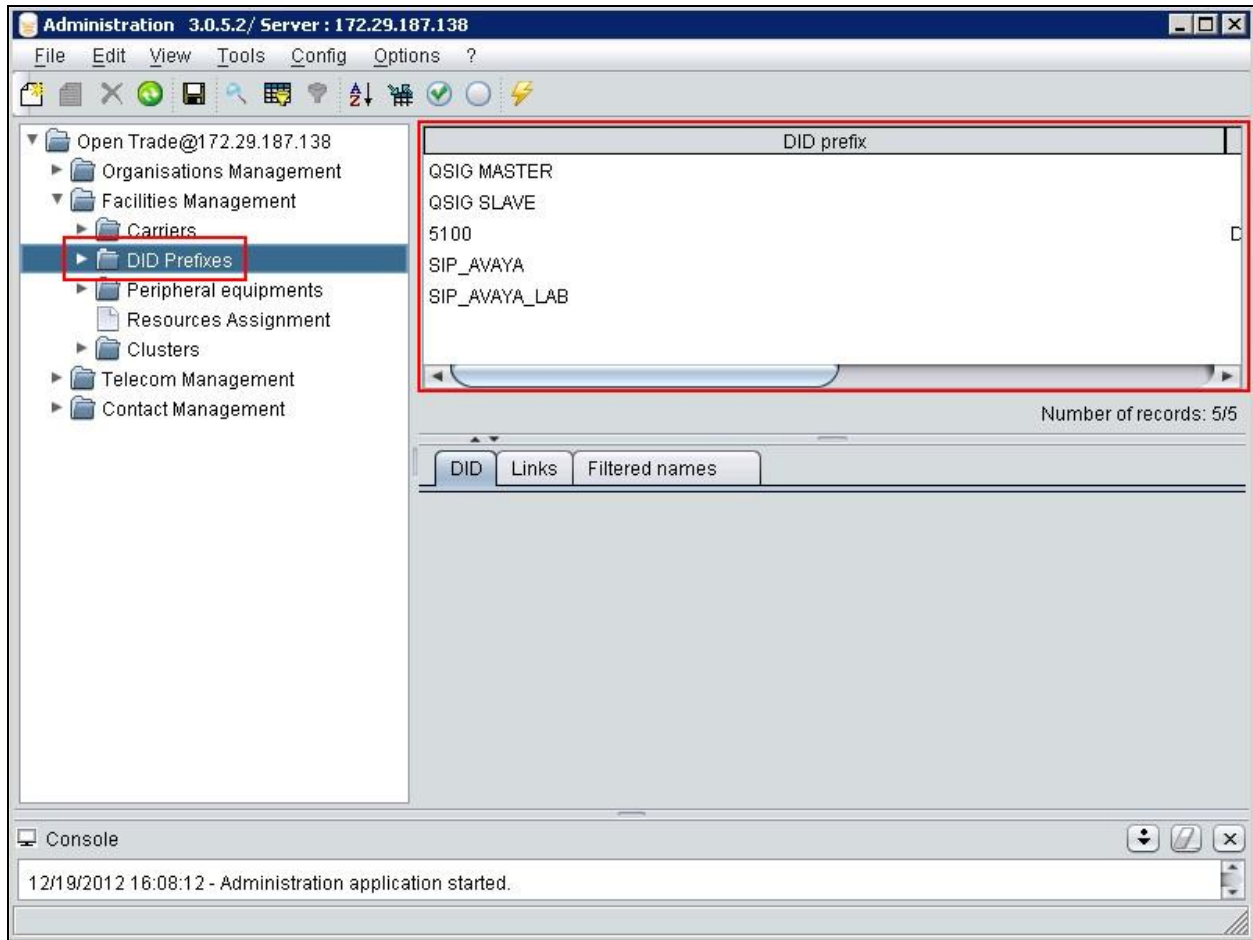


Enter an appropriate **Name** and **Description** and click **Add**.















7.2. Create DID Prefixes

Expand the **DID Prefixes** menu item. Place the cursor in the **DID prefix** pane and right-click the mouse.



Select **Create** from the menu which appears

 <u>C</u> reate	Insert
 <u>M</u> odify	Enter
 <u>D</u> elete	Delete
 Define F <u>i</u> lter	Ctrl+R
 <u>S</u> ort	Ctrl+T
 <u>S</u> earch	Ctrl+F
 <u>R</u> efresh	Ctrl+F5
 R <u>e</u> size columns	Ctrl+F7
 D <u>i</u> splay columns	Ctrl+F8
 S <u>e</u> lect <u>a</u> ll	Ctrl+A
 C <u>a</u> ncel selection	Ctrl+Z
 E <u>x</u> port <u>d</u> ata (active table)	Ctrl+E

Enter an identifying name in the **DID prefix** field and click **Add**.

DID prefix Add

DID prefix

DID prefix:

Filtered names (beginning with...):

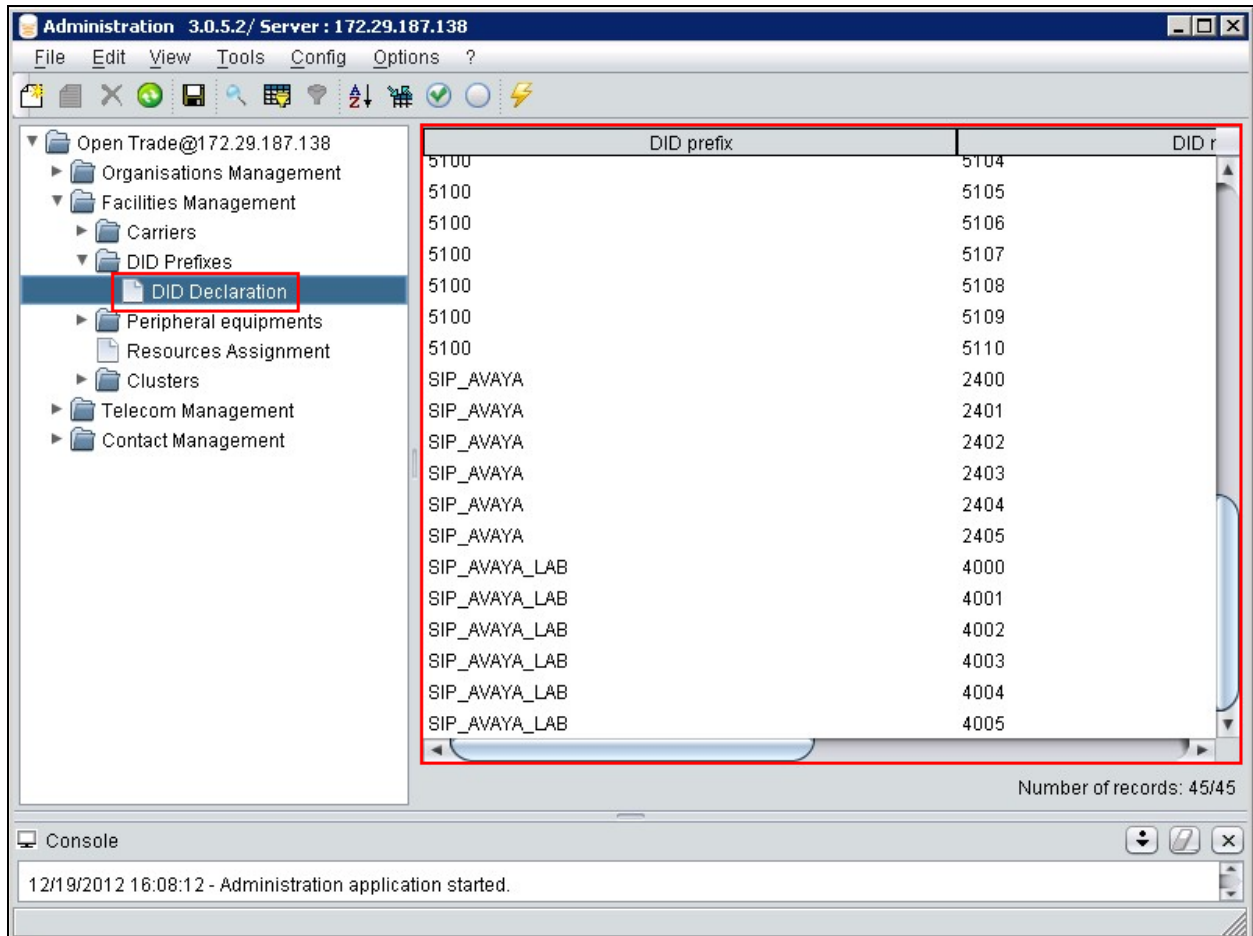
Names

Description:

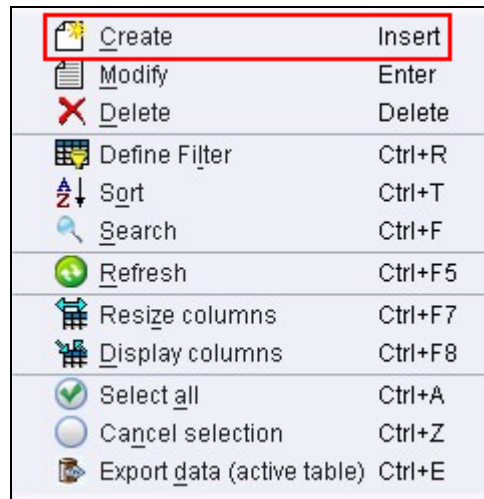
Created items: 0

7.3. Create DID Declaration

Expand the **DID Declaration** menu item. Place the cursor under the first blank entry in the **DID prefix** pane and right-click the mouse.



Select **Create** from the menu which appears.



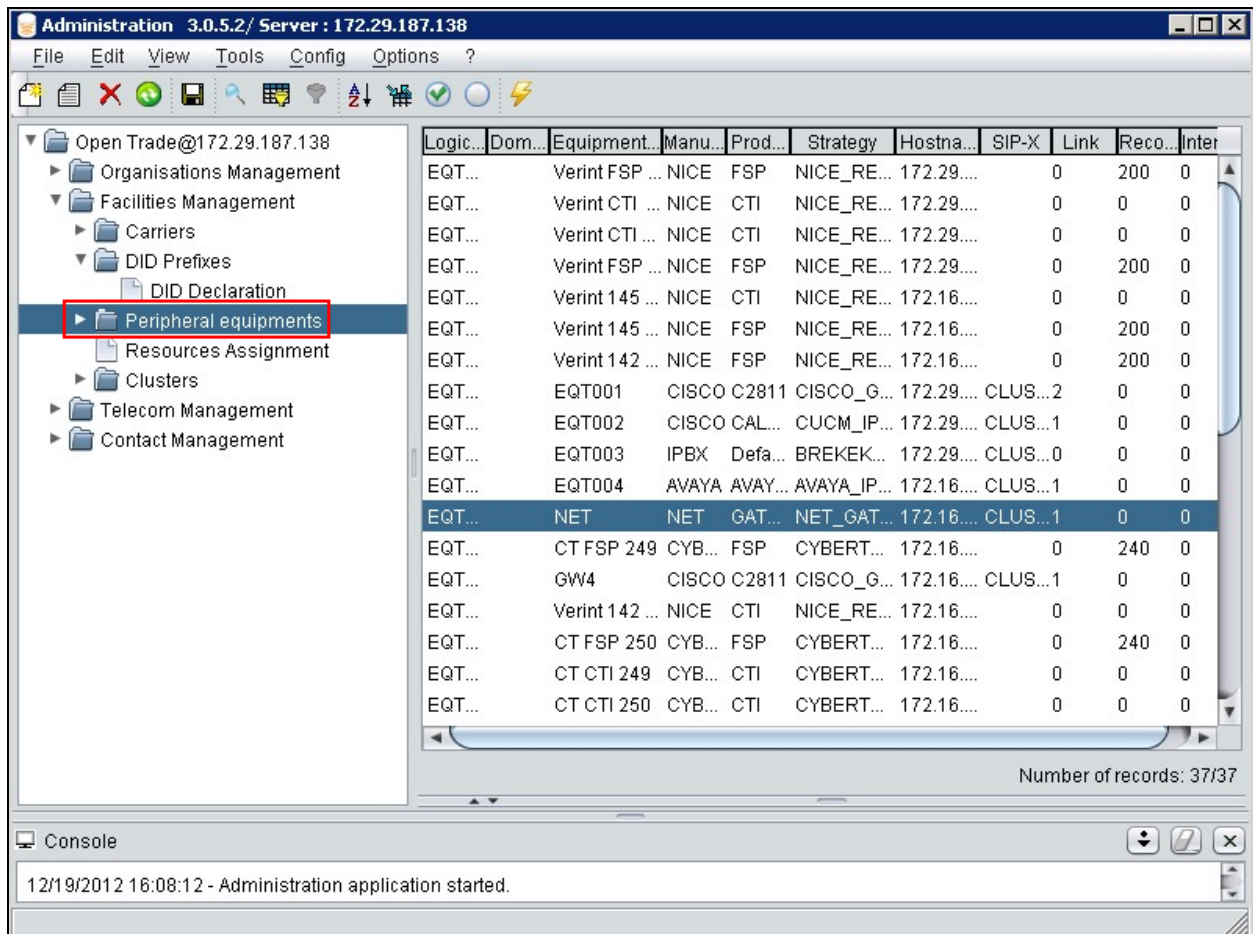
Enter the following values in the **Add DID** screen which appears and click **Add**.

- **DID prefix** – select the DID Prefix created in **Section 7.2**
- **From** – enter the first number of the range of numbers Open Trade will receive call for. In this case **4000**.
- **To** – enter the last number of the range of numbers Open Trade will receive calls for. In this case **4010**.
- **Organization** – select the name of the appropriate Organization from the drop-down menu, this is preconfigured and the details are not covered here.










A screenshot of a dialog box titled 'Add DID'. The dialog box has a blue header bar with a close button (X) on the right. The main area contains four fields: 'DID prefix:' with a dropdown menu showing 'SIP TRUNK', 'From:' with a text box containing '4000', 'To:' with a text box containing '4010', and 'Organisation:' with a dropdown menu showing 'Recording'. A red rectangular border highlights these four fields. At the bottom right, it says 'Created items: 0'. At the bottom left, there are three buttons: 'Add', 'Default values', and 'Cancel'. The 'Add' button is highlighted with a red rectangular border.

7.4. Create Peripheral Equipment

This section relates to the Avaya components from/to SIP traffic will be routed. Expand the **Peripheral equipments** menu item, Place the cursor under the first blank entry in the right hand pane and right-click the mouse.



Select **Create** from the menu which appears.

 <u>C</u> reate	Insert
 <u>M</u> odify	Enter
 <u>D</u> elete	Delete
 Define <u>F</u> ilter	Ctrl+R
 <u>S</u> ort	Ctrl+T
 <u>S</u> earch	Ctrl+F
 <u>R</u> efresh	Ctrl+F5
 <u>R</u> esize columns	Ctrl+F7
 <u>D</u> isplay columns	Ctrl+F8
 Select <u>a</u> ll	Ctrl+A
 <u>C</u> ancel selection	Ctrl+Z
 Export <u>d</u> ata (active table)	Ctrl+E

Enter the following values in the **Modify Peripheral equipment** screen which appears and click **Ok**.

- **Manufacturer** – select **AVAYA** from the drop down list.
- **Product name** – select **AVAYA AURA** from the drop down list.
- **SIP Strategy** – select **AVAYA_IPBX** from the drop down list.
- **Equipment name** – enter an identifying name.
- **IP Address or Hostname** – enter the IP address of Communication Manager, Session Manager and Modular Messaging.
- **Telco links** – enter **1**

Modify Peripheral equipment

Peripheral equipment

Logical name: EQT037

Equipment name: EQT037

SIP-X name: CLUSTER01-CABT001

SIP-X Logical name: CLUSTER01-CABT001

Contact parameters

Domain:

	IP Address or Hostname
1	10.10.16.148
2	10.10.16.142
3	10.10.16.26
4	

Resources

Telco Links: 1

Recording channels: 0

Interco capacity: 0

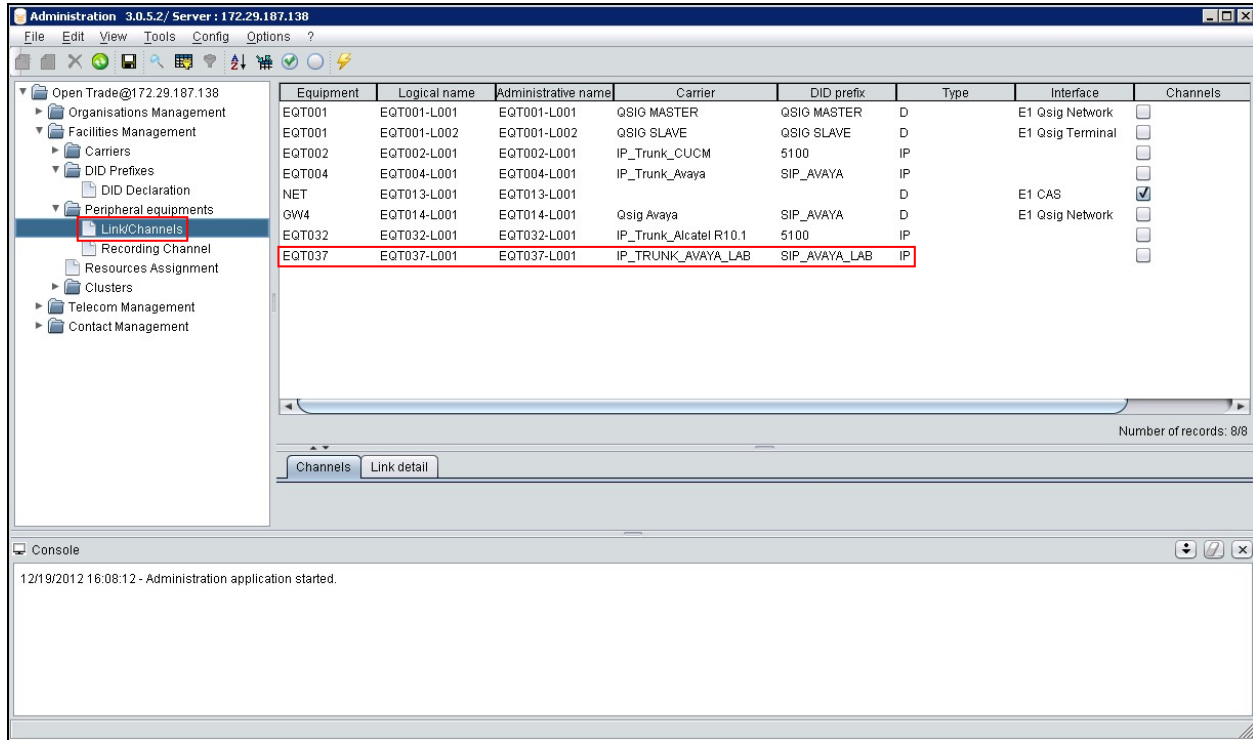
Description: Avaya Lab Certification (VPN)

Advanced configuration >>

Ok Restore Cancel

7.5. Create Link/Channels

Expand the **Link/Channels** menu item and double click the newly created Equipment created in **Section 7.4**.



Enter the following Link values in the **Update Telco Link** screen which appears and click **Ok**.

- **Link name** – enter an identifying name.
- **Carrier** – select the Carrier created in **Section 7.1**.
- **DID prefix** – select the DID prefix created in **Section 7.2**.
- **Type** – select **IP** from the drop down list.
- **Number of channels** – enter **30**.

Update Telco Link

Link identity

Equipment name: EQT037 Logical name: EQT037-L001

Link name: EQT037-L001

Description:

Link configuration

Carrier: AVAYA SIP

DID prefix: SIP TRUNK

Type: IP

Interface: None

Number of channels: 30

Leased lines (Dissociated channels) ☐

Ok Restore Cancel













7.6. Create Routing Rule

Expand the **Telecom Management** item and select the **Routing rules** menu element. Place the cursor under the first blank entry in the right hand pane and right-click the mouse to create a new routing rule to Session Manager.

The screenshot shows the Administration 3.0.5.2/ Server: 172.29.187.138 interface. The left sidebar shows the navigation tree with 'Telecom Management' expanded and 'Routing rules' selected. The main pane displays a table of routing rules. The table has columns: Domain, Outgoing access co..., Source prefix, Carrier, Target prefix, and Is activated. The table contains 15 records. The first record is highlighted in blue. The bottom status bar shows 'Number of records: 15/15'.

Domain	Outgoing access co...	Source prefix	Carrier	Target prefix	Is activated
PR	0	24	IP_Trunk_Awaya	24	<input checked="" type="checkbox"/>
PU	0		IP_TRUNK_AWAYA_LAB		<input checked="" type="checkbox"/>
PR	0	51	IP_Trunk_CUCM	51	<input checked="" type="checkbox"/>
PR		9	QSIG SLAVE	9	<input type="checkbox"/>
PR		3	QSIG MASTER	3	<input checked="" type="checkbox"/>
PR		7	Forbidden	7	<input checked="" type="checkbox"/>
PR	0	98	IP_Trunk_CUCM	98	<input checked="" type="checkbox"/>
PR	0	6	IP_Trunk_Awaya	6	<input type="checkbox"/>
PR		66	Qsig Awaya	6	<input checked="" type="checkbox"/>
PR		40	IP_Trunk_CUCM	40	<input checked="" type="checkbox"/>
PR	0	35	IP_Trunk_AlcateI R10.1	35	<input checked="" type="checkbox"/>
PR		88	IP_TRUNK_AWAYA_LAB	88	<input checked="" type="checkbox"/>
PU		9	IP_TRUNK_AWAYA_LAB	9	<input checked="" type="checkbox"/>
PR		6	IP_TRUNK_AWAYA_LAB	6	<input checked="" type="checkbox"/>
PR		50	IP_TRUNK_AWAYA_LAB	50	<input checked="" type="checkbox"/>

Select **Create** from the menu which appears.

 <u>C</u> reate	Insert
 <u>M</u> odify	Enter
 <u>D</u> elete	Delete
 Define <u>F</u> ilter	Ctrl+R
 <u>S</u> ort	Ctrl+T
 <u>S</u> earch	Ctrl+F
 <u>R</u> efresh	Ctrl+F5
 <u>R</u> esize columns	Ctrl+F7
 <u>D</u> isplay columns	Ctrl+F8
 <u>S</u> elect all	Ctrl+A
 <u>C</u> ancel selection	Ctrl+Z
 <u>E</u> xport data (active table)	Ctrl+E

Enter the following values in the **Modify Routing rule** screen which appears and click **Ok**.

- **Domain** – select **Private** from the drop down list.
- **Source prefix** – enter the first digit of the extension range configured for Avaya endpoints.
- **Carrier** – enter the Carrier configured in **Section 7.1**.
- **Target prefix** - enter the first digit of the extension range configured for Avaya endpoints.

Modify Routing rule

Routing rule:

Start hour: None None None

Country: All

Site: All

Site Outgoing Access code:

From

Domain: Private

Source prefix: 6

To

Carrier: AVAYA SIP

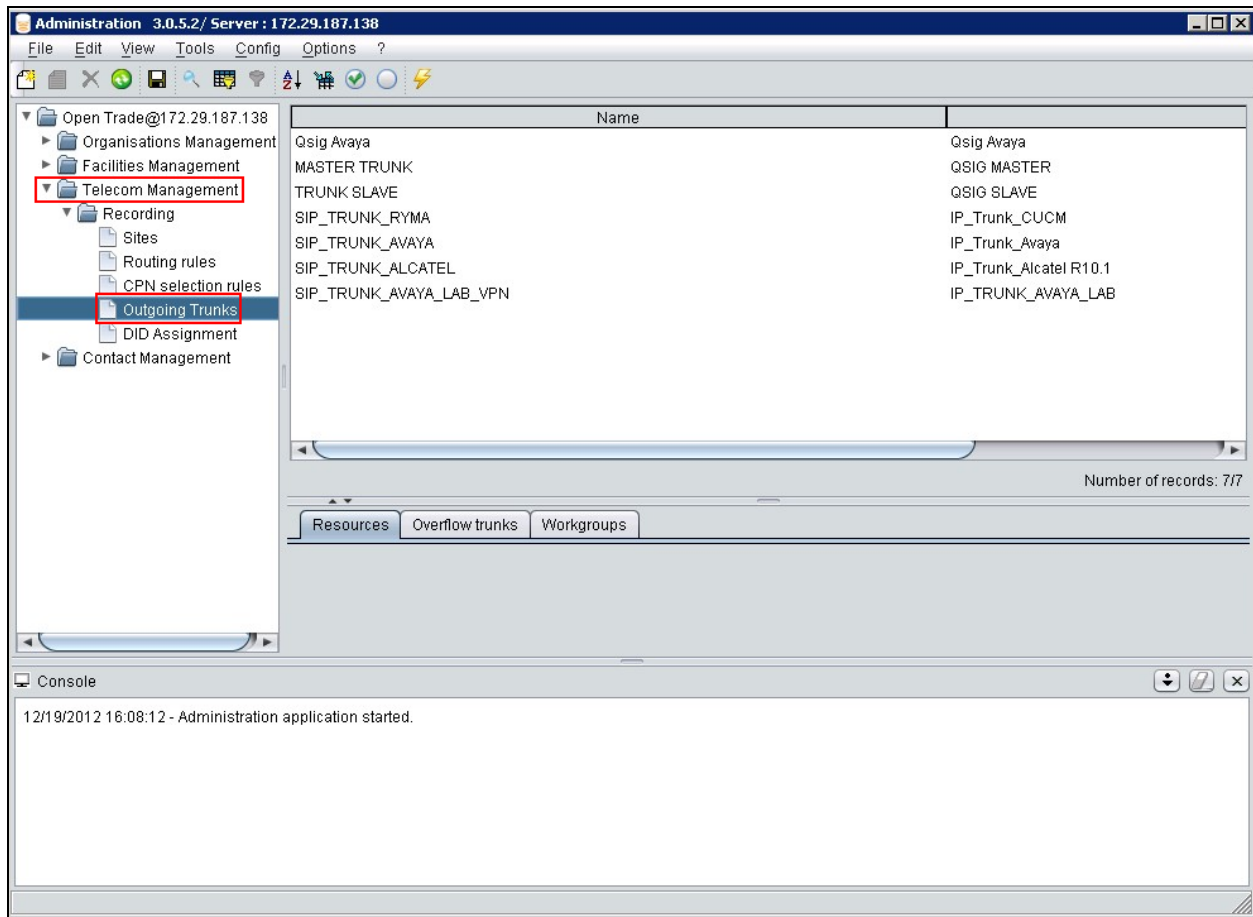
Target prefix: 6

☒ Is activated












Ok Restore Cancel

8. Create Outgoing Trunk

Expand the **Telecom Management** item and select the **Outgoing Trunks** menu element. Place the cursor under the first blank entry in the right hand pane and right-click the mouse to create a new outgoing trunk to the Avaya solution.



Select “Create” from the menu which appears.

 <u>C</u> reate	Insert
 <u>M</u> odify	Enter
 <u>D</u> elete	Delete
 Define <u>F</u> ilter	Ctrl+R
 <u>S</u> ort	Ctrl+T
 <u>S</u> earch	Ctrl+F
 <u>R</u> efresh	Ctrl+F5
 <u>R</u> esize columns	Ctrl+F7
 <u>D</u> isplay columns	Ctrl+F8
 <u>S</u> elect all	Ctrl+A
 <u>C</u> ancel selection	Ctrl+Z
 <u>E</u> xport data (active table)	Ctrl+E

Enter the following values in the **Modify Outgoing trunk** screen which appears and click **Ok**.

- **Carrier** – select the carrier created in **Section 7.1** from the drop down list.
- **Resources** – add the peripheral equipment created in **Section 7.4**.
- **Workgroup** – add the appropriate Workgroup from the drop-down menu, this is preconfigured and the details are not covered here.

Modify Outgoing trunk

Outgoing Trunk

Name: SIP_TRUNK_AVAYA_LAB_VPI Carrier: IP_TRUNK_...

Workgroups

Name	Supplementary name	BE
WG_Recording		BU_Recording

Add Remove

Resources

Type	Equipment	Logical name	Administrative name
Link	EQT037	EQT037-L001	EQT037-L001

Add Remove

Overflow trunks

Site	Trunk	Activated
DKE_Recording	None	<input type="checkbox"/>

Ok Restore Cancel

9. Verification Steps

The correct installation and configuration of Orange Open Trade trading solution can be verified by performing the following steps shown below.

9.1. Verify Communication Manager SIP Trunk

Using the SAT terminal, enter the **status signaling-group <n>** command, where <n> is the number of the SIP signaling group which connects to Session Manager. Verify that the signaling **Group State** is **in-service**.

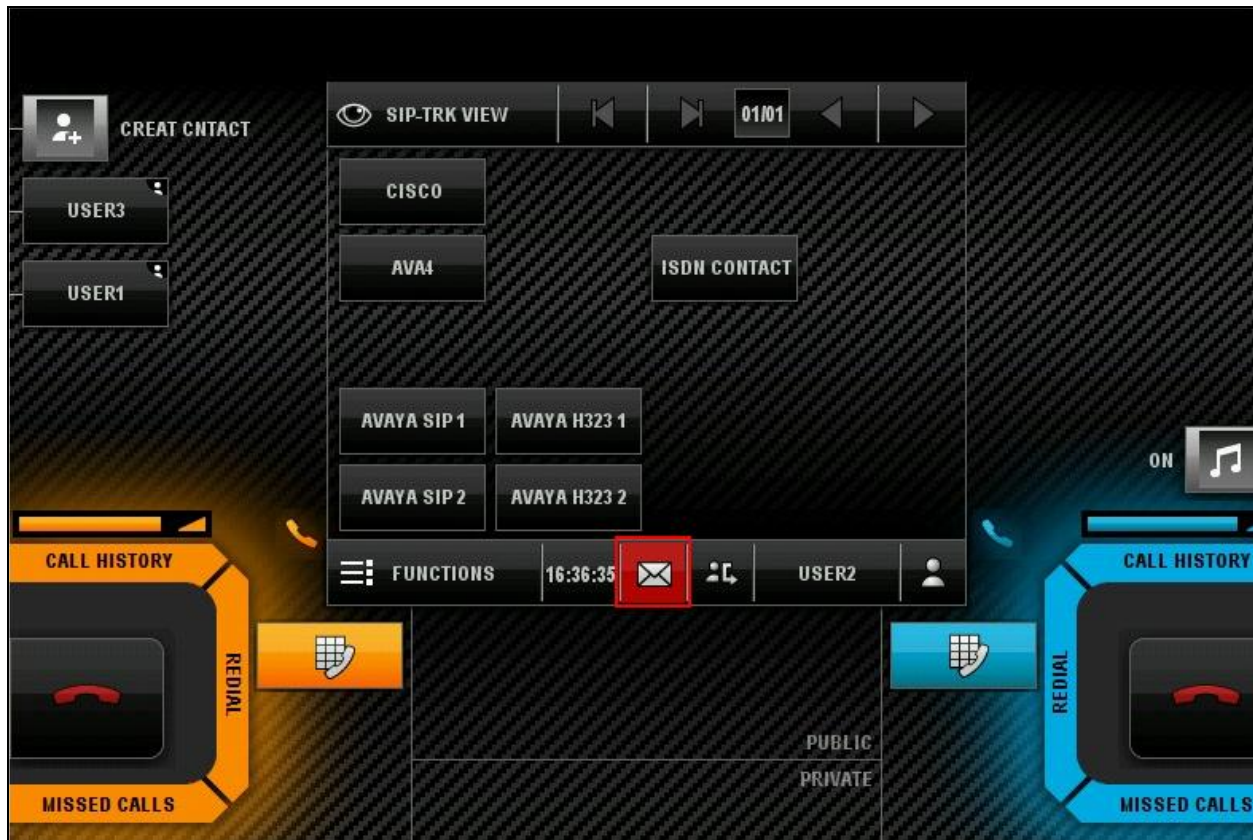
```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

9.2. Verify Open Trade Softphone Functionality

Place a call to/from an Open Trade turret extension number, ensure the call can be answered, controlled and terminated as expected. Leave a voicemail on the mailbox of the Open Trade extension, ensure that the message waiting indicator illuminates, highlighted below, and extinguishes when the voicemail is retrieved.



10. Conclusion

These Application Notes describe the compliance testing of the Orange Open Trade trading solution with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Open Trade passed all of the tests performed with observations noted in **Section 2.2**.

11. References

This section references documentation relevant to these Applications. Avaya product documentation, including the following, is available at <http://support.avaya.com>

- *Administering Avaya Aura® Communication Manager, Release 6.2*, 03-300509, Issue 7.0 December 2012

©2013 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.