



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.6 and Avaya Aura® Session Manager R6.3 to interoperate with Presence Technology OpenGate R10.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Presence Technology OpenGate to successfully interoperate with Avaya Communication Server 1000E and Avaya Aura® Session Manager. Presence Technology OpenGate provides ACD and CTI capabilities to companies that do not have any existing CTI or ACD capabilities on their PBX. Presence Technology OpenGate integrates with the Avaya solution using SIP trunks and digit manipulation.

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 verify Presence Technology OpenGate R10.0 can successfully interoperate with Avaya Communication Server 1000E R7.6 (CS1000E) and Avaya Aura® Session Manager R6.3. Presence Technology OpenGate is a telephony gateway that is fully integrated with Presence Technology's Contact Center Suite called Presence Suite. Presence Technology OpenGate allows the Presence Suite to integrate with the CS1000E PBX via a SIP connection to Session Manager.

2. General Test Approach and Test Results

Testing was performed manually by dialling numbers that were configured to route to OpenGate and receive ACD treatment. Testing included validation of correct operation of typical contact centre functions including, inbound voice call being delivered on an agent skill level basis and call queuing. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, and conference. The serviceability test cases were performed manually by busying out and releasing the SIP trunk and by disconnecting and reconnecting the LAN cables. Link Failure\Recovery was tested to ensure successful reconnection on link failure.

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

The focus of the interoperability test is the ACD functionality offered by OpenGate. All calls received from the PSTN by the CS1000E are routed via a SIP Trunk to Session Manager. Session Manager is then responsible for routing the calls to OpenGate to receive ACD treatment. OpenGate can route calls to Presence agents using Avaya 1140E endpoints. Presence OpenGate allows the Presence Suite to integrate with the CS1000E. The Presence Suite includes the Presence Server, Presence Mail Interactions Server, Presence Web Interactions Server, Presence Administrator, Presence Supervisor, and Presence Agent. The setup of Presence Suite is outside the scope of these Application Notes; please refer to **Section 10** in order to find information for the configuration of Presence Server.

These Application Notes assume that the installation and configuration relating to Presence Suite has already been completed and is not discussed. OpenGate specifies where to route each call and hence how to handle the calls, based on agent status information that the Presence Suite tracks from the Agent software, as well as the SIP trunk messaging for the calls it has routed.

In the sample configuration described in these Application Notes, calls are accepted from the PSTN and routed to OpenGate on digits 43xxxx. All calls that are destined for OpenGate are sent by dialling or routing PSTN calls to 43xxxx on the CS1000E which then routes the calls to Session Manager. OpenGate then maps these digits to an internal number which represents the ACD service queue and then routes the call to an available agent by dialling that agent's extension. OpenGate will have internal routing setup to route calls to the correct agent.

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on verifying OpenGate was capable of receiving calls from the CS1000E and providing ACD treatment to route those calls to available agents. The serviceability testing focused on verifying the ability of OpenGate to recover from adverse conditions, such as disconnecting the Ethernet cable from the OpenGate Server.

2.2 Test Results

All test cases passed successfully.

2.3 Support

Technical support can be obtained from Presence Technology OpenGate as follows:

- Email: support@presenceco.com
- Website: www.presenceco.com
- Phone: +34 93 10 10 300

3. Reference Configuration

Figure 1 shows the network topology in place during compliance testing. An Avaya Communication Server 1000E (CS1000E) was used as the hosting PBX. SIP trunks were configured between Session Manager and OpenGate. Presence Suite includes the Presence Agent desktop and the Presence OpenGate Server.

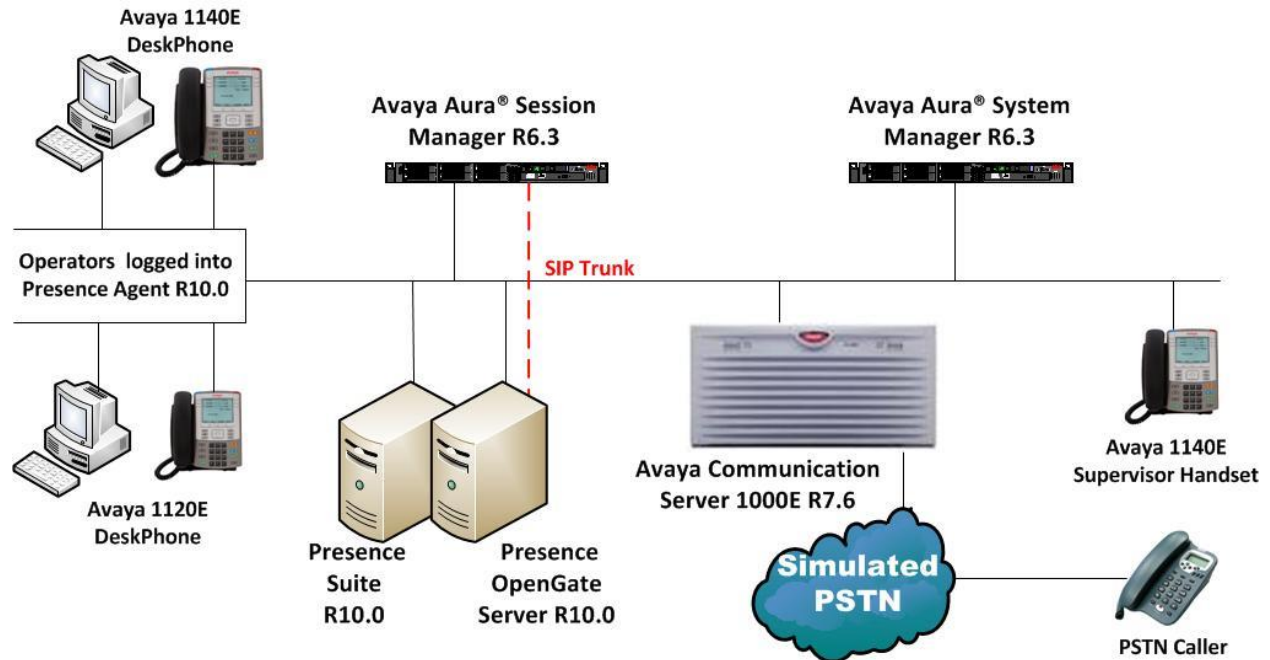


Figure 1: Network Topology used to test Presence Technology OpenGate

4. Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Avaya S8800 Server	R6.3 SP3 Build 6.3.0.8.5682-6.3.8.1814 Software Update Revision 6.3.3.5.1719
Avaya Aura® Session Manager running on an Avaya S8800 Server	R6.3 SP3 6.3.3.0.633004
Avaya CPPM running Avaya Communication Server 1000E	R7.6 (See Appendix A for Call Server and Signalling Server Patches)
Avaya 1140 Series Deskphone	UNISTim 0625C8Q
Avaya 1120 Series Deskphone	UNISTim 0624C8Q
Presence Server running on Windows Server 2008 SP2 containing: <ul style="list-style-type: none">• Presence Suite Server• Presence OpenGate Server	R10.0 R10.0
Presence Client running on Windows XP SP3 and Windows Server 2008 SP2	R10.0

Table 1: Hardware and Software Version Numbers

5. Configure Avaya Communication Server 1000E

The configuration and verification operations illustrated in this section were all performed using the PUTTY program. The information provided in this section describes the configuration of CS1000E for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Note: It is assumed that the CS1000E has already been configured for SIP and a connection is in place to Session Manager.

5.1 Create a Route for SIP calls

The following sections illustrate the setup of a new route and Coordinated Dial Plan (CDP) in order to send calls to OpenGate via Session Manager. To create a new route on the CS1000E overlay 16 is used. Use the **new** command in overlay 16 to create a new SIP route. Type **LD 16** at the > prompt to enter overlay 16. The route created is a **TIE** route in order to connect to Presence OpenGate via Session Manager. Subsets of these commands are listed below.

LD 16

Prompt	Response	Description
>	LD 16	Enter Overlay 16
REQ	new	Create new
TYPE	RDB	Route Data block
CUST	0	Customer Number as defined in LD15
ROUT	20	Route Number
TKTP	TIE	Route Type
VTRK	YES	Virtual Route
ZONE	1	Zone number associated with the route
PCID	SIP	Protocol for the route

5.2 Configure a Coordinated Dial Plan

A Coordinated Dial Plan is added to place calls across the SIP trunk to the OpenGate application. Add a Route List Block (RLB) to place calls over the SIP route created in **Section 5.1** above. Enter overlay 86 to configure a new RLB by typing **LD 86** at the > prompt. As shown below a new Route List Index (**RLI**) is added with a ROUT equal to that of the SIP Route created in **Section 5.1**.

LD 86

Prompt	Response	Description
>	LD 86	Enter Overlay 86
REQ	new	new/add
CUST	0	Customer number (default is 0)
FEAT	rlb	Route List Block
RLI	20	Route List index Number (any unused number)
ENTR	0	First Entry (0-2)
ROUT	20	Route Number configured in Section 5.1
DMI	0	Digit Manipulation Table (default is 0)
Return to end		

Once the RLB is added the Coordinated Dial Plan (CDP) is added in the form of a Distance Steering Code (**DSC**). Note that in the example below **43xxxx** is the **DSC** as this is the number used to route calls to the OpenGate application during the compliance testing. Enter overlay 87 to add a new **CDP** by typing **LD 87** at the > prompt.

LD 87

Prompt	Response	Description
>	LD 87	Enter Overlay 87
REQ	new	new/add
CUST	0	Customer number (default is 0)
FEAT	cdp	Coordinated Dial Plan
TYPE	dsc	Distance Steering Code
DSC	43	Extension number of the TENS Application
FLEN	6	Ext Length
DSP	LSC	DSP Type (Least Cost Routing)
RLI	20	Which RLB to use (Enter the RLB setup above)
Return to end		

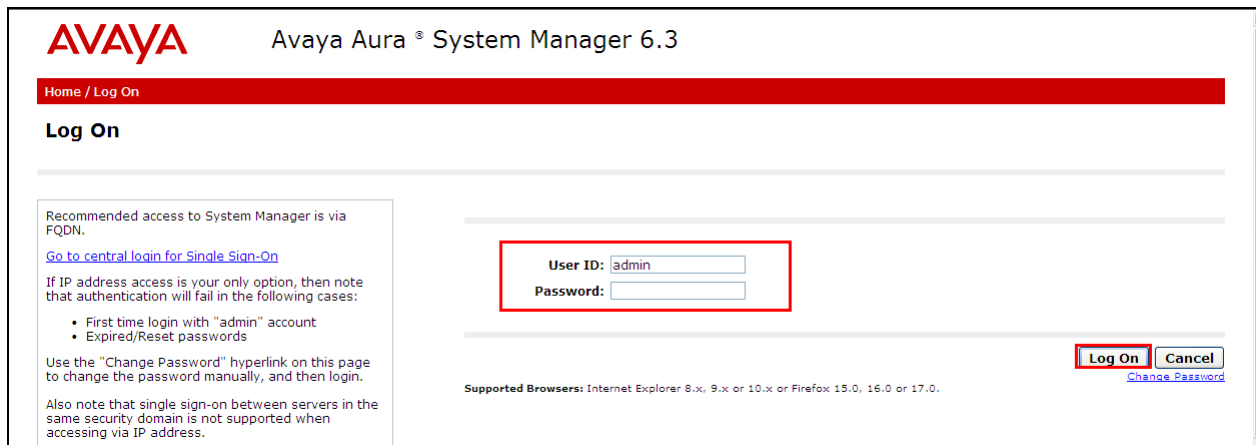
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

6.1 Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.



AVAYA Avaya Aura® System Manager 6.3

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.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

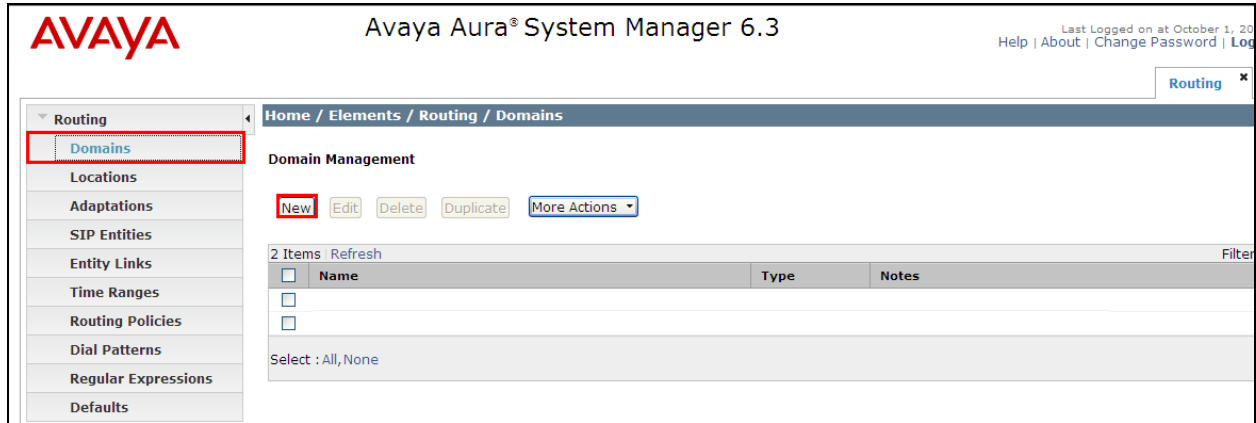
User ID: admin
Password:

Log On Cancel
[Change Password](#)

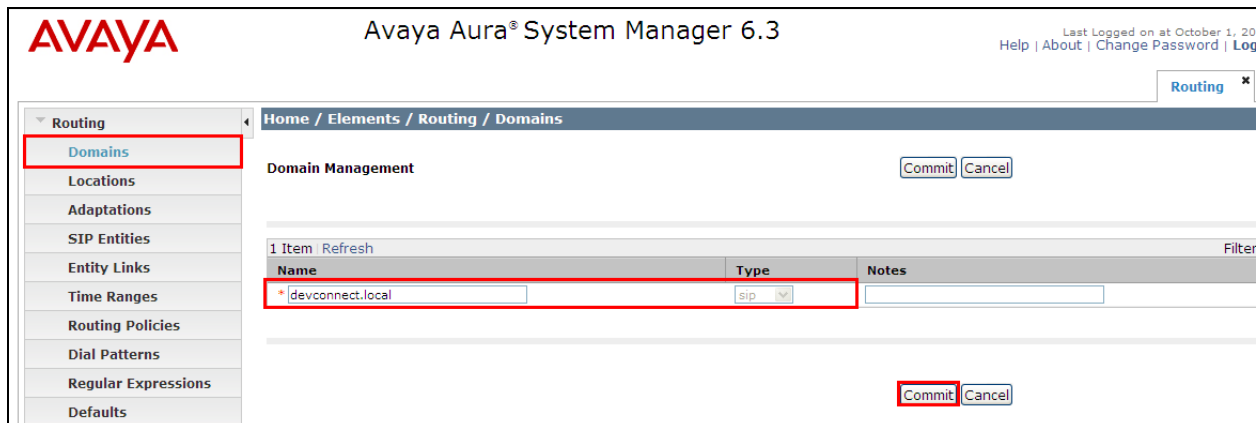
Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.

6.2 Administer SIP Domain

Click on **Routing** → **Domains** in the left window. If there is not a domain already configured click on **New** highlighted below.



Note the domain **Name** used in the compliance testing was **devconnect.local**. Note this domain is also referenced on the CS1000E Signalling Server the setup of which is outside the scope of these Application Notes. For more information on the Signalling Server setup please refer to **Section 10** document *Element Manager System Reference –Administration Avaya Communication Server 1000*. Once the domain name is entered click on **Commit** to save this.



6.3 Administer Location

Session Manager uses the origination location to determine which dial patterns to look at when routing a call. In this example, one Location has been created which will reference both the Session Manager location and the OpenGate location. Navigate to **Home → Elements → Routing → Locations → New** enter an identifying **Name**, as shown below.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with 'Locations' highlighted. The main content area is titled 'Location Details' and includes a 'General' tab. A red box highlights the 'Name' field, which contains the text 'DevConnectPG63'. Other fields visible include 'Notes', 'Dial Plan Transparency in Survivable Mode' (Enabled: ☐) 'Listed Directory Number', and 'Associated CM SIP Entity'.

At the bottom of the same page the **Location Pattern** is defined. Click **Add** and enter the IP address range used to logically identify the location. In this case the **IP Address Pattern** is **10.10.40.*** as shown below. Click **Commit** when done.

The screenshot shows the 'Location Pattern' configuration page. At the top, there are 'Alarm Threshold' settings for Overall and Multimedia, both set to 80%, and latency settings for both set to 5 minutes. Below this, the 'Location Pattern' section has an 'Add' button highlighted with a red box. A table lists the patterns, with the first entry '10.10.40.*' highlighted by a red box. The table has columns for a checkbox, the pattern, and notes. At the bottom right, the 'Commit' button is highlighted with a red box.

6.4 Administer SIP Entities

Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for Session Manager SIP Signalling Interface, CS1000E and OpenGate Solution respectively.

6.4.1 Configure Session Manager SIP Signalling Interface Entity

Click **Home** → **Elements** → **Routing** → **SIP Entities** → **New** assign an identifying **Name**, the **FQDN or IP Address** for Session Manager Security Module Interface, set the **Type** to **Session Manager** and the **Location** to the Location configured in **Section 6.3** and scroll down to configure the ports..

Avaya Aura® System Manager 6.3

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: SM63vmppg

FQDN or IP Address: 10.10.40.34

Type: Session Manager

Notes:

Location: DevConnectPG63

Outbound Proxy:

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

Select the box next to the entity that was just created and click **Edit** (not shown). Scroll down the page until the **Port** section is displayed, click **Add** and configure the **Port** as **5060** the **Protocol** **TCP** and the **Default Domain** as the domain configured in **Section 6.2**. Repeat this for the **UDP** connection which will be established to the OpenGate server, as shown below TLS is shown below but was not used in the connection to the OpenGate server. Click **Commit** when done.

Port

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Refresh

Port	Protocol	Default Domain	Notes
5060	TCP	devconnect.local	
5060	UDP	devconnect.local	
5061	TLS	devconnect.local	

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Refresh

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

Commit Cancel

6.4.2 Configure Avaya Communication Server 1000E SIP Entity

Click **Home** → **Elements** → **Routing** → **SIP Entities** → **New** assign an identifying **Name**, the **FQDN or IP Address** for the CS1000E Node IP Address which can be obtained from the Signalling Server, set the **Type** to **SIP Trunk** and the **Location** to the Location configured in **Section 6.3** and click on **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing' expanded, and 'SIP Entities' is selected. The main area is titled 'SIP Entity Details' with a 'General' tab. The 'Name' field is set to 'CS1KPG1'. The 'FQDN or IP Address' field is set to '10.10.40.111'. The 'Type' dropdown is set to 'SIP Trunk'. The 'Location' dropdown is set to 'DevConnectPG63'. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' is set to '4'. The 'Call Detail Recording' dropdown is set to 'none'. The 'Commit' button is highlighted with a red box.

6.4.3 Configure Presence Technology OpenGate Entity

Click **Home** → **Elements** → **Routing** → **SIP Entities** → **New** assign an identifying **Name**, the **FQDN or IP Address** for the OpenGate server, set the **Type** to **SIP Trunk**, leave all other settings default and click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing' expanded, and 'SIP Entities' is selected. The main area is titled 'SIP Entity Details' with a 'General' tab. The 'Name' field is set to 'Presence'. The 'FQDN or IP Address' field is set to '10.10.40.84'. The 'Type' dropdown is set to 'SIP Trunk'. The 'Location' dropdown is set to 'DevConnectPG63'. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'SIP Timer B/F (in seconds)' is set to '4'. The 'Call Detail Recording' dropdown is set to 'egress'. The 'Commit' button is highlighted with a red box.

6.5 Administer SIP Entity Link

A SIP Trunk between a Session Manager and a telephony system is described by an Entity Link. An entity link needs to be created between Session Manager and both the CS1000E and OpenGate.

6.5.1 Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Communication Server 1000E

Click on **Home** → **Elements** → **Routing** → **Entity Links** → **New** assign an identifying **Name** choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TCP**, enter **5060** for the **Port**, choose the CS1000E entity as **SIP Entity 2** and set the **Port** to **5060**, place an arrow in the **Trusted** box. Click **Commit** when done.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a red box around 'Entity Links' under the 'Routing' section. The main content area shows the 'Entity Links' configuration page with a breadcrumb trail 'Home / Elements / Routing / Entity Links'. A table lists one item with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
*SM63vmpg_CS1KPG	*SM63vmpg	TCP	*5060	*CS1KPG1	<input type="checkbox"/>	*5060	trusted

At the bottom right, there are 'Commit' and 'Cancel' buttons, with 'Commit' highlighted by a red box.

6.5.2 Administer SIP Entity Link from Avaya Aura® Session Manager to OpenGate

Click on **Home** → **Elements** → **Routing** → **Entity Links** → **New** assign an identifying **Name** choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **UDP**, enter **5060** for the **Port**, choose the OpenGate entity as **SIP Entity 2** and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop-down list. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to OpenGate.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a red box around 'Entity Links' under the 'Routing' section. The main content area shows the 'Entity Links' configuration page with a breadcrumb trail 'Home / Elements / Routing / Entity Links'. A table lists one item with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*Presence_UDP	*SM63vmpg	UDP	*5060	*Presence	*5060	trusted	<input type="checkbox"/>	

At the bottom right, there are 'Commit' and 'Cancel' buttons, with 'Commit' highlighted by a red box.

6.6 Administer Routing Policies

To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to an attached system. Two routing policies must be created, one for the Communications Manager and the second for OpenGate. These will be associated with the Dial Patterns created in **Section 6.7**.

6.6.1 Create Routing Policy to Avaya Communication Server 1000E

Click **Home** → **Elements** → **Routing** → **Routing Policies** → **New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the CS1000E SIP Entity and click **Select** (not shown). Click **Commit** when done.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing Policies' highlighted. The main area is titled 'Routing Policy Details' and has a 'Commit' button. The 'General' section contains a 'Name' field with 'ToCS1KPG1', a 'Disabled' checkbox, a 'Retries' field with '0', and a 'Notes' field. The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with the following data:

Name	FQDN or IP Address	Type	Notes
CS1KPG1	10.10.40.111	SIP Trunk	

6.6.2 Create Routing Policy to Presence Technology OpenGate

Click **Home** → **Elements** → **Routing** → **Routing Policies** → **New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the OpenGate SIP Entity and click **Select** (not shown). Click **Commit** when done.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing Policies' highlighted. The main area is titled 'Routing Policy Details' and has a 'Commit' button. The 'General' section contains a 'Name' field with 'ToPresence', a 'Disabled' checkbox, a 'Retries' field with '0', and a 'Notes' field. The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with the following data:

Name	FQDN or IP Address	Type	Notes
Presence	10.10.40.84	SIP Trunk	

6.7 Administer Dial Patterns

As one of its main functions, 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 dialled to the appropriate system.

6.7.1 Create Dial Pattern to Avaya Communication Server 1000E

A dial pattern must be created on Session Manager to route incoming calls from OpenGate to CS1000E Extensions 2xxx. To create a Dial Pattern to route 2xxx from Session Manager to the CS1000E, click **Home** → **Elements** → **Routing** → **Dial Patterns** → **New**. Under **Pattern** enter the numbers presented to Session Manager by OpenGate destined for the CS1000E, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that which was created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**. This brings up a new window (not shown) in this **window** under the **Origination Section**, click **All**, in the **Routing Policies** section click the routing policy created for the CS1000E. Click **Select** when done (not shown). Click **Commit** once finished.

The screenshot shows the Session Manager web interface for creating a Dial Pattern. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns** (highlighted), Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / Dial Patterns. Below the breadcrumb is the 'Dial Pattern Details' section with 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- * Pattern: 2
- * Min: 4
- * Max: 4
- Emergency Call: ☐
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: devconnect.local (dropdown menu)
- Notes:

 Below the 'General' section is the 'Originating Locations and Routing Policies' section, which includes 'Add' and 'Remove' buttons and a '1 Item Refresh' link. A table lists the existing configuration:

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	DevConnectPG63		ToCM63VMFG	0	<input type="checkbox"/>	CM63VMFG

6.7.2 Create Dial Pattern to OpenGate

In **Section 5.2** the CS1000E is configured to route the dialled numbers beginning **43xxxx** to Session Manager. To create a Dial Pattern to route **43xxxx** from Session Manager to OpenGate click **Home → Elements → Routing → Dial Patterns → New**. Under **Pattern** enter the numbers presented to Session Manager by CS1000E destined for OpenGate, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**. This brings up a new window (not shown) in this window under the **Origination Location** section click **All**, in the **Routing Policies** section click the routing policy created for OpenGate. Click **Select** when done (not shown). Click **Commit** when complete.

Routing / Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel

General

* Pattern: 43

* Min: 6

* Max: 6

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: devconnect.local

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	DevConnectPG63		ToPresence	0	<input type="checkbox"/>	Presence

Select : All, None

7. Configure the Presence Technology OpenGate

OpenGate is part of Presence Suite and is administered via Presence Administrator which resides on the Presence Server. A number of items are set up within Presence Administrator to configure the OpenGate ACD. This section will cover the following areas:

- Login to Presence Administrator
- Administer SIP trunk to Avaya Aura® Session Manager
- OpenGate Skill Configuration
- OpenGate Agent Login Configuration
- OpenGate Station Configuration
- OpenGate Service Configuration
- Outbound Routes
- Inbound Routes
- Logging in to OpenGate

Note: The following configuration details for Agent Login and Skillsets are all a part of the Presence OpenGate internal Call Centre and are not referenced anywhere else in these Application Notes.

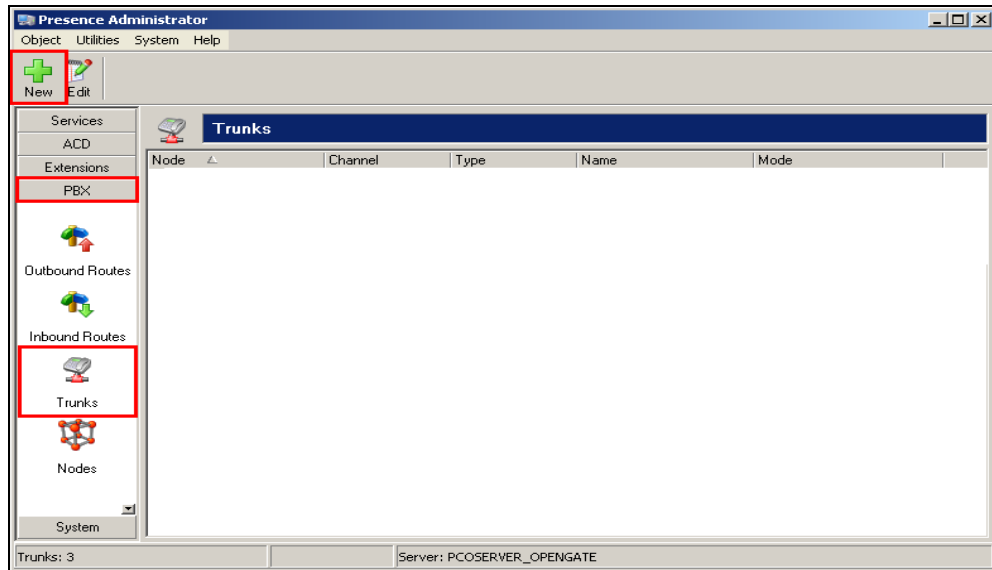
7.1 Login to Presence Administrator

Launch the Presence Administrator application by double clicking the **pcoadmin.exe** icon located in the Presence folder (not shown). The username and password that appear in the **User** and **Password** fields are created during the Presence Server installation.



7.2 Administer SIP Trunk to Avaya Aura® Session Manager

In the left window navigate to **PBX→Trunks**. Click on the **New** icon at the top left of the page.



Fill in the information as shown below. Please note that the **Node ogmaster** has already been established during the install of Presence OpenGate. Select **SIP Peer** as the **Channel** and **Advanced** as the **Mode**. Enter a suitable name for the **User**. Note the following entries shown in the main window. Click on OK once finished.

- **Fromdomain** = the domain that is referenced in **Sections 6.2**
- **Host** = IP address of Session Manager

The 'New trunk' dialog box contains the following configuration fields and text:

- Node:** ogmaster (dropdown menu)
- Channel:** SIP Peer (dropdown menu)
- Mode:** Advanced (dropdown menu)
- User:** avaya2013 (text field)

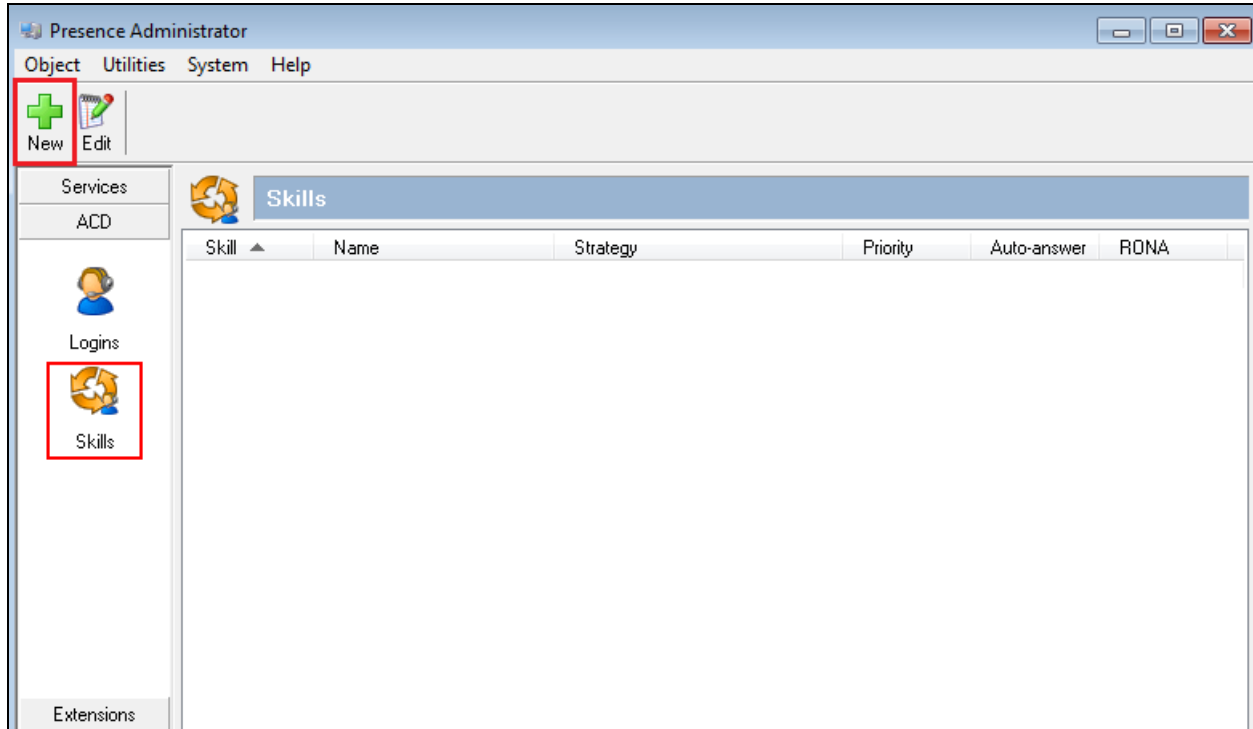
Below the fields, the following text is displayed in a monospaced font:

```
type=peer
fromdomain=devconnect.local
host=10.10.40.34
disallow=all
allow=all
dtmfmode=rfc2833
```

At the bottom of the dialog are three buttons: **OK**, **Cancel**, and **Apply**.

7.3 OpenGate Skill Configuration

To configure a skill, from the left hand side select **ACD** → **Skills** from the Presence Administrator main menu. Click the **New** button.



In the resulting screen define a **Skill** number and enter a **Name** to identify the skill. In the **Strategy** field use the two drop down menus to define the selection strategy that will be used by the skill. Set a **Priority** for the skill. All remaining fields can be left with default values. Click **OK** to save the configuration.

Add skill

☒ General
☐ Logins

☒ **General**

Skill: 3330

Name: 3330

Strategy: Skill Level measurement Agent Available the Longest

Priority: 10

RONA: 0 seconds

☐ Answer calls automatically (auto-answer)

OK Cancel Apply

7.4 OpenGate Agent Login Configuration

The login configured here will be used by the agent to login to OpenGate. The Agents will connect to OpenGate via the Presence Suite Agent application. To configure an ACD agent login, from the left hand side select **ACD** → **Logins** from the Presence Administrator main menu. Click the **Add** button.

Presence Administrator

Object Logins Utilities System Help

Group Login Edit **Add** Remove

Services

ACD

Logins

Groups	Name	Softphone

Group: [All] Logins: 2 Server: PRESENCE_SERVER

From the menu on the left side of the screen select **General**, enter a numerical ID in the **Logins** field. Define a **Password** for the agent login and repeat in the **Confirm Password** field.

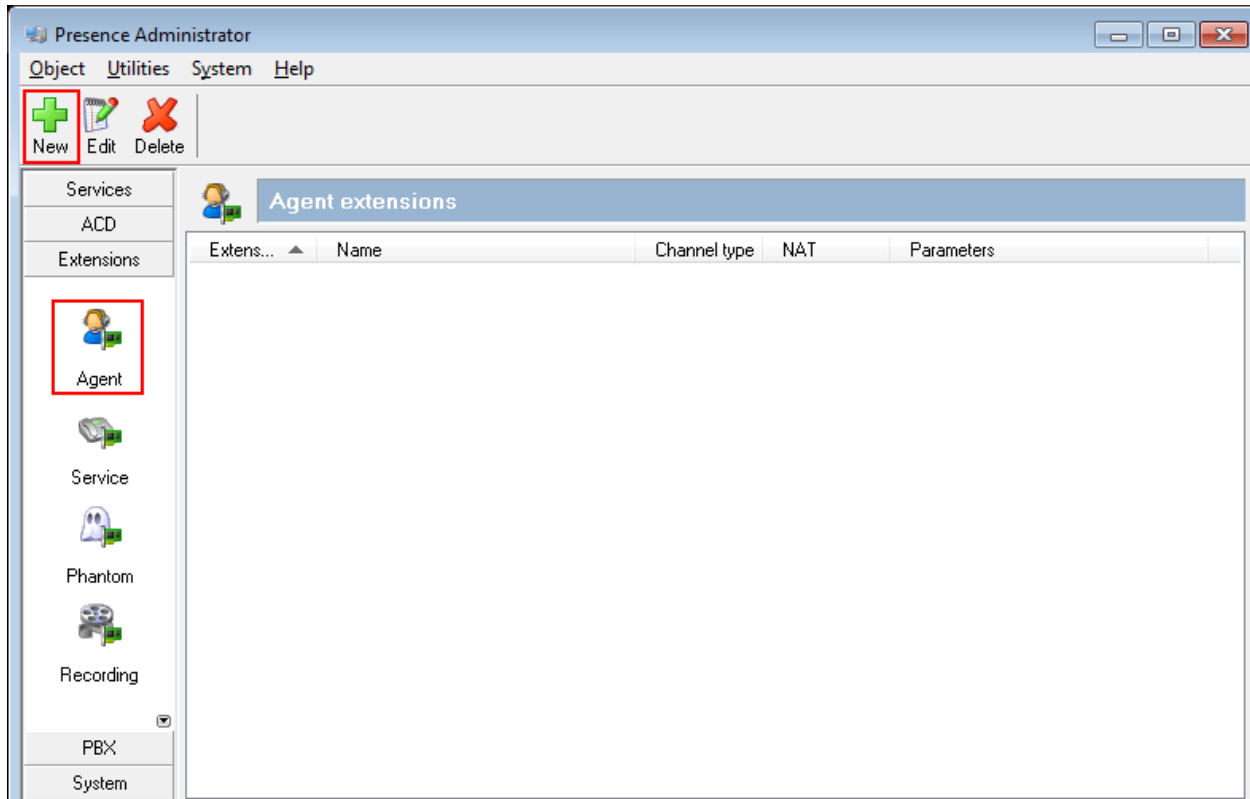
The screenshot shows the 'Insert logins' dialog box with the 'General' tab selected. The left sidebar has 'General' highlighted. The main area has a 'General' header. Below it, the 'Logins' field contains '4400'. The 'Password' and 'Confirm password' fields are masked with 'xxxx'. There are several checkboxes: 'Change password at next login' (unchecked), 'Agent cannot change password' (checked), 'Password never expires' (checked), 'Store outgoing calls of agent' (unchecked), and 'Answer calls automatically (auto-answer)' (unchecked). The 'OK' and 'Cancel' buttons are at the bottom right.

From the menu on the left side of the screen select **Skills**, use the drop down menu to select the **Skill** configured in **Section 7.3** and specify a **Level** for the skill to be applied against this agent login. Click the **Add** button and the skill should appear under **Assigned skills** (not shown here). Click **OK** to save the login configuration.

The screenshot shows the 'Insert logins' dialog box with the 'Skills' tab selected. The left sidebar has 'Skills' highlighted. The main area has a 'Skills' header. Below it, the 'Skill' dropdown menu shows '3330 - 3330'. The 'Level' field is empty. The 'Add' button is highlighted. Below the 'Add' button is a table titled 'Assigned skills' with columns 'Name' and 'Level'. The 'Remove' button is to the right of the table. The 'OK' and 'Cancel' buttons are at the bottom right.

7.5 Presence Technology OpenGate Station Configuration

Each telephone/endpoint that OpenGate could route calls to must be defined within Presence Administrator as an Agent extension. To define an Agent extension from the left hand side navigate to **Extensions** → **Agents** and click the **New** button.



In the resulting screen specify an **Extension** number that will be used by the Presence Agent application (**Section 7.8.1**). Note this any existing extension number on the CS1000E. Set a **Name** that the Agent extension will be known as. The password is not required in this case. In the **Channel** field use the drop down arrow to select **SIP**. In the following field define the number that will be dialled and the route used to reach the station, which should be expressed in the form of a URI. The user part is set to the number to be dialled and the host part is set to the name of the sip trunk defined **Section 7.2**. In this example **\${EXTEN}@avaya2013** is configured which means any number that is dialled will use trunk “avaya2013”, note **avaya 2013** is the SIP Trunk configured in **Section 7.2** above, so the URI is formatted as **\${EXTEN}@avaya2013**. Click **OK** to save.

Add agent extensions

Extension: 2000

Name: 2000

Password: ☐ Use extension as password

Channel: SIP

NAT: never

Network regions

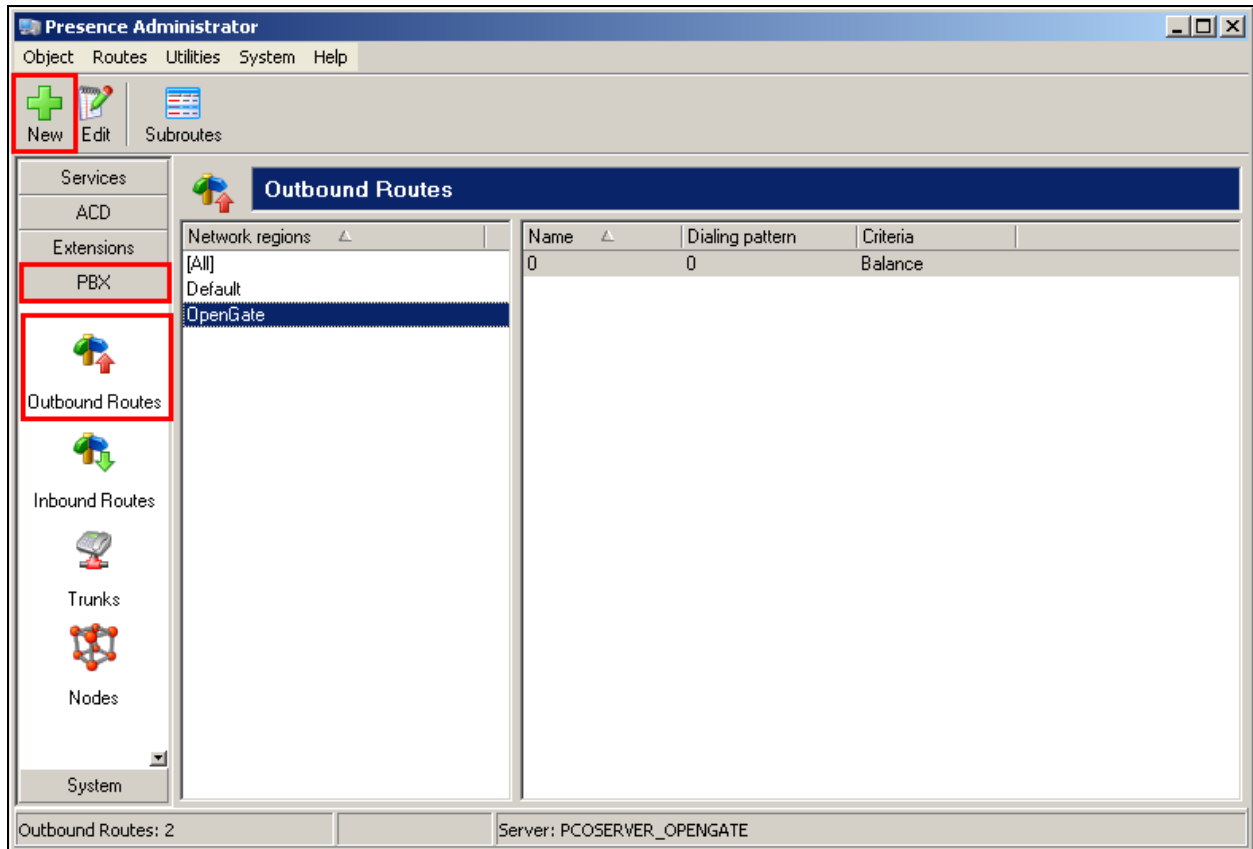
Add

Region
Default
OpenGate

Remove

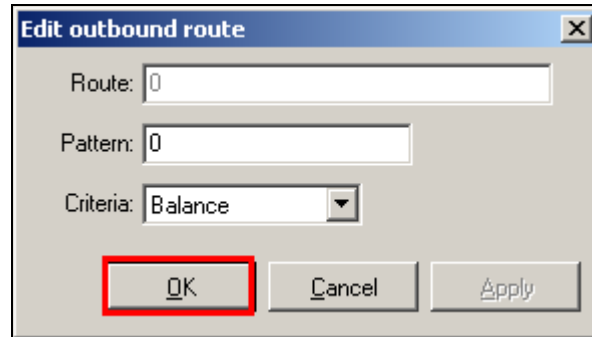
7.6 Outbound Routes

To define an outbound route, from the left hand side navigate to **PBX → Outbound Routes** and click the **New** button.



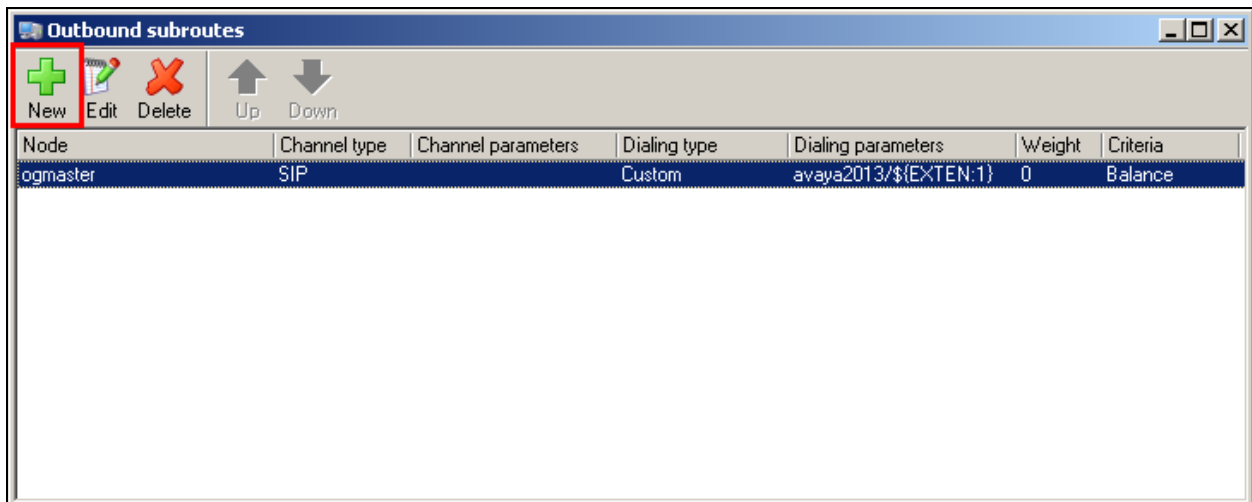
In the resulting screen enter a descriptive name in the **Route** field and in the **Pattern** field define any prefix required by outbound calls. This setup is only used for internal working of OpenGate and is not related to routing on the CS1000E. For **Criteria** use the drop-down menu to select the method that will be used to distribute calls among the subroutes configured in the next step.

Balance allows an even distribution of calls across the subroutes. Click **OK** to save the **outbound route**. Click **OK** to save.



The 'Edit outbound route' dialog box contains three input fields: 'Route' with the value '0', 'Pattern' with the value '0', and 'Criteria' with a dropdown menu set to 'Balance'. At the bottom, there are three buttons: 'OK' (highlighted with a red rectangle), 'Cancel', and 'Apply'.

To add an outbound subroute, from the outbound routes main page shown above, highlight the outbound route that was added in the previous step and click the subroutes button at the top of the screen (not shown). The **Outbound subroutes** window is then displayed as shown below, Click **New**.



The 'Outbound subroutes' window features a toolbar with icons for 'New' (a green plus sign, highlighted with a red rectangle), 'Edit' (a pencil), 'Delete' (a red X), 'Up' (an upward arrow), and 'Down' (a downward arrow). Below the toolbar is a table with the following data:

Node	Channel type	Channel parameters	Dialing type	Dialing parameters	Weight	Criteria
logmaster	SIP		Custom	avaya2013/\${EXTEN:1}	0	Balance

In the resulting window select the relevant **Node** (this was created during the OpenGate install), and under **Channel** select **SIP**. For **Dialing string** use the drop down menu to select **Custom** and in the secondary field enter a matching pattern using a regular expression. In the example below the expression used is `${EXTEN:1}@avaya2013`. The expression performs the following:

- **EXTEN** is an internal variable which represents the called number, therefore this pattern will match any called number beginning with a 0(2000)
- Remove the leading character (leaving 2000)
- Route it via the **avaya2013** trunk defined in **Section 7.2**.

This is done in order to use the same numbers that may be used on the Avaya PBX. Using 0 to make outgoing calls and then stripping the 0 before the call reaches the Session Manager and the CS1000E. Click **OK** to save.

Add outbound subroute

Node: ogmaster

Channel: SIP

Dialing string: Custom avaya2013/\${EXTEN:1}

Weight: 0

Billing code:

Outgoing calls identification

☐ Enable outgoing calls identification

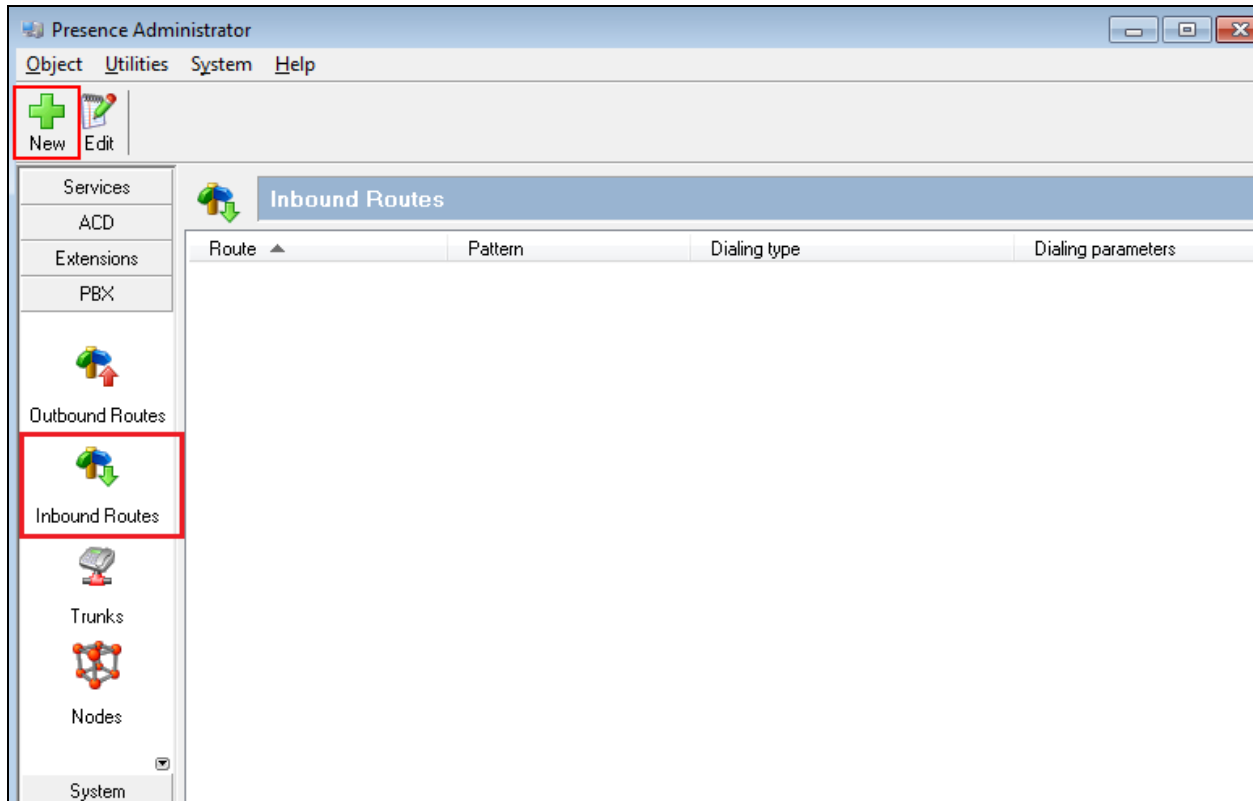
Phone no:

Description:

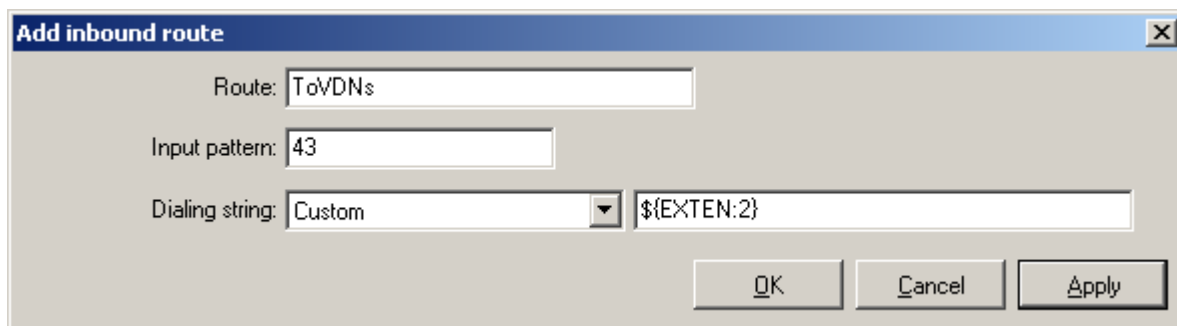
OK Cancel Apply

7.7 Inbound Routes

Inbound routes are used to map dialed numbers received to internal extensions within OpenGate. To define an inbound route, from the left hand side navigate to **PBX → Inbound Routes** and click the **New** button.



In the resulting window enter a descriptive name for **Route**. In the **Input pattern** field enter a numerical pattern that the inbound route will use to match incoming digits. Use the drop down menu in the **Dialing string** field to specify the digit manipulation to be performed. In the example below, incoming digits **43** will be replaced with **\${EXTEN:2}**. This will remove two digits from the incoming call (i.e., the 43) from the incoming call leaving 3300, which is the internal Service Extension used within OpenGate.



7.8 Logging into OpenGate

In order to receive calls from Open Gate, users must log in to the system via the Presence Agent application. This section describes the steps required to connect to OpenGate as an agent to receive ACD calls.

7.8.1 Presence Agent Configuration

The following steps are carried out on the Presence Agent PC. Prior to installing the Presence agent, ensure that the DBExpress driver (dpexpoda.dll) is located in the C:\Windows\System32 directory, if not contact Presence Technology support outlined in **Section 2.3** of these Application Notes. The DBExpress driver allows the agent application to communicate with the Presence Suite/OpenGate database.

Launch the **Presence Agent Configuration** application by double clicking the **pcoagentcfg.exe** located in the C: \Presence folder (not shown). Enter the **Presence Server IP address** as **10.10.40.83**. The **Presence Server port** can be left as the default value of **6100**. Enter the extension of the station that will be used with this workstation in the **Agent station** field. Check the **Hang up calls before logging in** check box. In the field **Use configuration for** choose **Machine** from the drop down menu. Click **OK**. This step is needed for each agent configured; only the agent station field will vary.

The screenshot shows the 'Presence Agent Configuration' dialog box with the 'General' tab selected. The 'General' tab is highlighted in the left sidebar and the main content area. The 'Presence Server' section contains 'IP address: 10.10.40.83' and 'Port: 6100'. The 'Station configuration' section contains 'Agent station: 2000', a checked 'Hang up calls before logging in' checkbox, and an unchecked 'Ask agent station at login window' checkbox. The 'Use configuration for:' dropdown menu is set to 'Machine'. The 'OK' button is highlighted with a red box.

Field	Value
IP address	10.10.40.83
Port	6100
Agent station	2000
Hang up calls before logging in	<input checked="" type="checkbox"/>
Ask agent station at login window	<input type="checkbox"/>
Use configuration for	Machine

7.8.2 Logging in Presence Agent

Launch the Presence agent configuration application by double clicking the pcoagent.exe located in the Presence folder. Enter the agent **Login** and **Password** configured in **Section 7.4** and click on **OK**.



A task bar is present at the top of the Agent PC. Click on the green arrow to put the agent into an available state.



The information status on the task bar goes to **Available** indicating the agent is ready to receive calls.



8. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager Home Tab click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **Up**.

Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

Session Counts

System Tools

Performance

All Entity Links for Session Manager: SM63vmpg

Status Details for the selected Session Manager:

Summary View

8 Items | Refresh

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ASCOMDECT1	10.10.40.181	5060	TCP	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	Presence	10.10.40.84	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CM62	192.168.50.13	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	CS1KPG1	10.10.40.111	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1KPG2	192.168.50.99	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	AAMessaging	192.168.50.60	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	NRS76	10.10.40.101	5060	TCP	FALSE	UP	200 OK	UP

2. Manually verify that calls can be placed to OpenGate and routed to Agents.

9. Conclusion

These Application Notes describe the configuration steps required for Presence Technology OpenGate R10.0 to successfully interoperate with Avaya Communication Server 1000E R7.6 and Avaya Aura® Session Manager R6.3. All functionality and serviceability test cases were completed successfully.

10. Additional References

This section references the Avaya and Presence Suite product documentation that are relevant to these Application Notes.

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

- [1] *Software Input Reference Administration Avaya Communication Server 1000*, Release 7.6; Document No. NN43001-611_05.02
- [2] *Administering Avaya Aura® Session Manager*
- [3] *Element Manager System Reference –Administration Avaya Communication Server 1000* Release 6.3, Release 7.6 NN43001-632, 05.04

The following documentation is available on request from Presence Technology OpenGate:

www.presenceco.com

- [1] *ACD Sys Presence Administrator Manual Presence Suite*, V10.0
- [2] *Presence Installation Guides Presence Software*, V10.0
- [3] *PBX/ACD Requirements Presence Software*, V10.0

Appendix A

Avaya Communication Server 1000E R7.6 - Linux Patches

Product Release: 7.65.16.00

In system patches: 0

In System service updates: 26

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
2	Yes	27/08/13	NO	YES	cs1000-dmWeb-7.65.16.21-01.i386.000
3	Yes	28/08/13	NO	yes	cs1000-snmp-7.65.16.00-01.i386.000
4	Yes	28/08/13	NO	YES	cs1000-nrsm-7.65.16.00-03.i386.000
5	Yes	28/08/13	NO	YES	cs1000-oam-logging-7.65.16.01-01.i386.000
6	Yes	28/08/13	NO	yes	cs1000-cs1000WebService 6-0-7.65.16.21-00.i386.000
7	Yes	28/08/13	NO	YES	cs1000-sps-7.65.16.21-01.i386.000
8	Yes	28/08/13	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
9	Yes	28/08/13	NO	YES	cs1000-shared-carrdtct-7.65.16.21-01.i386.000
10	Yes	28/08/13	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
11	Yes	28/08/13	NO	YES	cs1000-emWebLocal 6-0-7.65.16.21-01.i386.000
12	Yes	28/08/13	NO	yes	cs1000-dbcom-7.65.16.21-00.i386.000
13	Yes	28/08/13	NO	YES	cs1000-csmWeb-7.65.16.21-05.i386.000
14	Yes	28/08/13	NO	YES	cs1000-shared-xmsg-7.65.16.21-00.i386.000
15	Yes	28/08/13	NO	YES	cs1000-vtrk-7.65.16.21-29.i386.000
16	Yes	28/08/13	NO	YES	cs1000-tps-7.65.16.21-05.i386.000
17	Yes	28/08/13	NO	YES	cs1000-mscAnnc-7.65.16.21-02.i386.001
18	Yes	28/08/13	NO	YES	cs1000-mscAttn-7.65.16.21-04.i386.001
19	Yes	28/08/13	NO	YES	cs1000-mscConf-7.65.16.21-02.i386.001
20	Yes	28/08/13	NO	YES	cs1000-mscMusc-7.65.16.21-02.i386.001
21	Yes	28/08/13	NO	YES	cs1000-mscTone-7.65.16.21-03.i386.001
22	Yes	28/08/13	NO	YES	cs1000-bcc-7.65.16.21-21.i386.000
23	Yes	28/08/13	NO	YES	cs1000-Jboss-Quantum-7.65.16.21-3.i386.000
24	Yes	28/08/13	NO	YES	cs1000-emWeb 6-0-7.65.16.21-06.i386.000
25	Yes	10/12/13	NO	yes	cs1000-cs-7.65.P.100-01.i386.001
26	Yes	10/12/13	YES	yes	cs1000-linuxbase-7.65.16.21-08.i386.000
27	Yes	10/12/13	NO	YES	cs1000-patchWeb-7.65.16.21-06.i386.0

Avaya Communication Server 1000E R7.6 - Call Server Patches

VERSION 4121
RELEASE 7
ISSUE 65 P +
DepList 1: core Issue: 01 (created: 2013-06-14 03:54:33 (est))

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi01052968	ISS1:1OF1	p32540_1	11/12/2013	p32540_1.cpl	NO
001	wi01045058	ISS1:1OF1	p32214_1	11/12/2013	p32214_1.cpl	NO
002	wi01085855	ISS1:1OF1	p32658_1	11/12/2013	p32658_1.cpl	NO
003	wi01053314	ISS1:1OF1	p32555_1	11/12/2013	p32555_1.cpl	NO
004	wi01060382	iss1:1of1	p32623_1	11/12/2013	p32623_1.cpl	YES
005	wi01070580	ISS1:1OF1	p32380_1	11/12/2013	p32380_1.cpl	NO
006	wi01067822	ISS1:1OF1	p32466_1	11/12/2013	p32466_1.cpl	YES
007	wi01061481	ISS1:1OF1	p32382_1	11/12/2013	p32382_1.cpl	NO
008	wi01072032	ISS1:1OF1	p32448_1	11/12/2013	p32448_1.cpl	NO
009	wi01022599	ISS1:1OF1	p32080_1	11/12/2013	p32080_1.cpl	NO
010	wi01035976	ISS1:1OF1	p32173_1	11/12/2013	p32173_1.cpl	NO
011	wi01065922	ISS1:1OF1	p32516_1	11/12/2013	p32516_1.cpl	NO
012	wi01055480	ISS1:1OF1	p32712_1	11/12/2013	p32712_1.cpl	NO
013	wi01041453	ISS1:1OF1	p32587_1	11/12/2013	p32587_1.cpl	NO
014	wi01078723	ISS1:1OF1	p32532_1	11/12/2013	p32532_1.cpl	NO
015	WI0110261	ISS1:1OF1	p32758_1	11/12/2013	p32758_1.cpl	NO
016	wi01064599	iss1:1of1	p32580_1	11/12/2013	p32580_1.cpl	NO
017	wi01048457	ISS1:1OF1	p32581_1	11/12/2013	p32581_1.cpl	NO
018	wi01072027	ISS1:1OF1	p32689_1	11/12/2013	p32689_1.cpl	NO
019	wi01059388	iss1:1of1	p32628_1	11/12/2013	p32628_1.cpl	NO
020	wi01074003	ISS1:1OF1	p32421_1	11/12/2013	p32421_1.cpl	NO
021	wi00933195	ISS1:1OF1	p32491_1	11/12/2013	p32491_1.cpl	NO
022	wi00996734	ISS1:1OF1	p32550_1	11/12/2013	p32550_1.cpl	NO
023	wi01065118	ISS1:1OF1	p32397_1	11/12/2013	p32397_1.cpl	NO
024	wi01063864	ISS1:1OF1	p32410_1	11/12/2013	p32410_1.cpl	YES
025	wi01072023	ISS1:1OF1	p32130_1	11/12/2013	p32130_1.cpl	YES
026	wi01075359	ISS1:1OF1	p32671_1	11/12/2013	p32671_1.cpl	NO
027	wi01080753	ISS1:1OF1	p32518_1	11/12/2013	p32518_1.cpl	NO
028	wi01070473	ISS1:1OF1	p32413_1	11/12/2013	p32413_1.cpl	NO
029	wi01075355	ISS1:1OF1	p32594_1	11/12/2013	p32594_1.cpl	NO
030	wi01071379	ISS1:1OF1	p32522_1	11/12/2013	p32522_1.cpl	NO
031	wi01070756	ISS1:1OF1	p32444_1	11/12/2013	p32444_1.cpl	NO
032	wi01075353	ISS1:1OF1	p32613_1	11/12/2013	p32613_1.cpl	NO
033	wi01062607	ISS1:1OF1	p32503_1	11/12/2013	p32503_1.cpl	NO
034	wi01068851	ISS1:1OF1	p32439_1	11/12/2013	p32439_1.cpl	NO
035	wi01075352	ISS1:1OF1	p32603_1	11/12/2013	p32603_1.cpl	NO
036	wi01092300	ISS1:1OF1	p32692_1	11/12/2013	p32692_1.cpl	NO
037	wi01063263	ISS1:1OF1	p32573_1	11/12/2013	p32573_1.cpl	NO
038	wi01087528	ISS1:1OF1	p32700_1	11/12/2013	p32700_1.cpl	NO
039	wi01055300	ISS1:1OF1	p32543_1	11/12/2013	p32543_1.cpl	NO
040	wi01039280	ISS1:1OF1	p32423_1	11/12/2013	p32423_1.cpl	NO
041	wi01068669	ISS1:1OF1	p32333_1	11/12/2013	p32333_1.cpl	NO
042	wi01069441	ISS1:1OF1	p32097_1	11/12/2013	p32097_1.cpl	NO
043	wi01058621	ISS1:1OF1	p32339_1	11/12/2013	p32339_1.cpl	NO
044	wi01032756	ISS1:1OF1	p32673_1	11/12/2013	p32673_1.cpl	NO
045	wi01070465	iss1:1of1	p32562_1	11/12/2013	p32562_1.cpl	NO
046	wi01053920	ISS1:1OF1	p32303_1	11/12/2013	p32303_1.cpl	NO
047	wi00897254	ISS1:1OF1	p31127_1	11/12/2013	p31127_1.cpl	NO
048	wi01057403	ISS1:1OF1	p32591_1	11/12/2013	p32591_1.cpl	NO
049	wi01066991	ISS1:1OF1	p32449_1	11/12/2013	p32449_1.cpl	NO
050	wi01094305	ISS1:1OF1	p32640_1	11/12/2013	p32640_1.cpl	NO
051	wi01058359	ISS1:1OF1	p32331_1	11/12/2013	p32331_1.cpl	NO
052	wi01047890	ISS1:1OF1	p32697_1	11/12/2013	p32697_1.cpl	NO

053	wi01060241	ISS1:1OF1	p32381_1	11/12/2013	p32381_1.cpl	NO
054	wi01034307	ISS1:1OF1	p32615_1	11/12/2013	p32615_1.cpl	NO
055	wi01052428	ISS1:1OF1	p32606_1	11/12/2013	p32606_1.cpl	NO
056	wi00884716	ISS1:1OF1	p32517_1	11/12/2013	p32517_1.cpl	NO
057	wi01070468	iss1:1of1	p32418_1	11/12/2013	p32418_1.cpl	NO
058	wi01091447	ISS1:1OF1	p32675_1	11/12/2013	p32675_1.cpl	NO
059	wi01068042	ISS1:1OF1	p32669_1	11/12/2013	p32669_1.cpl	NO
060	wi01061483	ISS1:1OF1	p32359_1	11/12/2013	p32359_1.cpl	NO
061	wi01065125	ISS1:1OF1	p32416_1	11/12/2013	p32416_1.cpl	NO
062	wi01056633	ISS1:1OF1	p32322_1	11/12/2013	p32322_1.cpl	NO
063	wi01070474	iss1:1of1	p32407_1	11/12/2013	p32407_1.cpl	NO
064	wi01053597	ISS1:1OF1	p32304_1	11/12/2013	p32304_1.cpl	NO
065	wi01070471	ISS1:1OF1	p32415_1	11/12/2013	p32415_1.cpl	NO
066	wi01025156	ISS1:1OF1	p32136_1	11/12/2013	p32136_1.cpl	NO
067	wi01088775	ISS1:1OF1	p32659_1	11/12/2013	p32659_1.cpl	NO
068	wi01083584	ISS1:1OF1	p32619_1	11/12/2013	p32619_1.cpl	NO
069	wi01075360	iss1:1of1	p32602_1	11/12/2013	p32602_1.cpl	NO
070	wi01053195	ISS1:1OF1	p32297_1	11/12/2013	p32297_1.cpl	NO
071	wi01043367	ISS1:1OF1	p32232_1	11/12/2013	p32232_1.cpl	NO
072	wi01082456	ISS1:1OF1	p32596_1	11/12/2013	p32596_1.cpl	NO
073	wi01089519	ISS1:1OF1	p32665_1	11/12/2013	p32665_1.cpl	NO
074	wi01065842	ISS1:1OF1	p32478_1	11/12/2013	p32478_1.cpl	NO
075	wi01088585	ISS1:1OF1	p32656_1	11/12/2013	p32656_1.cpl	NO
076	wi01035980	ISS1:1OF1	p32558_1	11/12/2013	p32558_1.cpl	NO
077	wi01087543	ISS1:1OF1	p32662_1	11/12/2013	p32662_1.cpl	NO
078	wi01060826	ISS1:1OF1	p32379_1	11/12/2013	p32379_1.cpl	NO
079	wi01061484	ISS1:1OF1	p32576_1	11/12/2013	p32576_1.cpl	NO
080	wi01034961	ISS1:1OF1	p32144_1	11/12/2013	p32144_1.cpl	NO
081	wi01056067	ISS1:1OF1	p32457_1	11/12/2013	p32457_1.cpl	NO
082	WI01077073	ISS1:1OF1	p32534_1	11/12/2013	p32534_1.cpl	NO
083	wi01073100	ISS1:1OF1	p32599_1	11/12/2013	p32599_1.cpl	NO
084	wi01060341	ISS1:1OF1	p32578_1	11/12/2013	p32578_1.cpl	NO
MDP>LAST SUCCESSFUL MDP REFRESH :2013-08-27 14:24:01(Local Time)						
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-08-27 09:21:58(est)						

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.