



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Flare® Experience on iPad with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2 – Issue 1.0

Abstract

These Application Notes describe the configuration of the Avaya Flare® Experience on iPad device with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2.

- Avaya Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura® Communication Manager operates as an Evolution Server for the SIP endpoints which communicate with Avaya Aura® Session Manager over SIP trunks.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura® Session Manager to support registration of AvayaFlare® Experience on iPad endpoints and enables connectivity to Avaya Aura® Communication Manager Evolution Server 6.2 using SIP trunks.

As shown in **Figure 1**, Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. Flare Experience on iPad endpoints configured as SIP endpoints utilize the Avaya Aura® Session Manager User Registration feature and Avaya Aura® Communication Manager operating as an Evolution Server. Communication Manager Evolution Server is connected to Session Manager via a SIP signaling group and associated SIP trunk group.

For the sample configuration, Avaya Aura® Session Manager runs on an Avaya S8800 Server. Avaya Aura® Communication Manager 6.2 Evolution Server runs on a S8800 server with an Avaya 450 Media Gateway and an Avaya G650 Media Gateway. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura® Communication Manager 6.2.

These Application Notes will focus on the configuration of Avaya Flare® Experience in Communication Manager Evolution Server and Session Manager. Detailed administration of Communication Manager Evolution Server will not be described (see the appropriate documentation listed in **Section 9**).

For the Avaya Flare® Experience on iPad, Avaya expects an existing user to have a SIP Main extension (e.g., 41801) associated with a DID number. There would be a hard SIP phone in the office logged in as 41801. When using Flare on iPad, log in with this same SIP extension (41801).

In general, people will often have an H.323 VPN phone at home, and this H.323 extension would have a bridged appearance of the SIP hardphone extension in the office that is tied to the user's DID number.

To use the Avaya Flare® Experience on iPad from outside the corporate network, download Junos Pulse for iOS/iPAD to connect to the corporate network.

Avaya Flare® Experience on iPad - SIL FST Westminster Fiscal Q2'12

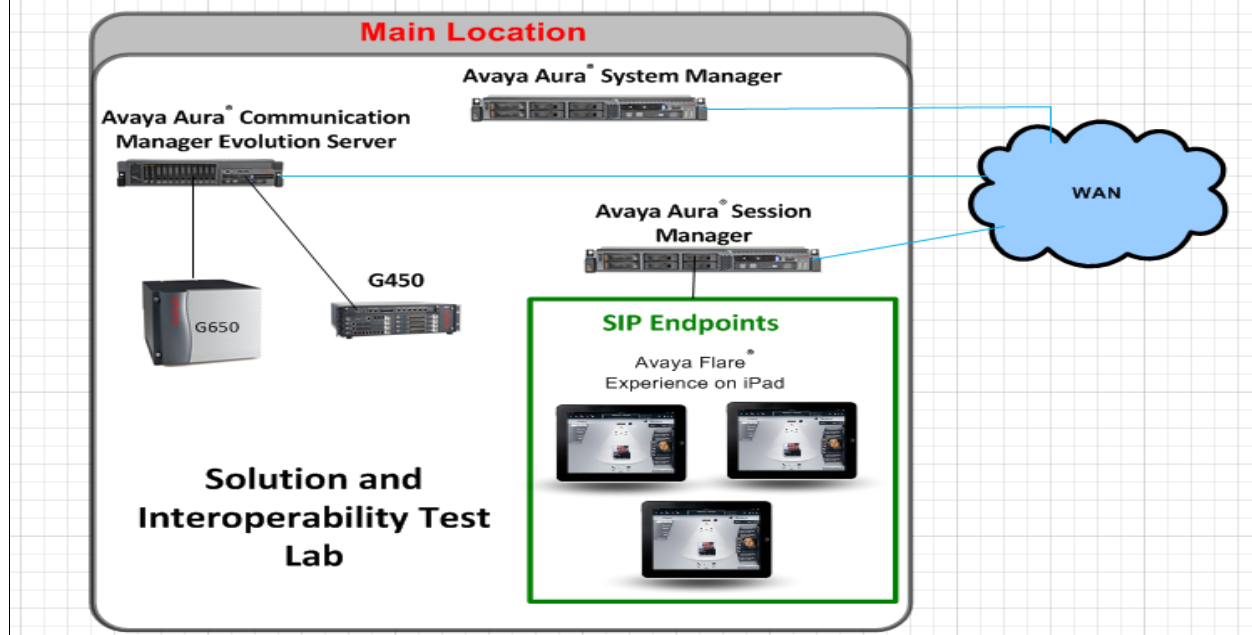


Figure 1: Sample Configuration

2. Equipment and Software Validated

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

Equipment	Software Release
Avaya Aura® Communication Manager <ul style="list-style-type: none"> Avaya S8800 Server Evolution Server 	R016x.02.0.823.0-19926
Avaya Aura® System Manager <ul style="list-style-type: none"> Avaya S8800 Server 	Release 6.2.0
Avaya Aura® Session Manager <ul style="list-style-type: none"> Avaya S8800 Server 	Release 6.2.0.0.622005
Avaya Flare® Experience on iPad	Release: 1.0 Build: R1.0 NGUE-FLAREIOSATLINT-JOB1-113
Avaya G650 Media Gateway IP Server Interface TN2312BP Clan TN799DP IPMedpro TN2602AP	Hardware 15 Firmware 51 Hardware 01 Firmware 38 Hardware 08 Firmware 55
Avaya G450 Media Gateway	Hardware 1 Firmware 31.20.1

3. Avaya Flare® Experience on iPad Limitations

- ▶ SRTP: Not supported
- ▶ Supports audio only.
- ▶ There's no Drop button. The user has to press the red handset image when active on a call to end.
- ▶ Call Pickup is supported via Feature Access Code only.
- ▶ Call Park, and Bridged Call Appearance features: not supported.
- ▶ Dual registration and Failover: not supported Remote iPad user is not supported with Avaya 3050 VPN Gateway.
- ▶ Hand-off from cellular to wifi or vice-versa: not support.
- ▶ Sipera support is very restricted w Flare iPad R1.0

4. Configure AvayaAura® Session Manager

The following steps describe configuration of Session Manager for use with Flare Experience on iPad. The following section describes administering SIP Entities between Session Manager and the Communication Manager Evolution Server in order to establish a SIP Entity link between Session Manager and the Communication Manager Evolution Server. Administering the Flare Experience on iPad to register to Session Manager is also discussed.

4.1. Access Avaya Aura® System Manager

Access the System Manager web interface, by entering **http://<ip-addr>/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running System Manager graphical user interface. Log in with the appropriate **Username** and **Password** and press the **Log On** button to access System Manager.

The screenshot shows the Avaya Aura System Manager 6.2 login interface. At the top left is the Avaya logo, and to its right is the title "Avaya Aura® System Manager 6.2". Below the logo is a red navigation bar with the text "Home / Log On". The main heading is "Log On". On the left, a box contains a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable laws." To the right of the disclaimer are two input fields: "User ID:" with the value "admin" and "Password:" with masked characters "••••••••". At the bottom right are two buttons: "Log On" and "Clear".

AVAYA Avaya Aura® System Manager 6.2

Home / Log On

Log On

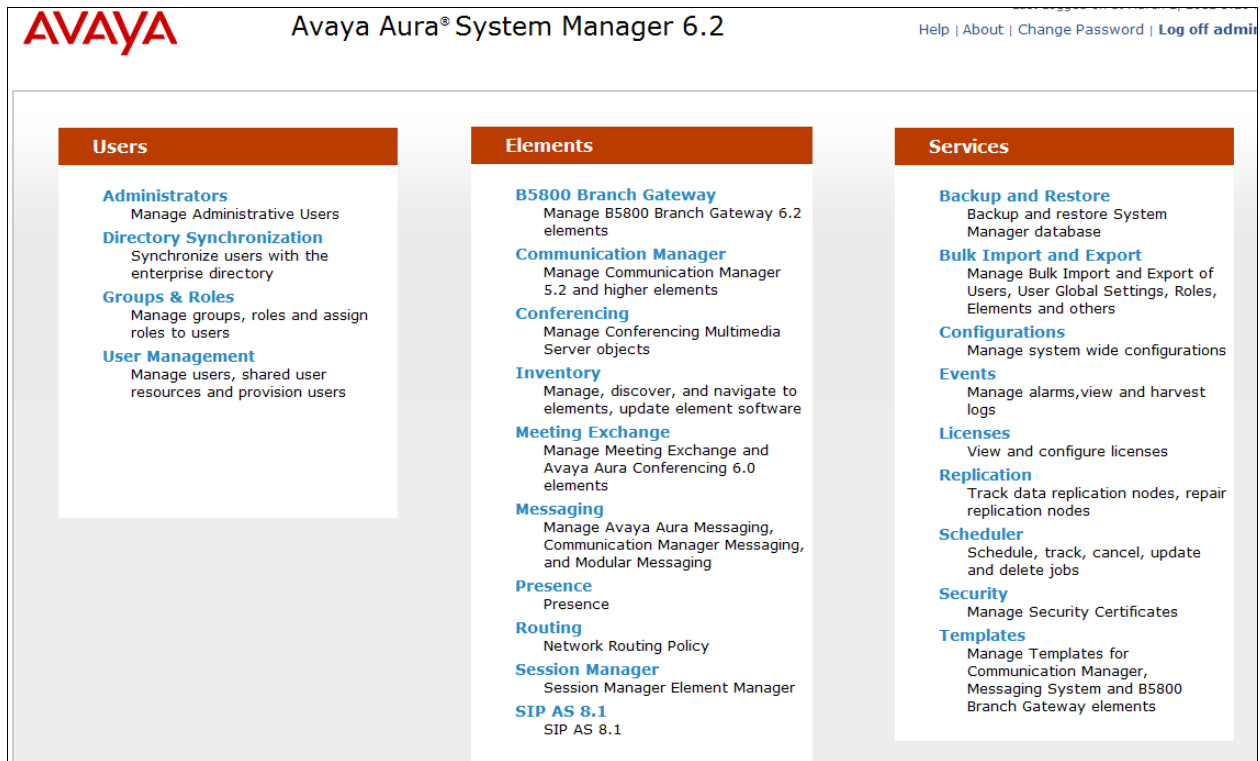
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable laws.

User ID:

Password:

The **main menu** of the **System Manager Graphical User Interface** is displayed in the following screen.



4.2. Administer SIP Domain

From the previous screen under the column **Elements** select **Routing** from the middle column of the main menu of System Manager. The following screen shows the configuration used to add a **SIP Domain**. The name of the SIP Domain used in Session Manager **dr.avaya.com** was added. The type was set to **sip**. Press the **Commit** button to add the SIP Domain.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a menu with 'Routing' and 'Domains' highlighted. The main content area is titled 'Domain Management' and includes a warning about SIP Domain name changes. Below the warning is a table with one item: 'dr.avaya.com' of type 'sip'. The 'Commit' button is highlighted.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log out

Routing * Home

Home / Elements / Routing / Domains

Domain Management

Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.

1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* dr.avaya.com	sip	<input type="checkbox"/>	SIL Lab domain

* Input Required

Commit Cancel

4.3. Add Location

To add a new Location, click on **Routing** and access the **Locations** sub heading. A location Name **135.9.xxx** was added to Session Manager. A Location Pattern of **135.9.xxx.*** was also added. The **Commit** button was pressed to confirm changes. Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

AVAYA Avaya Aura® System Manager 6.2 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / Locations

Location Details [Help ?](#) **Commit** **Cancel**

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
See Session Manager -> Session Manager Administration -> Global Settings

General

* Name: 135.9

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Mbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Audio Alarm Threshold: 80 %

* Latency before Audio Alarm Trigger: 5 Minutes

Location Pattern

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

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 135.9 <input type="text"/> <input type="text"/>	<input type="text"/>

Select : All, None

A location **Name 20.20.20** was added to the Session Manager. A Location Pattern of 20.20.20.* was also added. The **Commit** button was pressed to confirm changes.

AVAYA Avaya Aura® System Manager 6.2 Last Logged On at March 16, 2012 4:41 PM
Help | About | Change Password | Log off admin

Routing x Home

▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Locations

Location Details Commit Cancel [Help ?](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
See Session Manager -> Session Manager Administration -> Global Settings

General

* Name: 20.20.20

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▼

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec ▼

Alarm Threshold

Audio Alarm Threshold: 80 % ▼

* Latency before Audio Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 20.20.20.*	<input type="text"/>

Select : All None

4.4. Administer Avaya Aura® Session Manager SIP Entity

Under **Routing** select the sub heading **SIP Entities**. The Session Manager SIP Entity is the first part of the link between Session Manager and Communication Manager Evolution Server. Enter the **Name** of the SIP Entity. For the test configuration, **silasm3** was used. The **FQDN or IP Address** was set to **135.9.xxx.xxx** (Note: IP address is partially hidden for security). This is the IP Address of the SIP Signaling Interface in the Session Manager server. The **Type** was set to **Session Manager**. The **Location** was set to **135.9.xxx**, the **Time Zone** set to **America/Denver** and the **SIP Link Monitoring** was set to **Use Session Manager Configuration**. Press the **Commit** button.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: silasm3

* FQDN or IP Address: 135.9.xxx.xxx

Type: Session Manager

Notes: Mixed Enterprise SM

Location: 135.9.xxx

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

The following screen shows what **Port** settings need to be configured for the SIP Entity. With the signaling protocol being set to **TLS** port **5061** was used in the SIP Entity SIP trunk. Press the **Commit** button.

Port

TCP Failover port:

TLS Failover port:

Add Remove

3 Items | Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	dr.avaya.com	
<input type="checkbox"/>	5060	UDP	dr.avaya.com	
<input type="checkbox"/>	5061	TLS	dr.avaya.com	

Select : All, None

* Input Required

Commit Cancel

4.5. Administer Avaya Aura® Communication Manager Evolution Server SIP Entity

The Evolution Server SIP Entity is the second part of the link between the Session Manager and Communication Manager Evolution Server. The **Name** of the SIP Entity was **cm8**. The **FQDN or IP Address** was set to **135.9.xxx.xxx**(Note: IP address is partially hidden for security)which is the IP Address of the Evolution Server. The **Type** was set to **CM** for Communication Manager. The Location was set to **135.9.xxx** and the **SIP Link Monitoring** was set to **Use Session Manager Configuration**. Press the **Commit** button.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The breadcrumb trail shows 'Home / Elements / Routing / SIP Entities'. The left-hand menu has 'Routing' and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains the following configuration fields:

- Name:** cm8
- FQDN or IP Address:** 135.9.xxx.xxx
- Type:** CM
- Notes:** silcm8 - Business Collaboration Sol
- Adaptation:** Presence Buddy List adapter
- Location:** 135.9.xxx
- Time Zone:** America/Denver
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

A 'Commit' button is located in the top right corner of the configuration area.

4.6. Administer SIP Entity Link

To administer the SIP Entity link access the sub heading **Entity Links** on the left hand side of the System Manager GUI. The SIP **Entity Link** is the link between Session Manager and Communication Manager Evolution Server. **SIP Entity 1**, the Session Manager SIP Entity was called **silasm3_cm8_5061_TLS**. **SIP Entity 2**, the Evolution Server SIP Entity was called **cm8**. The protocol used for signaling purposes for the sip trunk was **TLS** and port number **5061** as shown in **Section 4.4**.

The screenshot displays the Avaya Aura System Manager 6.2 interface. On the left, a navigation menu includes 'Routing' (highlighted with a red box), 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links' (highlighted with a red box), 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Home / Elements / Routing / Entity Links'. It features a 'Commit' button (highlighted with a red box) and a 'Cancel' button. Below this is a table with one item, 'silasm3_cm8_5061_Tl'. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row values are: 'silasm3_cm8_5061_Tl', 'silasm3', 'TLS', '5061', 'cm8', '5061', 'Trusted', and an empty field. A red box highlights the entire row. At the bottom, there is a 'Commit' button and a 'Cancel' button. A note at the bottom left states '* Input Required'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* silasm3_cm8_5061_Tl	* silasm3	TLS	* 5061	* cm8	* 5061	Trusted	

4.7. Administer Avaya Aura® Session Manager

In order to provide the link between Session Manager and System Manager, Session Manager must be added to the configuration. From the **Home** screen, under the **Elements** column select **Session Manager**. Under the **Session Manager** heading on the left hand side of the System Manager GUI click on the **Session Manager Administration** sub heading.

The **SIP Entity Name** was set to **silasm3**. The **Management Access Point Host Name/IP** was set to **135.9.xxx.xxx**. This is the management IP Address for the server running Session Manager. **Direct Routing to Endpoints** was set to **Enable**. The **SIP Entity IP Address** was set to **135.9.xxx.xxx**(Note: IP address is partially hidden for security). This is the IP Address of the SIP Signaling Interface in Session Manager. The **NetworkMask** was set to **255.255.255.0** and the **Default Gateway** was set to **135.9.xxx.254**.

AVAYA Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Session Manager Routing Home

Session Manager Administration

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

SIP Entity Name silasm3

Description

Management Access Point Host Name/IP 135.9.xxx.xxx

Direct Routing to Endpoints Enable

Security Module

SIP Entity IP Address 135.9.xxx.xxx

Network Mask 255.255.255.0

Default Gateway 135.9.xxx.254

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID

4.8. Administer Avaya Aura® Communication Manager as an Evolution Server

In order for Communication Manager to supply configuration and feature support to SIP phones when they register to Session Manager, Communication Manager must be added as an application. From the **Home** screen, under the **Elements** column select **Inventory**. Under the **Inventory** heading on the left hand side of the System Manager GUI access the **Manage Elements** sub heading. The **Name** was set to **cm8**. The **Type** was set to **Communication Manager**. The **Node** was set to IP Address **135.9.xxx.xxx** (Note: IP address is partially hidden for security).

The screenshot displays the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below this, a breadcrumb trail reads 'Home / Elements / Inventory / Manage Elements'. The left sidebar contains a tree view with 'Inventory' and 'Manage Elements' selected. The main content area is titled 'Edit Communication Manager: cm8' and features a 'Commit' button. The 'General' tab is active, showing the following fields: 'Name' (cm8), 'Type' (Communication Manager), 'Description' (silcm8 - Business Collaboration Solution R6.2), and 'Node' (135.9.xxx.xxx).

Access the **Attributes** tab from the previous screen and set the **Login**. This was the login used to access the Communication Manager Evolution Server. The **Password** was set to the password used to access the Communication Manager Evolution Server. The **Port** was set to **5022**.

Attributes ▼

* Login

SILlab

Password

•••••

Confirm Password

•••••

Is SSH Connection

☒

* Port

5022

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled

☐

ASG Key

Confirm ASG Key

Location

Enable Notifications

☐

4.9. Administer Avaya Aura® Communication Manager Evolution Server Application

To configure the Communication Manager Evolution Server Application expand **Elements** → **Session Manager** and select **Application Configuration** from the left navigation menu. To add the application access the **Applications** sub heading. The **Name** was set to **CM8**. Select the **SIP Entity** (already created) **cm8** from the dropdown. The **CM System for SIP Entity** was set to **cm8** from the **View/Add CM Systems**. This will be used later in administering the iPad Flare Experience as a SIP user in Session Manager in **Section 4.12**

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and links for "Help | About | Change Password | Log off admin". Below this, a breadcrumb trail shows the path: "Home / Elements / Session Manager / Application Configuration / Applications". The left-hand navigation menu is expanded to "Session Manager", and within it, "Application Configuration" and its sub-item "Applications" are highlighted. The main content area is titled "Application Editor" and contains the following fields and sections:

- Application** section:
 - *Name**: Text input field containing "CM8".
 - *SIP Entity**: Dropdown menu with "cm8" selected.
 - *CM System for SIP Entity**: Dropdown menu with "cm8" selected, accompanied by a "Refresh" button and a link to "View/Add CM Systems".
 - Description**: Text input field containing "CM Rel 6.2 - Business Collaboration".
- Application Attributes (optional)** section:
 - A table with two columns: "Name" and "Value".
 - Row 1: "Application Handle" with an empty text input field.
 - Row 2: "URI Parameters" with an empty text input field.
- Application Media Attributes** section:
 - Enable Media Filtering**: A checkbox that is currently unchecked.
 - A table with five columns: "Audio", "Video", "Text", "Match Type", and "If SDP Missing".
 - Row 1: "Audio" (YES), "Video" (YES), "Text" (YES), "Match Type" (NOT_EXACT), and "If SDP Missing" (ALLOW).

At the bottom of the form, there is a legend indicating that an asterisk (*) denotes a required field. Two "Commit" and "Cancel" buttons are located at the bottom right of the form area.

4.10. Administer Avaya Aura® Communication Manager Evolution Server Application Sequence

To configure the Communication Manager Evolution Server Application Sequence access **Home**, **Elements** column, **Session Manager** and then from the **Session Manager** heading on the left hand side System Manager GUI access the sub heading **Application Configuration** and then the sub heading **ApplicationSequences**. The Evolution Server Application Sequence **Name** was added as **CM8**. This will be used later in administering the Flare Experience on iPad as a SIP user on Session Manager in **Section 4.12**.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Inventory * Session Manager * Routing * Home

Session Manager

Home /Elements / Session Manager / Application Configuration / Application Sequences

Help ?

Application Sequence Editor

Commit Cancel

Application Sequence

*Name

Description

Applications in this Sequence

Move First Move Last Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		CM8	cm8	<input checked="" type="checkbox"/>	CM Rel 6.2 - Business Collaboration Solution

Select : All, None

Available Applications

7 Items Refresh Filter: Enable

	Name	SIP Entity	Description
+	CM7	cm7	CM Rel 6.2
+	CM8	cm8	CM Rel 6.2 - Business Collaboration Solution

4.11. Synchronize Communication Manager Data

To synchronize the CM Data with Session Manager go to the **Home** screen and under the **Elements** column select **Inventory**. Under the **Inventory** heading on the left hand side select **Synchronize** and then select the sub heading **Communication System**. The following screen shows **cm8**. To begin the synchronization of the Communication Manager Evolution Server and the Session Manager highlight the **Initialize data for the selected devices** option and select the **Now** key.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Inventory Session Manager Routing Home

Inventory Home / Elements / Inventory / Synchronization / Communication System

Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while sync is in progress.

Synchronize CM Data/Launch Element Cut Through

6 Items Refresh Show ALL Filter: Enable

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location
cm7	135.9 [redacted]	March 4, 2012 10:00:00 PM - 07:00	10:00 pm SAT MAR 3, 2012	Incremental	Failed	
cm8	135.9 [redacted]	MAR 6, 2012 11:00:09 PM - 07:00	10:00 pm TUE MAR 6, 2012	Incremental	Completed	
cmfa1	135.9 [redacted]	March 7, 2012 12:26:30 PM - 07:00	10:00 pm TUE MAR 6, 2012	Incremental	Completed	
slcm2	135.9 [redacted]	March 6, 2012 11:00:09 PM - 07:00	10:00 pm TUE MAR 6, 2012	Incremental	Completed	
slcm4	135.9 [redacted]	March 7, 2012 2:00:09 AM - 07:00	10:07 pm TUE MAR 6, 2012	Incremental	Completed	
slcm5	135.9 [redacted]	March 4, 2012 10:00:16 PM -	10:00 pm SUN MAR 4, 2012	Incremental	Failed	

Select: All, None

☒ Initialize data for selected devices
☐ Incremental Sync data for selected devices
☐ Execute 'save trans all' for selected devices

Now Schedule Cancel Launch Element Cut Through

4.12. Add SIP User

To add a user to the Session Manager access **Home**→**Users**column, **User Management** and then from the heading on the left hand side of the System Manager GUI access the sub heading **Manage Users**. For the sample configuration in the **Identity** tab for the SIP User added was **Last Name** with a value of **Experience** and **First Name** with a value of **SIL iPad**. The **Login Name** is the extension plus the domain **41801@dr.avaya.com** in this scenario. **Authentication Type** is the default value of **Basic**. Add any **New Password** and **Confirm Password**.

The screenshot displays the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and links for "Help | About | Change Password | Log off admin". The breadcrumb trail is "Home / Users / User Management / Manage Users". The left sidebar shows "User Management" and "Manage Users" highlighted. The main content area is titled "User Profile Edit: 41801@dr.avaya.com" and features tabs for "Identity", "Communication Profile", "Membership", and "Contacts". The "Identity" tab is active, showing the following fields:

- * Last Name: Experience
- * First Name: SIL iPad
- Middle Name: (empty)
- Description: Password = password
- Status: Offline
- Update Time: January 19, 2012 5:15:00
- * Login Name: 41801@dr.avaya.com
- * Authentication Type: Basic
- [Change Password](#)
- * New Password: (masked with dots)
- * Confirm Password: (masked with dots)
- Source: local
- Localized Display Name: Experience, SIL iPad
- Endpoint Display Name: Experience, SIL iPad
- Title: (empty)
- Language Preference: English (United States)
- Time Zone: (empty)
- Employee ID: (empty)

Access the **Communication Profile** tab from the User Profile. For the **Communication Profile Password** enter value used to log in endpoint in the **Communication Profile Password** and **Confirm Password** fields. In the **Communication Address** the **Type** was set to **Avaya SIP**. The **Fully Qualified Address** was set as 41801@dr.avaya.com. Select the **Add** button to save the changes.

User Profile Edit: 41801@dr.avaya.com

Communication Profile

Communication Profile Password: [Masked Password] [Edit](#)

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya E.164	+13035341801	dr.avaya.com
<input checked="" type="checkbox"/> Avaya SIP	41801	dr.avaya.com
<input type="checkbox"/> Avaya XMPP	41801@ps.dr.avaya.com	

Select : All, None

Type: Avaya SIP

* Fully Qualified Address: 41801 @ dr.avaya.com

Add Cancel

Be certain to **check** the **Session Manager Profile** box. The **Primary Session Manager** was set to **silasm3** as shown below. This equates to the Session Manager SIP entity. The **Origination and Termination Application Sequence** was set to **CM8**. This is the Communication Manager Evolution Server Application Sequence name. The **Home Location** was set to **20.20.20**. (Note: Flare Experience® on iPad does not support failover or Survivability).

☒ **Session Manager Profile**

* **Primary Session Manager** silasm3

Primary	Secondary	Maximum
17	3	20

Secondary Session Manager (None)

Primary	Secondary	Maximum

Origination Application Sequence CM8

Termination Application Sequence CM8

Conference Factory Set (None)

Survivability Server (None)

* **Home Location** 20.20.20

In order for the Station Profile template information to be pushed from Session Manager down to Communication Manager Evolution Server, **check** the **CM Endpoint Profile** box. The System was set to **cm8**. This is the Communication Manager Evolution Server Element Name. The **Profile Type** was set to **Endpoint**. The **Extension** was set to **41801**. For the **Security Code** value used to log in endpoint The **Port** was set to **IP**.

☒ **CM Endpoint Profile**

* **System** cm8

* **Profile Type** Endpoint

Use Existing Endpoints ☐

* **Extension** 41801 Endpoint Editor

Template Select/Reset

Set Type 9640SIP

Security Code *****

* **Port** S00014

Voice Mail Number

Preferred Handle (None)

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☐

Override Endpoint Name ☒

Click on **Endpoint Editor** and select the **Feature Options** tab. Enable **IP softphone** y placing a check in the box next to each respective feature. Select **Done** and Select **Commit**(not shown) when back to the main User Profile screen.

The screenshot shows the 'Feature Options (F)' tab selected. The settings are as follows:

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)	

Active Station Ringing	single	Auto Answer	none
MWI Served User Type	Select	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	Select	Display Language	english
IP Phone Group ID		Hunt-to Station	
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19
LWC Reception	spe	Survivable COR	internal
AUDIX Name	Select	Time of Day Lock Table	Select
Speakerphone	Select	Voice Mail Number	
Short/Prefixed Registration Allowed	default		
EC500 State	enabled		

Features

<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> IP Video Softphone
<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control

*Required

Done Cancel

5. Administer Avaya Aura® Communication Manager Evolution Server

This section highlights the important commands for defining the Flare Experience iPad as an Off-PBX Station (OPS) and administering a SIP Trunk and Signaling Group to carry calls between Flare Experience on iPad in Communication Manager Evolution Server.

This section describes the administration of Communication Manager Evolution Server using a System Access Terminal (SAT). These instructions assume the G450 Media Gateway and G650 Media Gateway are already configured on Communication Manager Evolution Server. Some administration screens have been abbreviated for clarity.

5.1. Verify OPS Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Off-PBX Telephones – OPS** has been set to the value that has been licensed, and that this value will accommodate addition of the SIP telephones. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to obtain additional capacity.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                         Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 77
Maximum Stations: 41000 13
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 10
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0

(NOTE: You must logoff & login to effect the permission changes.)
```

Verify that there are sufficient licenses to administer the SIP Trunk. This is the **Maximum Administered SIPTrunks** value on **Page 2** of System Parameter Customer-Options.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	8000	12	
Maximum Concurrently Registered IP Stations:	18000	3	
Maximum Administered Remote Office Trunks:	8000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	128	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	0	
Maximum Video Capable IP Softphones:	100	3	
Maximum Administered SIP Trunks: 5000 160			
Maximum Administered Ad-hoc Video Conferencing Ports:	8000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	522	0	
Maximum TN2501 VAL Boards:	10	1	
Maximum Media Gateway VAL Sources:	250	0	
Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
Maximum TN2602 Boards with 320 VoIP Channels:	128	0	
Maximum Number of Expanded Meet-me Conference Ports:	300	0	

5.2. Administer Dial Plan Analysis

This section describes the **Dial Plan Analysis** screen. This configuration enables Communication Manager to interpret digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The **Dialed String** beginning with the number **41** and with a **Total Length** of **5** digits will be used to administer the **extension** range used for the Flare Experience on iPad.

displaydialplan 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
31		5 ext						
32		5 ext						
38		5 ext						
41		5 ext						
79		5 ext						
8		1 fac						
9		1 fac						
*		3 fac						
#		4 dac						

5.3. Administer IP Node-Name

This section describes **IP Node-Name**. This is where Communication Manager assigns the IP Address and node-name to Session Manager. The node-name is **silasm3** and the IP Address is **135.9.xxx.xxx**.

```
list node-names all

                                NODE NAMES

Type      Name                  IP Address
IP         default              0.0.0.0
IP         procr                135.9.xxx.xxx
IP         procr6               ::
IP        silasm3              135.9.xxx.xxx
```

5.4. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip** and the **Transport Method** was set to **tls**. Since the sip trunk is between Communication Manager Evolution Server and Session Manager the **Near-end Node Name** is the node name of the “procr” of the Communication Manager Evolution Server. The **Far-end Node Name** is the node name of the Session Manager Server that is **silasm3**. The **Near-end Listen Port** and **Far-end Listen Port** are both set to port number **5061**. The **Far-end Network-Region** was set to **1**.

```
display signaling-group 10                                     Page 1 of 2

                                SIGNALING GROUP

Group Number: 10                      Group Type: sip
IMS Enabled? n                        Transport Method: tls
Q-SIP?n
    IP Video? n                      Priority Video? n          Enforce SIPS URI for SRTP? y
    Peer Detection Enabled? y        Peer Server: SM

Near-end Node Name: procr              Far-end Node Name: silasm3
Near-end Listen Port: 5061            Far-end Listen Port: 5061
Far-end Network Region: 1

                                Far-end Secondary Node Name:
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? n
H.323 Station Outgoing Direct Media?n    Initial IP-IP Direct Media? n
                                           Alternate Route Timer(sec): 6
```

5.5. Administer Trunk Group

This section describes the **Trunk Group** used to carry calls between the Flare Experience on iPad. Trunk Group 10 was configured as a SIP Trunk with the **Group Type** set as **sip**. The trunk **Group Name** was set to **SIP TG to silasm3**. The TAC was set to **#010**. The **Direction** of the calls was set to **two-way** as there will be calls to and from the Flare Experience on iPad. The **Service Type** was set to **tie** as the trunk is an internal trunk between Communication Manager Evolution Server and Session Manager. The **Signaling Group** number assigned to this trunk is **10**. The **Number of Members** assigned to this trunk group is **64**. All other fields on this page are left as default.

```
display trunk-group 10                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 10                Group Type: sip           CDR Reports: y
Group Name: SIP TG to silasm3   COR: 1                 TN: 1         TAC: #010
Direction: two-way             Outgoing Display? y
Dial Access? n                 Night Service:
Queue Length: 0
Service Type: tie              Auth Code? n
Member Assignment Method: auto
Signaling Group: 10
Number of Members: 64
```

On Page 3 of the trunk group form **Numbering Format** was set to **private**.

```
display trunk-group 10                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment?n              Measured: none
Maintenance Tests?y

Numbering Format: private

                               UUI Treatment: service-provider

                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n

                               Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
DSN Term?n
```

5.6. Administer IP Network Region

This section describes the **IP Network Region** screen. It was decided to place the Flare Experience on iPad in network region 1. The **Authoritative Domain** must mirror the domain name of Session Manager. This was **dr.avaya.com**. The codecs used on the SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** was set to **yes**.

```
displayip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: dr.avaya.com
Name: BCS
MEDIA PARAMETERS                                Intra-region IP-IP Direct Audio: yes
Codec Set: 1      Inter-region IP-IP Direct Audio: yes
UDPPort Min: 2048                                IP Audio Hairpinning? n
UDPPort Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.7. Administer IP Codec Set

This section describes the **IP Codec Set** screen. IP Codec **G.711MU**, **G.711A**, **G.729**, and **G.722-64k** were used for testing purposes with the Flare Experience on iPad

```
displayip-codec-set 1                                         Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   PerPkt      Size (ms)
1: G.711MU      n          2          20
2: G.711A      n          2          20
3: G.729      n          2          20
4: G.722-64K    2          20
```

5.8. Administer Off PBX Telephone Station Mapping

This section shows the **off-pbx-telephone station-mapping**. The Flare Experience on iPad extension **41801** uses off pbx **Application OPS** which is used for SIP enabled telephones. The **SIP Trunk Selection** is set to **aar**. The **Config Set** which is the desired call treatment was set to **1**.

display off-pbx-telephone station-mapping						
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Config SelectionSet	Dual Mode
41800	OPS	-		41800	aar	1
41801	OPS	-		41801	aar	1
41802	OPS	-		41802	aar	1
		-				
		-				

The **Call Limit** is set to **3** as shown below. This is the maximum amount of simultaneous calls for extension 41801. The **Mapping Mode** field was set to **both** in this configuration setup. This is used to control the degree of integration between SIP telephones. The **Calls Allowed** field was set to **all**. This identifies the call filter type for a SIP Phone. The **Bridged Calls** field was set to **none** as it was not needed for testing purposes.

display off-pbx-telephone station-mapping						
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION						
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location
41800	OPS	3		both	all	none
41801	OPS	3		both	all	none
41802	OPS	3		both	all	none

5.9. Administer Station Screen

This screen describes the **station** form setup for the Flare Experience on iPad on Communication Manager. The **Extension** used was **41801** with phone **Type 9640SIP**. Phone type 9640SIP was the recommended phone type to use for the Flare Experience on iPad. The **Name** of the phone was set to **Experience, SIL iPad** and the **IP SoftPhone** was set to **y**, this is required for the Flare Experience on iPad. All other values on **Page 1** of the station form were left as default.

display station 41801		Page 1 of 6
STATION		
Extension: 41801	Lock Messages? n	BCC: M
Type: 9640SIP	Security Code: xxxxxx	TN: 1
Port: S00014	Coverage Path 1: 1	COR: 1
Name: Experience, SIL iPad	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19		
	Message Lamp Ext: 41801	
Display Language: english	Button Modules: 0	
Survivable COR: internal		
Survivable Trunk Dest?y	IP SoftPhone? y	
IP Video Softphone?n		
	Short/Prefixed Registration Allowed: default	

5.10. Administer Private Numbering

This screen describes the **private numbering** form on Communication Manager. The **Ext Len** was set to **5** digits. The **Extension Code** was **41**. The **Total Length** set to **5**.

Displayprivate-numbering 0		Page 1 of 2			
NUMBERING - PRIVATE FORMAT					
Ext Len	ExtTrk Code	Private Grp(s)	Total Prefix	Len	
5	31			5	Total Administered: 5
5	32			5	Maximum Entries: 540
5	38			5	
5	41			5	
5	79			5	

This screen describes the **aar analysis** form setup for the Flare Experience on iPad on Communication Manager. When an extension beginning with **4** is dialed the aar analysis table expects a **minimum** and a **maximum** of **5** digits. The aar analysis table routes the call to Route Pattern 10. The call type was **aar**.

5.12. Administer Routing Pattern

```

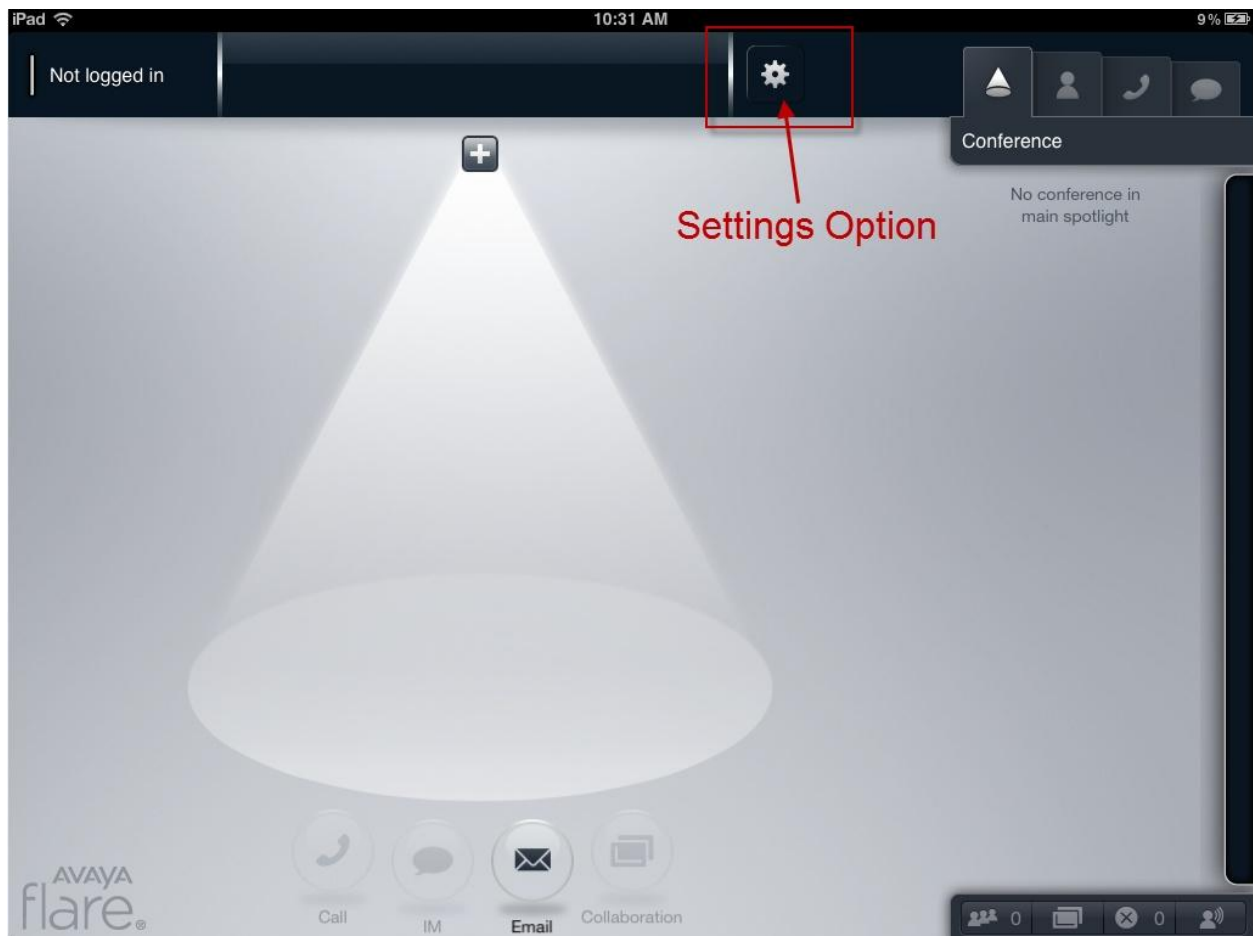
display route-pattern 10
                                Page 1 of 3
                                Pattern Number: 10 Pattern Name: Route 2 silasm3
                                SCCAN? n Secure SIP? n
  Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC
  No          Mrk Lmt List Del Digits  QSIG
                                Dgts      Intw
1: 10 0
                                n user
2:
                                n user
3:
                                n user
4:
                                n user
5:
                                n user
6:
                                n user

  BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
  0 1 2 M 4 W Request      Dgts Format
                                Subaddress
1: y y y y y n n rest lev0-pvt none
2: y y y y y n n rest none

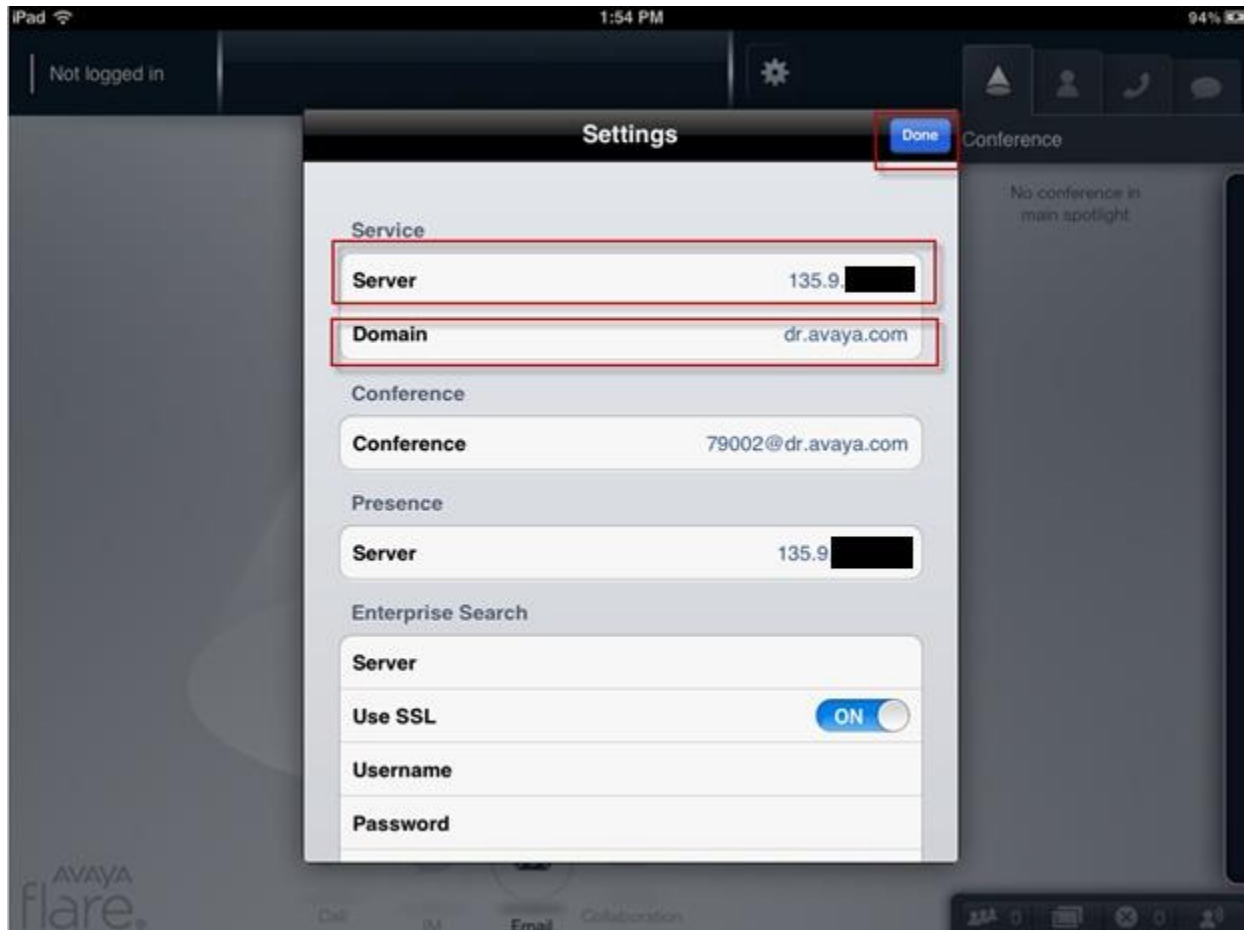
```

6. Configure the Flare Experience on iPad

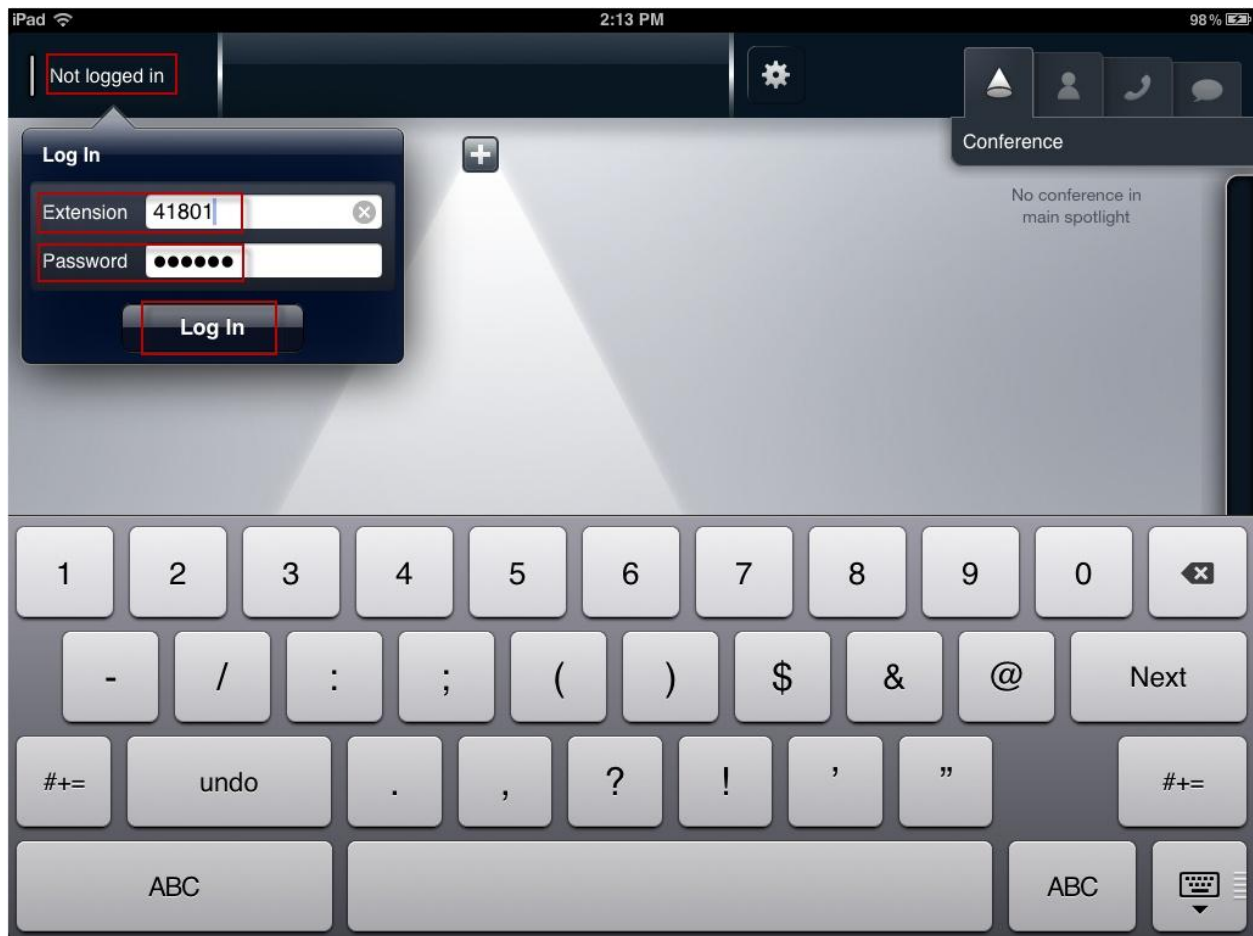
This section describes steps needed to configure and connect the Flare Experience on iPad to Session Manager. It's assumed the Flare Experience application is already loaded on the iPad and the iPad is already on the correct wireless network. Once the Flare Experience application is opened the following screen is displayed.



Press on the **Settings** option on the top of the Flare Experience application, see previous screen. The **Settings** menu appears with several options to configure the device, see screen below. Under the title **Service** press anywhere in the **Server** box. Enter the IP Address of the Session Manager's SIP Signaling Interface. Press anywhere in the **Domain** box. Enter the Domain of the network you are connecting to. Press on **Done** when finished. The main Flare Experience screen will be displayed again as in the previous screen.



Press on the **Not logged in** button as seen in the screen below. The **Log In** window will appear. Enter the **Extension** and **Password** that was administered in **Section 4.12** under the **Communication Profile** tab. Press on the **Log In** button.



7. Verification Steps

The following five verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

1. Verified the Flare Experience on iPad extension 41801 was registered to the Session Manager. Verified the extension 41801 was logged in successfully to the Flare Experience on iPad.
2. Verified a call could be made with clear audio between the Flare Experience on iPad. Verified the call was seen to be active on the SIP Trunk within Communication Manager. This was successful.
3. Verified supplementary features such as Call Hold, Mute, and Conference could be completed between the Flare Experience on iPad. This was successful.

Access **Elements**→**Session Manager**→**System Status**→**User Registrations** to see the Flare Experience on iPad extension **41801** registered to Session Manager.

Avaya Aura® System Manager 6.2

Home / Elements / Session Manager / System Status / User Registrations

User Registrations

Select rows to send notifications to AST devices. Click on Details column for complete registration status.

Advanced Search Criteria

Login Name: Contains 418

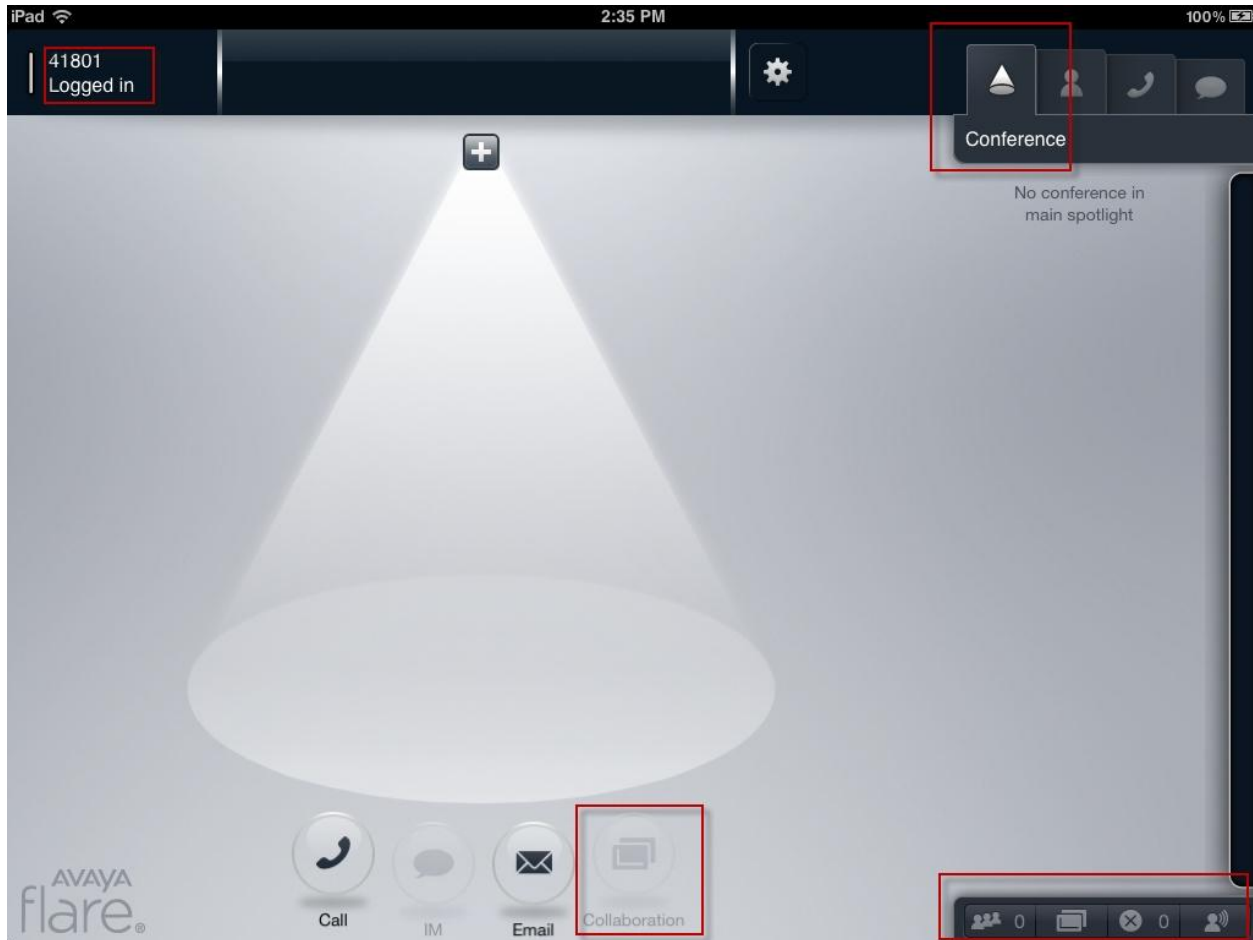
Clear Search Close

AST Device Notifications: Reboot Reload Failback As of 9:15 PM

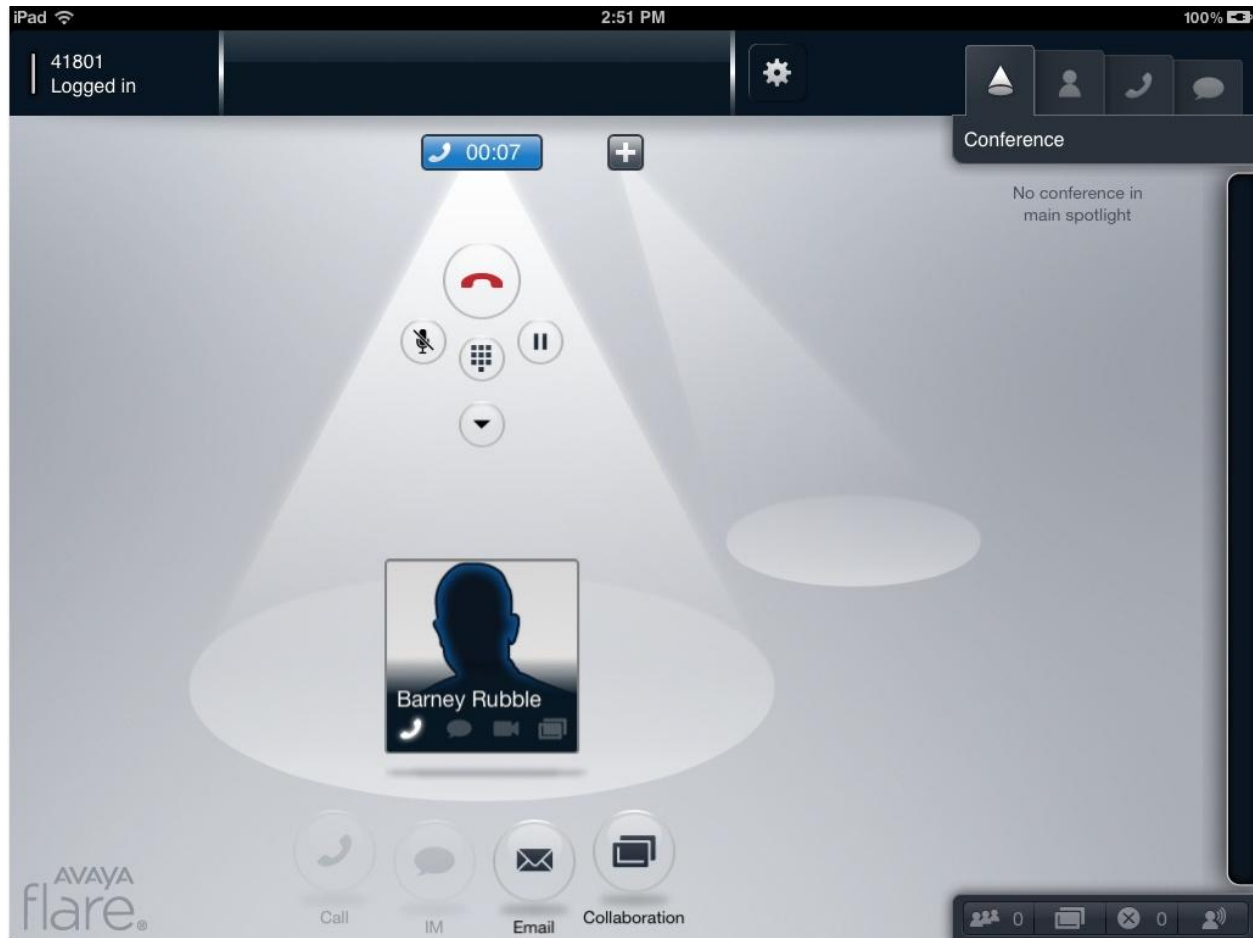
7 Items Refresh Reset Show ALL Filter: Enable

Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
								Prim	Sec	Surv
Show	---	41800@dr.avaya.com	iPad Flare Experience	Martinez	20.20.20	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	41801@dr.avaya.com	41801@dr.avaya.com	Fred	Flintstone	20.20.20	135.9.100.5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

On the top left hand corner of the screen below the extension **41801** and **Logged in** is displayed. This means that the Flare Experience is now logged and is able to make/receive audio phone calls. Notice the other icons displayed including Collaboration, Conference, and Conference icons on the bottom right hand corner. These items are only displayed and functional with Flare Experience and not Flare Communicator.



From the screen below, a successful call was made from the Flare Experience on iPad.



8. Conclusion

These Application Notes have described the administration steps required to register Avaya Flare® Experience on iPad to Avaya Aura® Session Manager with Avaya Aura® Communication Manager running as an Evolution Server and make a successful audio call.

Interoperability testing included successfully making bi-directional calls between several different types of audio endpoints.

9. Additional References

- [1] [“Avaya Aura® Session Manager Overview”, Document Number 03-603323, Release 6.2, February 2012](#)
- [2] [“Implementing Avaya Aura® Session Manager”, Document Number 03-603473, Release 6.2, February 2012](#)
- [3] [“Administering Avaya Aura® Session Manager”, Document Number 03-603324, Release 6.2, February 2012](#)
- [4] [“Maintaining and Troubleshooting Avaya Aura® Session Manager, Document Number 03-603325, Release 6.2, February 2012](#)
- [5] [“Installing and Upgrading Avaya Aura® System Manager”, Release 6.1, November 2010](#)
- [6] [“Administering Avaya Aura® System Manager”, Release 6.2, February 2012](#)
- [7] [“Avaya Aura™ Communication Manager Overview”, Document Number 03-300468, Issue 7, Release 6.0, June 2010](#)
- [8] [“Administering Avaya Aura® Communication Manager”, Document Number 03-300509, Issue 7.0, February 2012](#)
- [9] [“Avaya Aura® Communication Manager Feature Description and Implementation”, Document Number 555-245-205, Issue 9.0, February 2012](#)
- [10] [“Administering Network Connectivity on Avaya Aura® Communication Manager”, Document Number 555-233-504, Issue 16, February 2012](#)
- [11] [“SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers”, Document Number 555-245-206, Issue 9, May 2009”](#)

©2012 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com