



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Flare® Experience on iPad device with Avaya Aura® Communication Manager 6.2 FP2 and Avaya Aura® Session Manager 6.2 FP2 – 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 FP2 and Avaya Aura® Session Manager 6.2 FP2.

- Avaya Aura® Communication Manager operates as an Evolution Server for the SIP endpoints which communicate with Avaya Aura® Session Manager over SIP trunks.
- 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.

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 Avaya Flare® Experience on iPad endpoints and enables connectivity to Avaya Aura® Communication Manager Evolution Server 6.2 FP2 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 FP2 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 FP2.

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 hard phone extension in the office that is tied to the users 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.

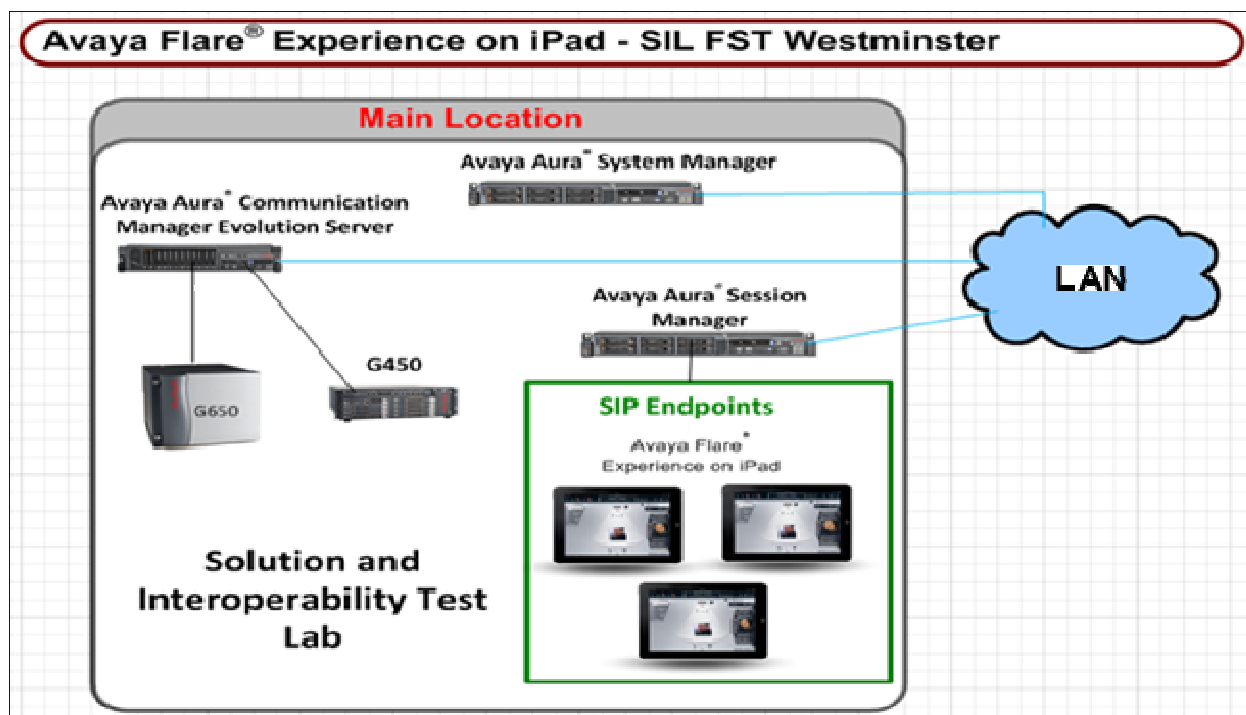


Figure 1: Sample Configuration

2. Equipment and Software Validated

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

Equipment	Software Release
Avaya Aura® Communication Manager Evolution Server <ul style="list-style-type: none"> Avaya S8800 Server 	R016x.03.0.124.0- 20553
Avaya Aura® System Manager <ul style="list-style-type: none"> Avaya S8800 Server 	Release 6.2.0 – FP2
Avaya Aura® Session Manager <ul style="list-style-type: none"> Avaya S8800 Server 	Release 6.3.2.0.632023
Avaya Flare® Experience on iPad	Release: 1.1.1 Build: NGUE-FLAREIOSPACSP1INT-JOB1-21
Avaya G650 Media Gateway <ul style="list-style-type: none"> 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

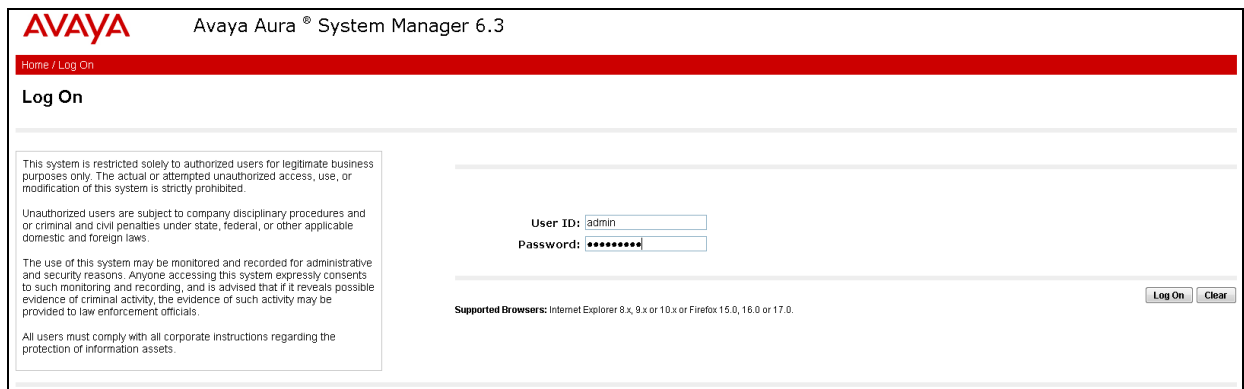
- ▶ Requires Avaya Aura® Conferencing 7.0 or later to make a conference call or transfer a call.
- ▶ Collaboration Agent is not supported on the iPad.
- ▶ SRTP: Not supported
- ▶ Call Pickup is supported via Feature Access Code only.
- ▶ Call Park, and Bridged Call Appearance features: not supported.
- ▶ Dual registration and Failover is not supported
- ▶ Remote iPad user is not supported with Avaya 3050 VPN Gateway.
- ▶ Hand-off from cellular to wifi or vice-versa: not supported.

4. Configure Avaya Aura® 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.

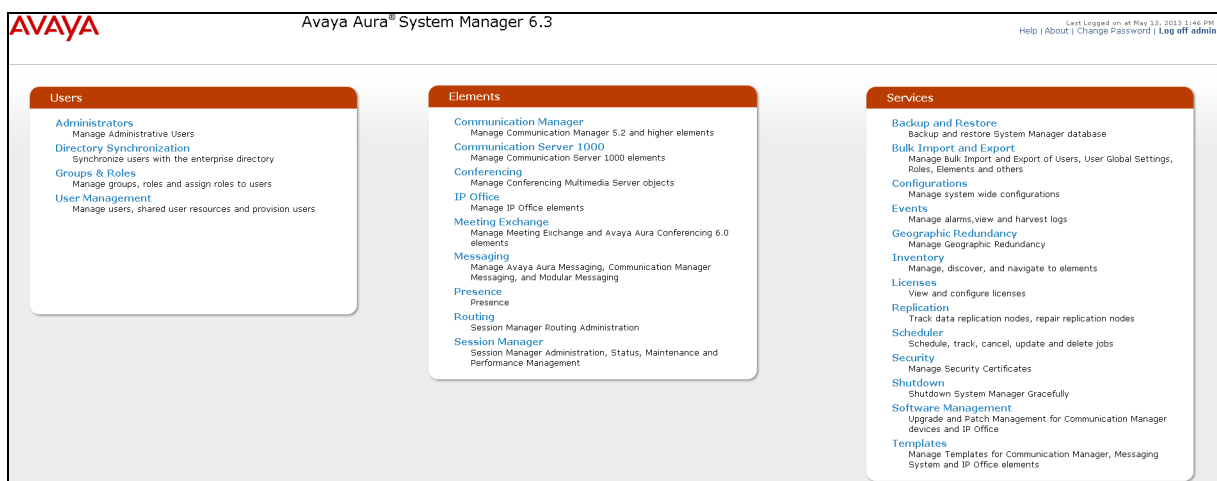
4.1. Access Avaya Aura® System Manager

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 6.3 login page. At the top, the Avaya logo and title "Avaya Aura® System Manager 6.3" are displayed. Below this is a red navigation bar with "Home / Log On". The main heading is "Log On". On the left, a disclaimer states: "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 domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets." In the center, there are input fields for "User ID:" (containing "admin") and "Password:" (masked with dots). Below these fields, it says "Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0." At the bottom right, there are "Log On" and "Clear" buttons.

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 6.3 interface. The left sidebar contains a menu with 'Routing' and 'Domains' highlighted. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for Name, Type, and Notes. The Name field contains 'dr.avaya.com', the Type field is set to 'sip', and the Notes field contains 'SIL Lab domain'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table.

Avaya Aura® System Manager 6.3

Last Logged on at May 17, 2013 12:10 PM
Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Notes
* dr.avaya.com	sip	SIL Lab domain

Commit Cancel

4.3. Add Location

To add a new Location, click on **Routing** and access the **Locations** sub heading. Select **New** (not shown). A location **Name SIL Lab** was added to Session Manager. Select Add under Location Pattern. A Location Pattern of 10.80.120.* 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.

AVAYAAvaya Aura® System Manager 6.3

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Location Details

CommitCancel

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 See Session Manager -> Session Manager Administration -> Global Settings

General

* Name: SIL Lab

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

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

AddRemove

1 Item Refresh

IP Address Pattern

* 10.80.120.*

Note:

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 **10.10.10.1**. This is the IP Address of the SIP Signaling Interface in the Session Manager server. The **Type** was set to **Session Manager**. Select the appropriate **Location**. Press the **Commit** button.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Commit Cancel

* Name: silasm3

* FQDN or IP Address: 10.10.10.1

Type: Session Manager

Notes: AAC SM

Location: SIL Lab

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

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
5060	TCP	dr.avaya.com	
5060	UDP	dr.avaya.com	
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 test SIP Entity is **cm8**. The **FQDN or IP Address** was set to **10.10.10.2** which is the IP Address of the Evolution Server. The **Type** was set to **CM** for Communication Manager. Select the appropriate **Location**. Press the **Commit** button.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: cm8

*** FQDN or IP Address:** 10.10.10.2

Type: CM

Notes: silcm8 - Business Collaboration Sol

Adaptation: Presence Buddy List adapter

Location: SIL Lab

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

*** SIP Timer B/F (in seconds):** 4

Credential name:

Call Detail Recording: none

Loop Detection Mode: Off

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Commit **Cancel**

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. The Session Manager SIP Entity **silasm3** configured in **Section 4.4** was selected for **SIP Entity 1**. The Communication Manager Evolution Server SIP Entity **cm8** configured in **Section 4.5** was selected for **SIP Entity 2**. The protocol used for signaling purposes for the sip trunk was **TLS** with port number **5061** as shown in **Section 4.4**.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/> silasm3_cm8_5061_T1	<input type="text" value="silasm3"/>	<input type="text" value="TLS"/>	<input type="text" value="5061"/>	<input type="text" value="cm8"/>	<input type="text" value="5061"/>	<input type="text" value="trusted"/>	<input type="checkbox"/>

Select : All, None

Commit Cancel

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 **10.10.10.3**. 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 **10.10.10.1**. This is the IP Address of the SIP Signaling Interface in Session Manager. The **Network Mask** was set to **255.255.255.0** and the **Default Gateway** was set to **10.10.10.254**. The rest of the values were left as default.

AVAYA Avaya Aura® System Manager 6.3

Home / Elements / Session Manager / Dashboard

Edit Session Manager Commit Cancel

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: 10.10.10.3

*Direct Routing to Endpoints: Enable

VMware Virtual Machine: ☐

Security Module

SIP Entity IP Address: 10.10.10.1

*Network Mask: 255.255.255.0

*Default Gateway: 10.10.10.254

*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 **Services** 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 **Hostname or IP Address** was set to **10.10.10.2**. In this example the **Login** was set to **tjm**. This is the login used to access the Communication Manager Evolution Server. Select the appropriate **Authentication Type** and **Password**. Use the default **Port 5022**.

Avaya Aura® System Manager 6.3

Left Logged on at May 20, 2013 3:33 PM
Help | About | Change Password | Log off admin

Inventory Home

Home / Services / Inventory / Manage Elements

Edit Communication Manager cm8

Commit Reset Cancel

General Attributes (G) SNMP Attributes (S)

Name cm8 Description silcm8 - Business Collaboratio

Hostname or IP Address 10.10.10.2 Alternate IP Address

Login tjm Enable Notifications

Authentication Type Password Port 5022

ASG Key Location

Password *****

Confirm Password *****

SSH Connection ☒

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Commit Reset Cancel

Access the **SNMP Attributes** tab from the previous screen and select **V1** for **Version**. In the example **Read Community** is set to **public**. Select **Avaya Aura® Communication Manager** from the dropdown list for **Device Type**. Use the default values for the remaining fields. Select **Commit**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows the navigation menu with 'Inventory' and 'Manage Element' highlighted. The main content area is titled 'Edit Communication Manager cm8'. Within this area, the 'SNMP Attributes' tab is active. The configuration fields are as follows:

- Version:** Radio buttons for None, V1 (selected), and V3.
- Read Community:** Text input field containing 'public'.
- Write Community:** Text input field containing 'private'.
- Retries:** Spin box set to '1'.
- Timeout (ms):** Spin box set to '5000'.
- Device Type:** Dropdown menu showing 'Avaya Aura(R) Communication Manager'.

At the top right of the configuration area, there are buttons for 'Commit', 'Reset', and 'Cancel'. The 'Commit' button is highlighted with a red box. The bottom right of the page also contains 'Commit', 'Reset', and 'Cancel' buttons.

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** (created in **Section 4.5**) **cm8** from the dropdown list. The **CM System for SIP Entity** was set to **cm8** from the **View/Add CM Systems** link. This will be used later in administering the iPad Flare Experience as a SIP user in Session Manager in **Section 4.12**. Select **Commit**.

Avaya Aura® System Manager 6.3

Home / Elements / Session Manager / Application Configuration / Applications

Application Editor Commit Cancel

Application

*Name

*SIP Entity

*CM System for SIP Entity Refresh [View/Add CM Systems](#)

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

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 **Application Sequences**. 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**. Under the **Available Application** section select the **+** next to **CM8** and CM8 will be added to the list under **Applications in this Sequence** as seen below. Select **Commit**.

Avaya Aura® System Manager 6.3

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

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
<input type="checkbox"/>		CM8	cm8	<input checked="" type="checkbox"/>

Select : All, None

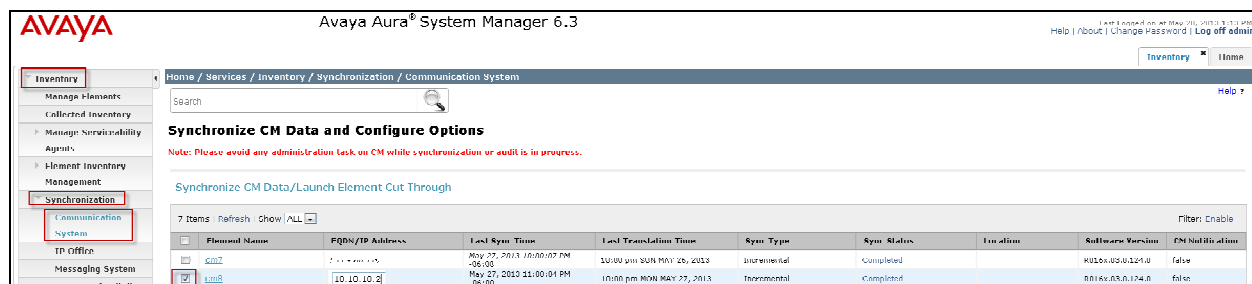
Available Applications

6 Items | Refresh

	Name	SIP Entity
<input type="checkbox"/>	CM7	cm7
<input checked="" type="checkbox"/>	CM8	cm8

4.11. Synchronize Communication Manager Data

To synchronize the CM Data with Session Manager go to the **Home** screen and under the **Services** 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 synchronization of the Communication Manager Evolution Server and the Session Manager check the box next to CM8 and select the radio **Initialize data for the selected devices** option and select the **Now** key (not shown).



Avaya Aura[®] System Manager 6.3

Home / Services / Inventory / Synchronization / Communication System

Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while synchronization or audit is in progress.

Synchronize CM Data/Launch Element Cut Through

7 Items Refresh Show ALL

Plan	Plan Name	PQDN/TP Address	Last Syn Time	Last Translation Time	Syn Type	Syn Status	Location	Software Version	CM Synchronization
<input type="checkbox"/>	cm7	10.10.10.15	May 27, 2013 10:00:07 PM -05:00	10:00 pm SUN MAY 26, 2013	Incremental	Completed		KOLON-02-0.124.0	false
<input checked="" type="checkbox"/>	cm8	10.10.10.3	May 27, 2013 11:00:04 PM -05:00	11:00 pm MON MAY 27, 2013	Incremental	Completed		0016x.A3.0.174.0	false

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 6.3 interface. The top header shows the Avaya logo, the system name "Avaya Aura® System Manager 6.3", and links for "Help | About | Change Password | Log off admin". The breadcrumb trail is "Home / Users / User Management / Manage Users". The left sidebar contains a "User Management" menu with "Manage Users" selected. 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 fields for "Last Name" (Experience), "First Name" (SIL iPad), "Middle Name", "Description" (Password = password), "Status" (Offline), "Update Time" (January 19, 2012 5:15:00), "Login Name" (41801@dr.avaya.com), "Authentication Type" (Basic), "New Password", "Confirm Password", "Source" (local), "Localized Display Name" (Experience, SIL iPad), "Endpoint Display Name" (Experience, SIL iPad), "Title", "Language Preference" (English (United States)), "Time Zone", and "Employee ID".

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** section, 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: 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** enter value used to log in endpoint The **Port** was set to **IP** (to be automatically changed to a specific port setting) .

The screenshot shows a configuration form for a CM Endpoint Profile. The following fields and controls are highlighted with red boxes:

- ☒ **CM Endpoint Profile** (with a dropdown arrow)
- * System**: A dropdown menu showing **cm8**.
- * Profile Type**: A dropdown menu showing **Endpoint**.
- Use Existing Endpoints**: An unchecked checkbox.
- * Extension**: A text input field containing **41801**, followed by a button labeled **Endpoint Editor**.
- Template**: A dropdown menu showing **Select/Reset**.
- Set Type**: A text input field containing **9640SIP**.
- Security Code**: A text input field containing six dots (••••••).
- * Port**: A text input field containing **S00014**.
- Voice Mail Number**: An empty text input field.
- Preferred Handle**: A dropdown menu showing **(None)**.
- Delete Endpoint on Unassign of Endpoint from User or on Delete User**: An unchecked checkbox.
- Override Endpoint Name**: A checked checkbox.

Click on **Endpoint Editor** and select the **Feature Options** tab. Enable **IP softphone** and **IP Video Softphone** by placing a check in the box next to each respective feature. Select **Done** and Select **Commit** (not shown) to go 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 (E)	Group Membership (M)	

Settings:

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

Features

- ☐ Always Use
- ☐ IP Audio Hairpinning
- ☐ Bridged Call Alerting
- ☐ Bridged Idle Line Preference
- ☒ Coverage Message Retrieval
- ☐ Data Restriction
- ☒ Survivable Trunk Dest
- ☐ Bridged Appearance Origination Restriction
- ☒ Restrict Last Appearance
- ☐ Idle Appearance Preference
- ☒ IP SoftPhone
- ☒ LWC Activation
- ☐ CDK Privacy
- ☒ Precedence Call Waiting
- ☒ Direct IP-IP Audio Connections
- ☐ H.320 Conversion
- ☒ IP Video Softphone
- ☐ 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 to and from 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 SIP Trunks** value on **Page 2**.

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 administrator can specify 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.

display dialplan 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 **10.10.10.1**.

```
list node-names all
```

NODE NAMES		
Type	Name	IP Address
IP	default	0.0.0.0
IP	procr	10.10.10.2
IP	procr6	::
IP	silasm3	10.10.10.1

5.4. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip**, **Transport Method** was set to **tls**, and **IP Video** was set to **y**. 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? y              Priority Video? n      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

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** as administered in **Section 5.4**. 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                     SIP ANAT Supported? n
```

5.6. Administer IP Network Region

This section describes the **IP Network Region** screen. The test configuration placed 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** as administered in **Section 4.2**. The codecs used on the SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on by setting both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to yes.

```
display ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: dr.avaya.com
Name: BCS      Stub Network Region: n
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 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: 123456	TN: 1
Port: S00014	Coverage Path 1: 1	COR: 5
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? y	
	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**.

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

5.11. Administer AAR Analysis

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 tables 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**.

Change aar analysis 0							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
				Location: all		Percent Full: 1	
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
2		7	7	999	aar		n
3		5	5	10	unku		n
388		5	5	10	aar		n
4		5	5	10	aar		n
5		7	7	999	aar		n
6		7	7	999	aar		n
7		7	7	999	aar		n
79		5	5	10	aar		n
8		7	7	999	aar		n
9		7	7	999	aar		n

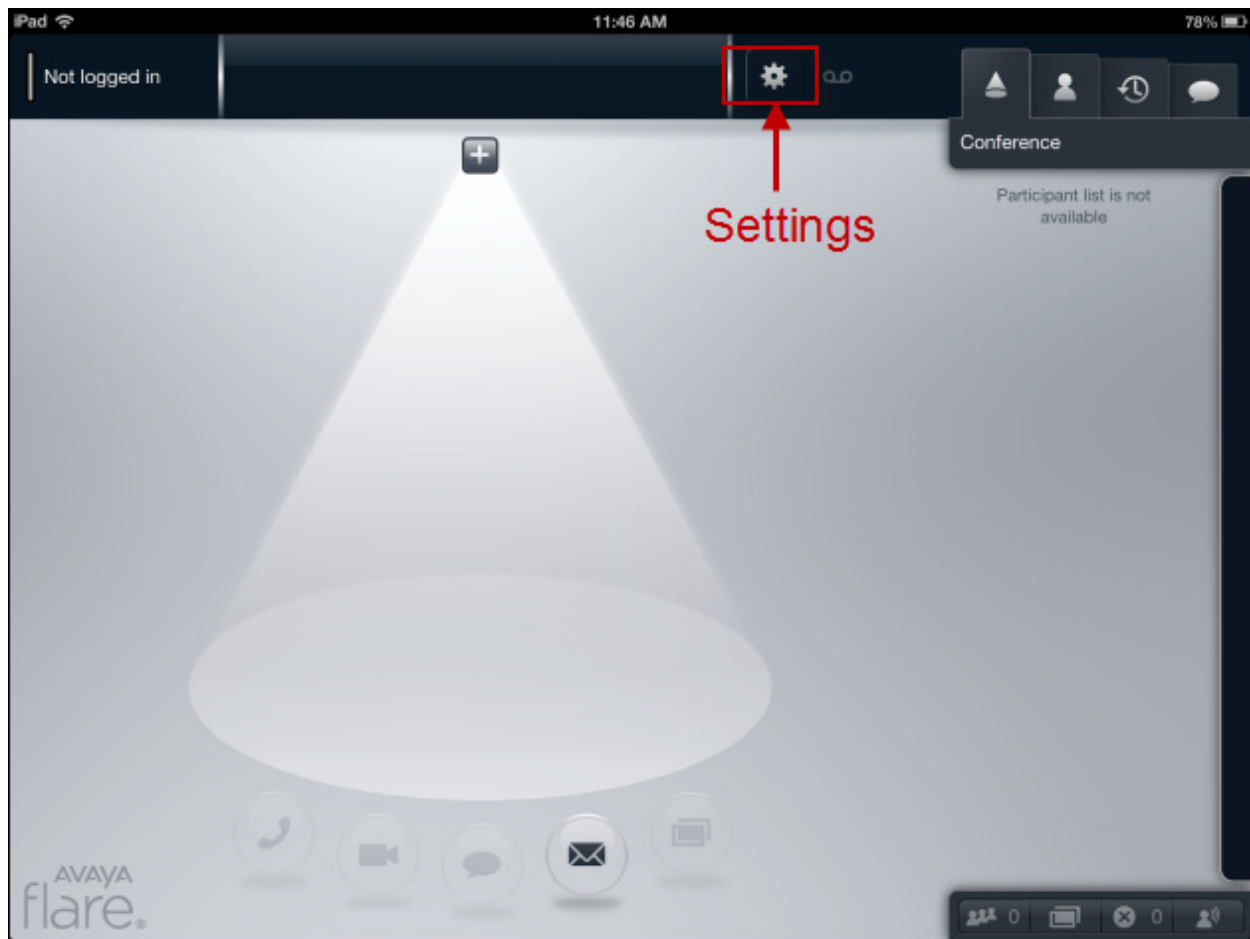
5.12. Administer Routing Pattern

This screen describes the **Route Pattern** form setup for the Flare Experience on iPad on Communication Manager. Route Pattern sends the call out trunk **10**.

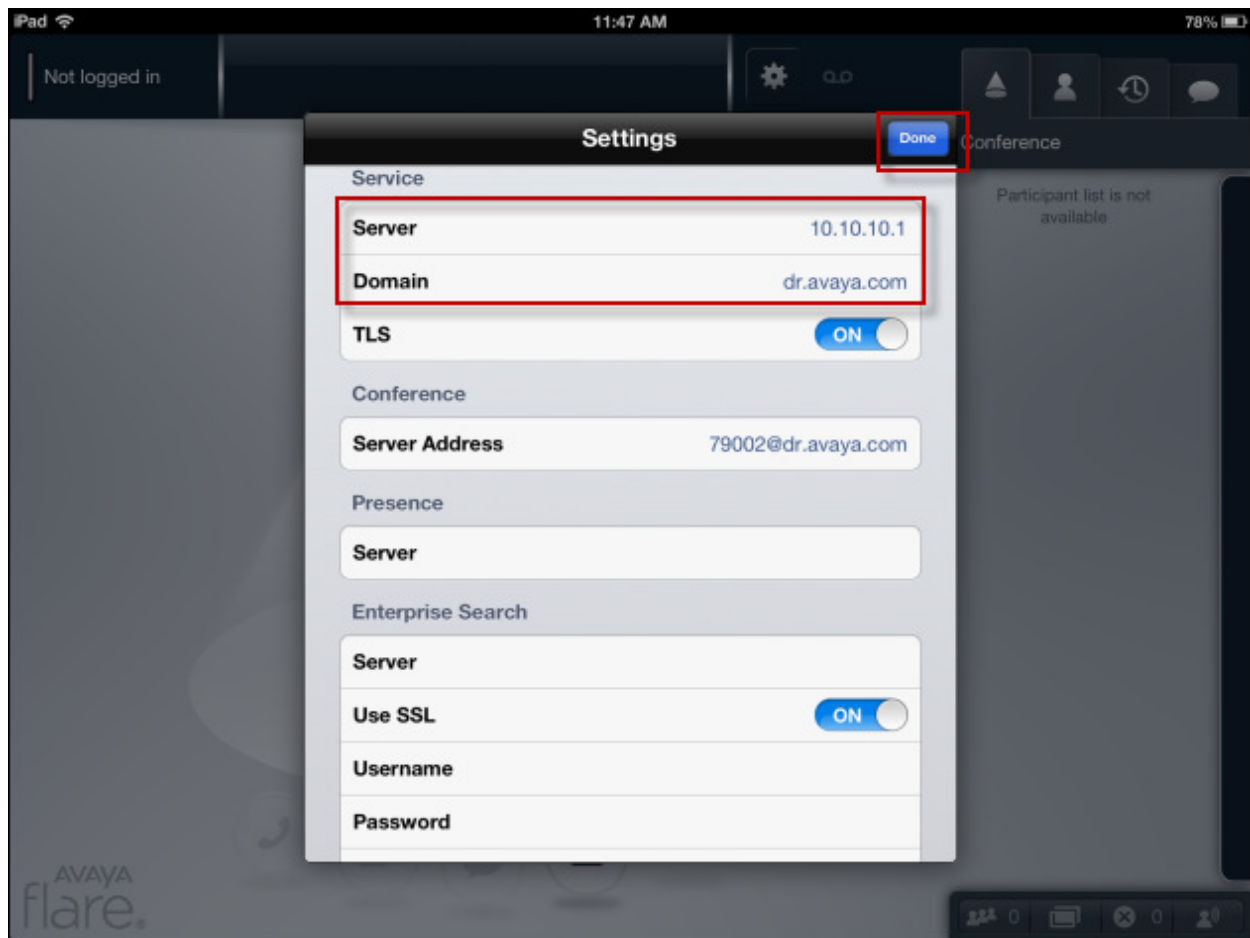
display route-pattern 10														Page 1 of 3							
Pattern Number: 10 Pattern Name: Route 2 silasm3																					
SCCAN? n Secure SIP? n																					
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted							DCS/	IXC						
No			Mrk	Lmt	List	Del	Digits							QSIG							
														Intw							
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. It's not required to fill in the rest of the values. Press **Done** when finished. The main Flare Experience screen will be displayed again as in the previous screen.



Press on **Not logged in** 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 **Log In**.



7. Verification Steps

The following three 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 and video 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, audio Mute/unMute, video Mute/unMute, and long call duration 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 6.3

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

User Registrations

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

View: Default Force Unregister ANI Device Notification: Reboot Rebuild Failback As of 12:22 PM

1 item: Refresh Refresh Show All

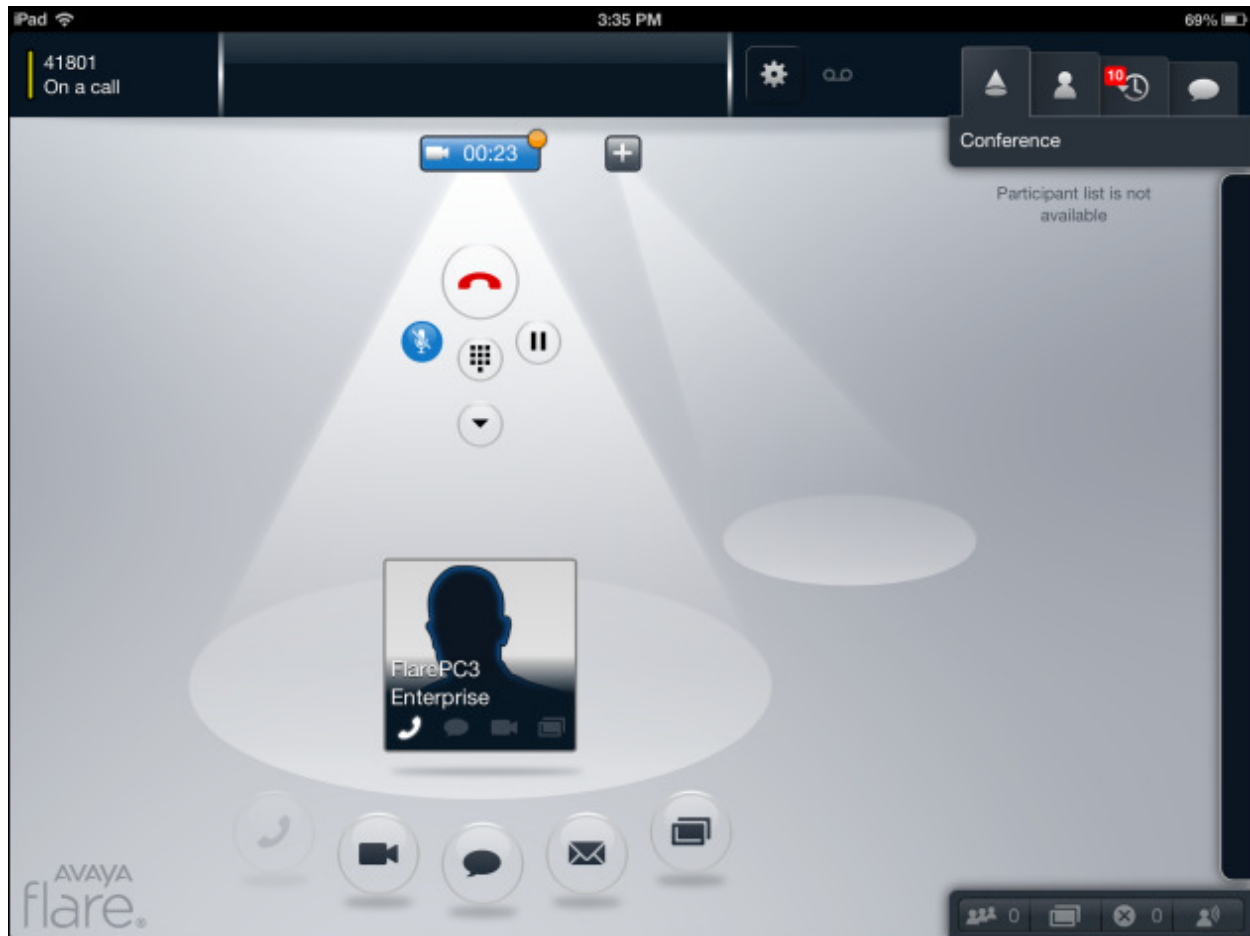
Details	Address	First Name	Last Name	Actual Location	IP Address	Resource Office	Shared Control	Simult. Devices	AXT Device	Registered
<input type="checkbox"/>	41801@dr.avaya.com	STL iPad	Experience		10.10.10.120001	E1	E1	4/4	M	<input checked="" type="checkbox"/> (Yes)

Select: All, None

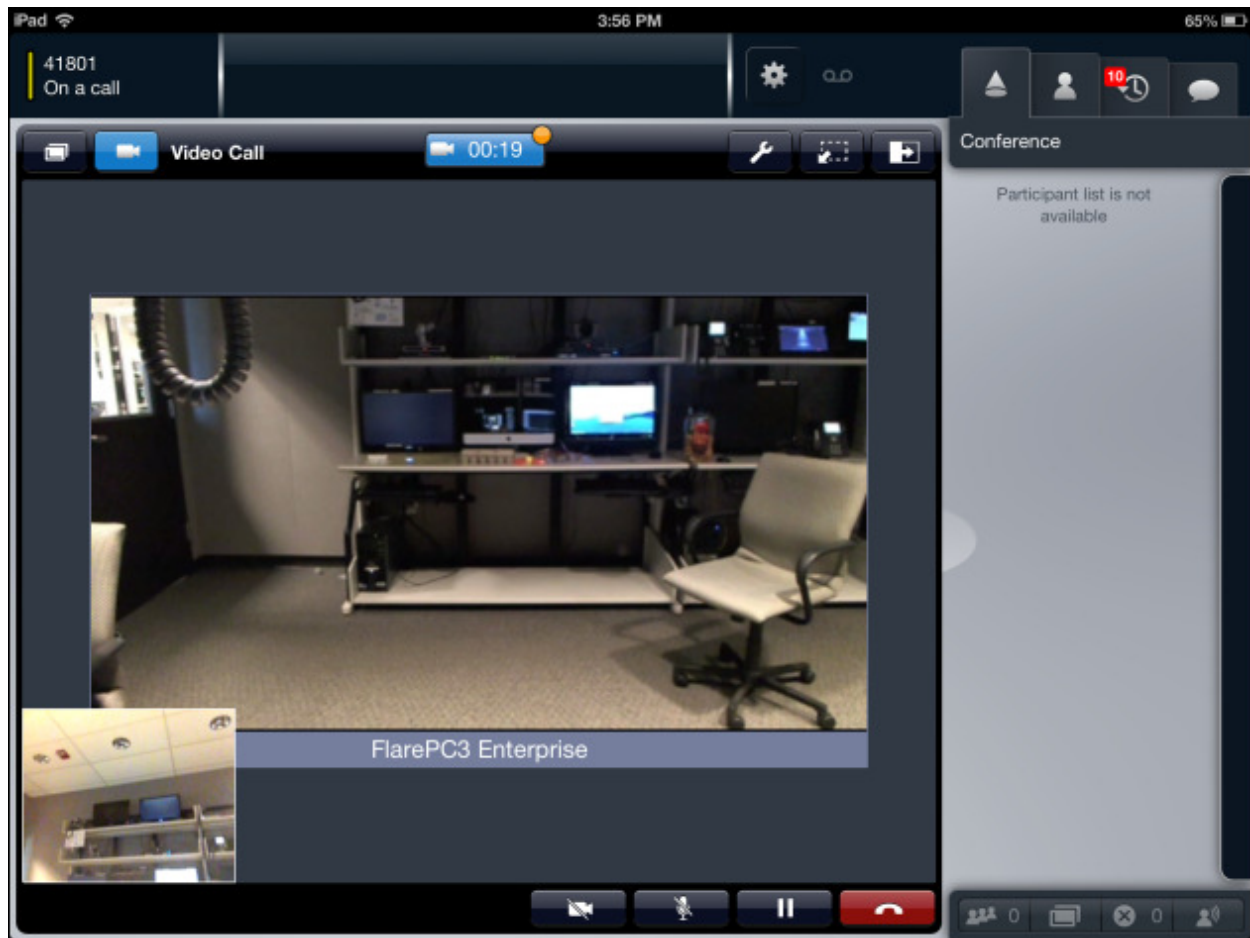
On the top left hand corner of the screen below the extension **41801** verify **Logged in** is displayed. This means that the Flare Experience is now logged in and is able to make/receive audio and video phone calls. Notice the other icons displayed including Collaboration, and the Conference tab in the upper right hand corner, 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 screens below, a successful audio/video call was made from the Flare Experience on iPad. This is what Flare Experience looks like when active on a video call with the video window minimized, similar to an audio only call.



This is what Flare Experience looks like when active on a video call and the video window is open.



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/video call.

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

9. Additional References

This section references the product documentation relevant to these Application Notes. All Avaya documents are available at <http://support.avaya.com>.

Avaya Aura® Session Manager

1. Avaya Aura® Session Manager Overview, Doc ID 03-603323
2. Installing and Configuring Avaya Aura® Session Manager
3. Avaya Aura® Session Manager Case Studies
4. Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325
5. Administering Avaya Aura® Session Manager, Doc ID -3-603324

Avaya Aura® Communication Manager

6. Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479
7. Administering Avaya Aura® Communication Manager, Doc ID 03-300509
8. Avaya Aura® Communication Manager Software and Firmware Compatibility Matrix

Avaya Flare Experience

9. Avaya Flare® Overview and Planning Avaya, Doc ID: 18-603948, Issue 3
10. Administering Avaya Flare® Experience for iPad Devices, Doc ID: 18-604079, Issue 1
11. Implementing Avaya Flare® Experience for iPad Devices, Doc ID: 18-604078, Issue 1

©2013 Avaya Inc. All Rights Reserved.

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

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