



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya IP Office 9.0 with Avaya Aura® 6.2 FP2 for Unified Communication Solution - Issue 1.0

Abstract

These Application Notes present a sample configuration of Avaya Aura® System Manager centrally managing Avaya IP Office 9.0 for administration and maintenance tasks as well as providing centralized call routing amongst the Headquarters and Branch locations using Avaya Aura® Session Manager 6.2 FP2.

This solution proposes to use Avaya Aura® System Manager, Avaya Aura® Session Manager and the associated centralized Aura® Applications, utilizing a direct WAN connection between the Headquarters and Branch site locations.

In case of a WAN outage, IP Office 9.0 provides survivability for Centralized SIP users and it uses PSTN trunks to provide features like Voicemail, Conferencing and others.

Table of Contents

1.	Introduction.....	4
2.	Interoperability Testing.....	5
2.1.	Centralized Administration, Management and Maintenance of Branch Solution	5
2.2.	Call Scenarios for Distributed, Mixed & Centralized Branch Deployment.....	6
2.3.	Test Results and Observations	7
3.	Reference Configuration	7
3.1.	Solution Configuration	8
3.2.	Network Configuration	9
3.3.	Dial plan Configuration.....	9
3.4.	Signaling and Media Parameters Configuration	11
4.	Equipment and Software Validated	12
5.	Assumptions.....	12
6.	Configure Avaya Aura® Communication Manager.....	13
6.1.	Configure System Parameters	13
6.2.	Configure Feature Access Codes	14
6.3.	Configure IP Network Region.....	15
6.4.	Configure IP Codec Set.....	16
6.5.	Configure Node-Names.....	16
6.6.	Configure Signaling Group	17
6.7.	Configure Trunk Group.....	18
6.8.	Configure Route Pattern.....	18
6.9.	Configure Automatic Alternate Routing Analysis	19
7.	Configure Avaya Aura® Session Manager	19
7.1.	Configure SIP Domain	21
7.2.	Configure SIP Entities.....	21
7.3.	Configure Entity Links.....	23
7.4.	Configure Routing Policy.....	25
7.5.	Configure Dial Patterns.....	26
8.	Configure Avaya IP Office	27
8.1.	Access IP Office ICU (Initial Configuration Utility).....	27
8.2.	Configure IP Office Element on System Manager.....	29
8.3.	Synchronizing IP Office System Configuration and Users with System Manager.....	30
8.4.	Launch IP Office Manager via System Manager	31
8.4.1.	IP Office License Configuration.....	31
8.4.2.	Configure Codec Preference.....	32
8.4.3.	Configure Voicemail	33
8.4.4.	Configure SM Line	33
8.4.5.	Configure ARS for SM Line	35
8.4.6.	Configure Incoming Call Route	36
8.5.	Configure Centralized SIP Users for IP Office Branch Using System Manager	39
8.6.	Configure H.323 User for IP Office branch using System Manager	43
9.	Configure Avaya Aura® Messaging	45
9.1.	Configure Entity	45
9.2.	Configure Entity Links.....	45

9.3.	Configure Routing Policy.....	46
9.4.	Configure Dial Pattern	47
9.5.	Configure Messaging Profile to User.....	48
10.	Configure Avaya Aura® Conferencing.....	49
10.1.	Configure Entity	49
10.2.	Configure Entity Links	49
10.3.	Configure Routing Policy	50
10.4.	Configure Dial Pattern.....	51
10.5.	Configure Conferencing profile to user.....	52
11.	Verification Steps	53
11.1.	Verify Avaya Aura® Session Manager Configuration	53
11.2.	Verify SIP Entity Link Status	53
11.3.	Verify Registrations of SIP Endpoints	54
11.4.	Verify IP Office System Status	54
11.5.	Verify IP Office WebLM Connectivity.....	55
11.6.	Verify Call Scenarios.....	55
12.	Conclusion	56
13.	Additional References.....	57

1. Introduction

These Application Notes present a sample configuration of Avaya Aura® System Manager centrally managing IP Office 9.0 for administration and maintenance as well as provide call routing and unified communication applications amongst the Headquarters (HQ) and multiple branches locations deployed in Centralized, Distributed and Mixed mode through Avaya Aura® Session Manager 6.2 FP2.

Important components of this solution are:

IP Office 9.0 serving as the basic Telephony interface for IP and other phones in the branch and Unified Communication services like Messaging and Conferencing from Headquarters in Sunny-Day and providing survivability with limited features for Centralized SIP phone users at branch in Rainy-Day.

Avaya Aura® System Manager 6.2 FP2 provides centralized administration and maintenance capabilities for up-to 2000 IP Office 9.0 branches.

Avaya Aura® Session Manager 6.2 FP2 provides centralized & distributed call routing capabilities amongst the HQ and branch locations including Centralized Unified Communication applications like Messaging and Conferencing.

Avaya Aura® Messaging 6.2 provides a centralized Voice Mail system for HQ and branch users.

Avaya Aura® Conferencing 7.2 provides Audio/Video & Web Collaboration for Centralized SIP users and a bridge conferencing solution for all phones across HQ and branch locations.

2. Interoperability Testing

2.1. Centralized Administration, Management and Maintenance of Branch Solution

This section focuses on Centralized Control of Avaya Aura® 6.2 FP2 and all the IP Office 9.0 Branches using System Manager.

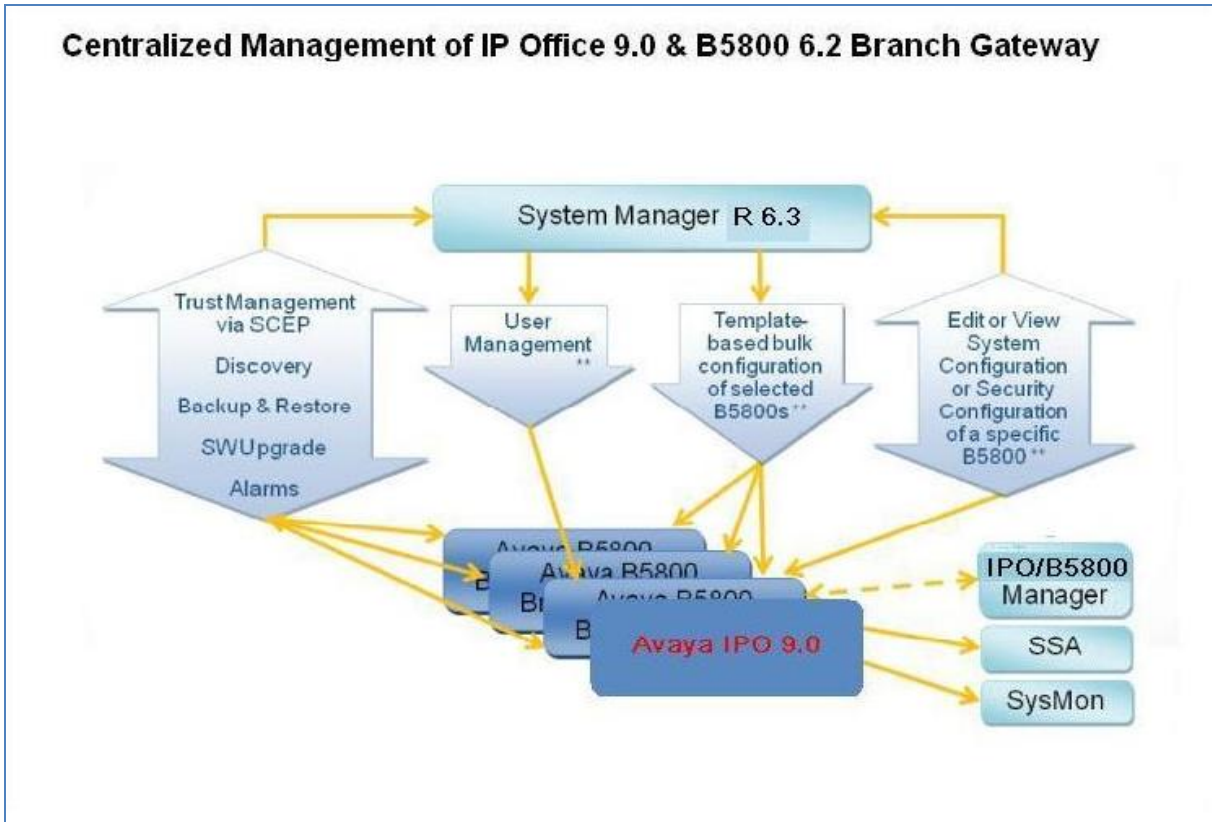


Figure 1: Centralized Management Configuration

- Centralized Administration of System level parameters for IP Office 9.0 through System Manager.
- Centralized Administration of Headquarter and Branch users through System Manager.
- Centralized Administration of Voice Mail for Headquarter and Branch users through System Manager.
- Centralized Administration of Conferencing for Headquarter and Branch users through System Manager.
- Bulk Administration of Headquarter and Branch users through System Manager .
- Centralized Administration of WebLM license services for IP Office.
- Centralized Maintenance Services for backup, restore & software upgrades through System Manager

- Remote Maintenance of solution through SAL Gateway Integration.

2.2. Call Scenarios for Distributed, Mixed & Centralized Branch Deployment

This section focus on Unified Communication (UC) features between the HQ location and different IP Office branch locations for Sunny-Day scenarios. The HQ location has Avaya Aura® 6.2 FP2 Core and UC Applications. The Branch locations have IP Office 9.0 deployed in a Distributed, Mixed and Centralized mode configuration. Both HQ and Branch location have PSTN connectivity for external incoming and outgoing calls.

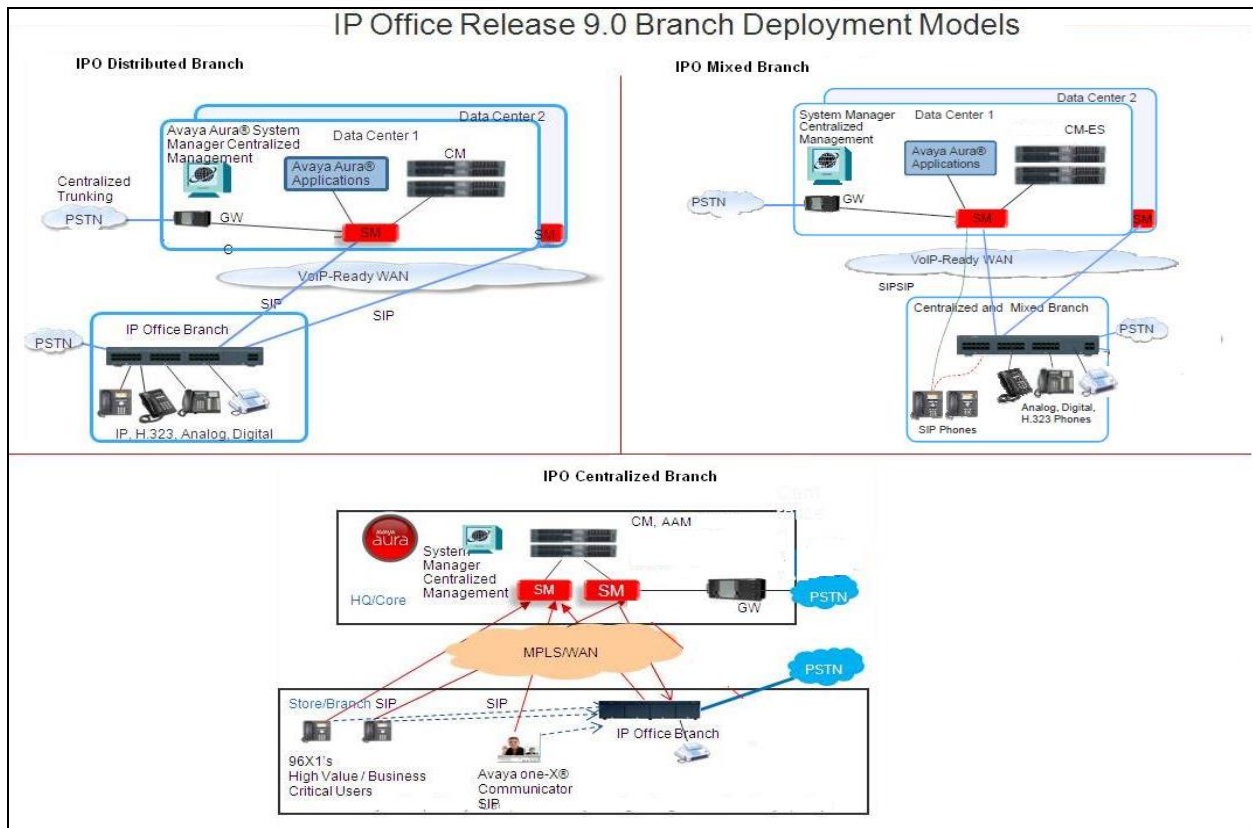


Figure 2: UC Branch Deployment Configuration Models

- End-Point “Basic” and “Supplemental” call features
- Local Branch PSTN Trunk Services
- Centralized and Distributed Call Routing for PSTN and SIP Trunk Services
- Centralized Services and Applications
 - Conferencing Features - Bridge, Ad-Hoc, Web conference.
 - Messaging Features - Voice Mail, Message Waiting Indicator (MWI), Find Me, Notify Me.

2.3. Test Results and Observations

The following administrative and maintenance tasks were successfully tested:

- Centralized administration of System & User templates
- Centralized Administration of SIP, H.323, Digital and Analog users.
- Centralized WebLM Service for Avaya Aura® and IP Office applications.
- Centralized Maintenance services like Backup, Restore and Software Upgrades.

The following call flows were successfully tested in **Sunny-Day**:

- Basic telephony features like, Hold, Transfer, Conference
- Avaya Aura® Messaging features like Voice Mail, MWI, Find Me and Notify.
- Avaya Aura® Conferencing features like Audio, Video, Web Collaboration for Bridge and Ad-Hoc Conferences.
- TCP/TLS for Signaling.
- RTP/SRTP for Media.
- G.711A, G.711Mu, G.729 for codec.

The following call flows were successfully tested in **Rainy-Day**:

- Basic Telephony features like, Hold, Transfer, Conference
- Avaya Aura® Messaging Voice Mail via PSTN trunk
- Avaya Aura® Conferencing Audio Conferencing via PSTN trunk

Limitations:

- Bulk Administration of users and system parameters for 2000 branch locations needs to be performed in smaller batches, for more details see **Section 13**
- Maintenance Services for 2000 branch locations like Synchronization, Back up, Restore, Upgrade needs to be performed in smaller batches, for more details see **Section 13**
- Media Encryption should be configured consistently on Avaya Aura® Communication Manager, and central Avaya Aura® Communication Manager Media Gateway, Avaya Aura® Session Manager, IP Office, and the Centralized SIP phone otherwise users will hear noise in case SRTP/RTP shuffling happens.
- MWI does not work on Centralized ATA 6219 phone.
- **In Rainy-Day:**
 - MWI does not work.
 - Centralized SIP users will not be able to use Ad-Hoc Conferencing features.
 - HQ user needs to dial a prefix to reach branch users via PSTN as Dial Plan Transparency is not supported on Avaya IP Office 9.0
 - For seamless dialing amongst the branch and HQ locations to work Direct Inward dialing (DID) should be provided by the PSTN trunk provider.

3. Reference Configuration

Following sub section describes the solution, network, dial plan and signaling overview used in sample configuration.

3.1. Solution Configuration

HQ location consists of Avaya Aura® Core and Unified Communication (UC) Applications deployed at two separate Data Centers to provide High Availability, Disaster Recovery enabled services for users.

In the sample configuration four branch locations were configured that consist of Avaya IP Office 9.0 deployed in Distributed, Mixed and Centralized mode.

Centralized and Mixed Branch: All the Centralized SIP & Centralized ATA Analog endpoints (Connected to IP Office 500 v2) registered to Avaya Aura® Session Manager in Sunny-Day. For Rainy-Day scenarios the endpoints would registered to IP Office Branch for survivability.

Mixed and Distributed branch: All H.323, Digital and Analog phones were registered to IP Office and use centralized applications located within the HQ via Avaya Aura® Session Manager in Sunny-Day. For Rainy-Day scenarios, the PSTN trunk was used to reach HQ and other branch locations

WebLM license server hosted on System Manager was used to provide licensing for Avaya Aura® Core Applications and IP Office.

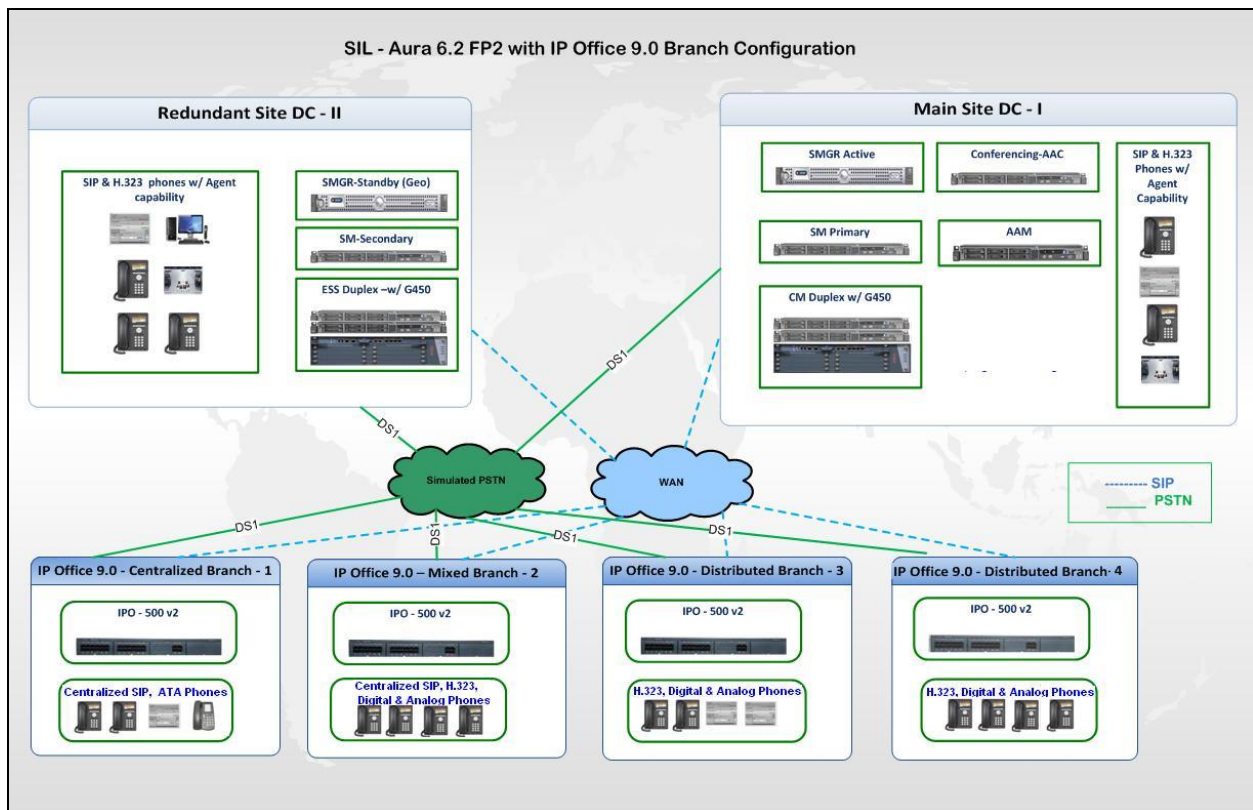


Figure 3: Solution Configuration

3.2. Network Configuration

The network for the primary and secondary Data Center was configured using multi-vendor VLAN based architecture.

Network of all the branches consist of Avaya SR2330 Branch Router and Avaya Switches providing Local Network and DHCP Services for Branch Phones and Computers.

The Network Connectivity across Data Centers and multiple branch locations was configured using Open Shortest Path First (OSPF) Routing Protocols through a centralized Avaya SR4134 Router.

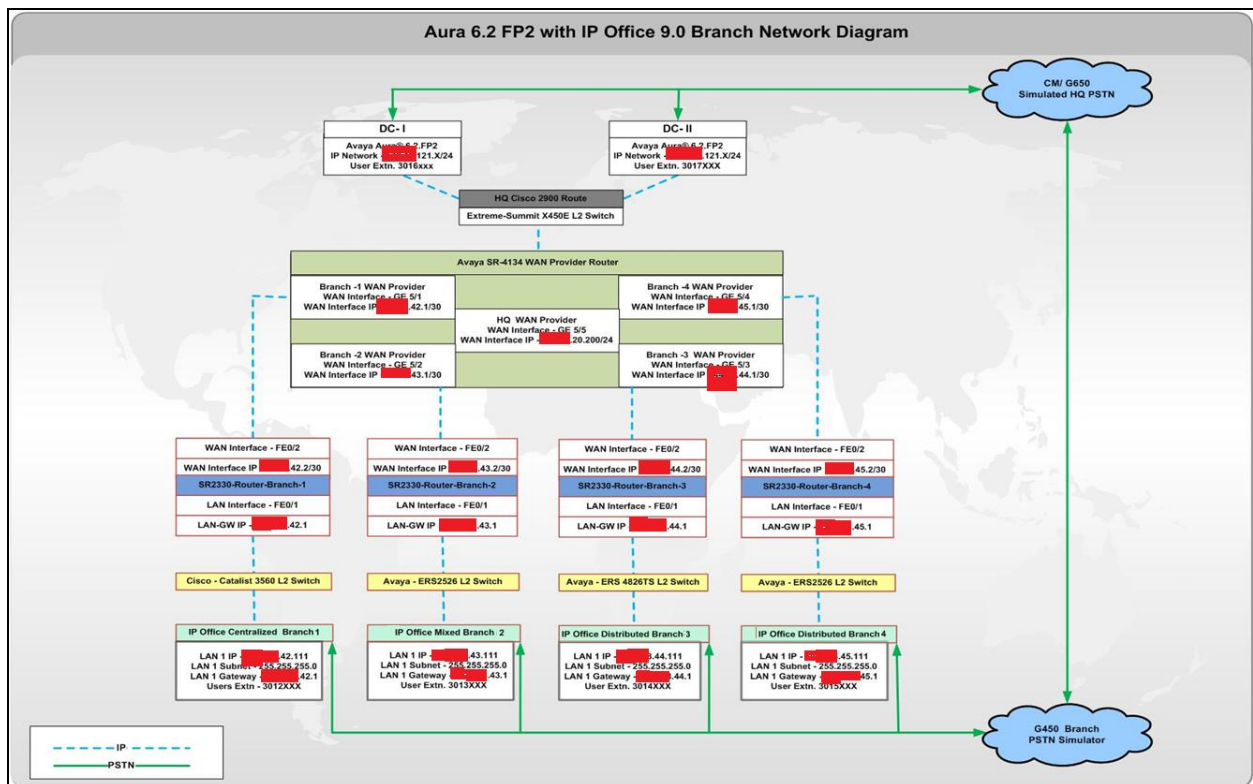


Figure 4: Network Configuration

3.3. Dial plan Configuration

Centralized dial plan was configured to access applications like messaging and conferencing as well as to reach users across HQ and branch locations.

Seven digit access code was configured for Unified Applications and Users across locations. At the HQ location, the prefix “9” was used for Avaya Aura® Communication Manager Automatic Route Selection (ARS) to access the PSTN trunk to reach IP Office Branch users. At the Branch location, the prefix “99” was used for IP Office ARS to access the PSTN trunk to reach HQ users and centralized applications.

Note: In the sample configuration **Incoming call treatment** feature was used on a simulated PSTN server (Avaya Aura® Communication Manager) to remove the prefix before forwarding to HQ or Branch IP Office.

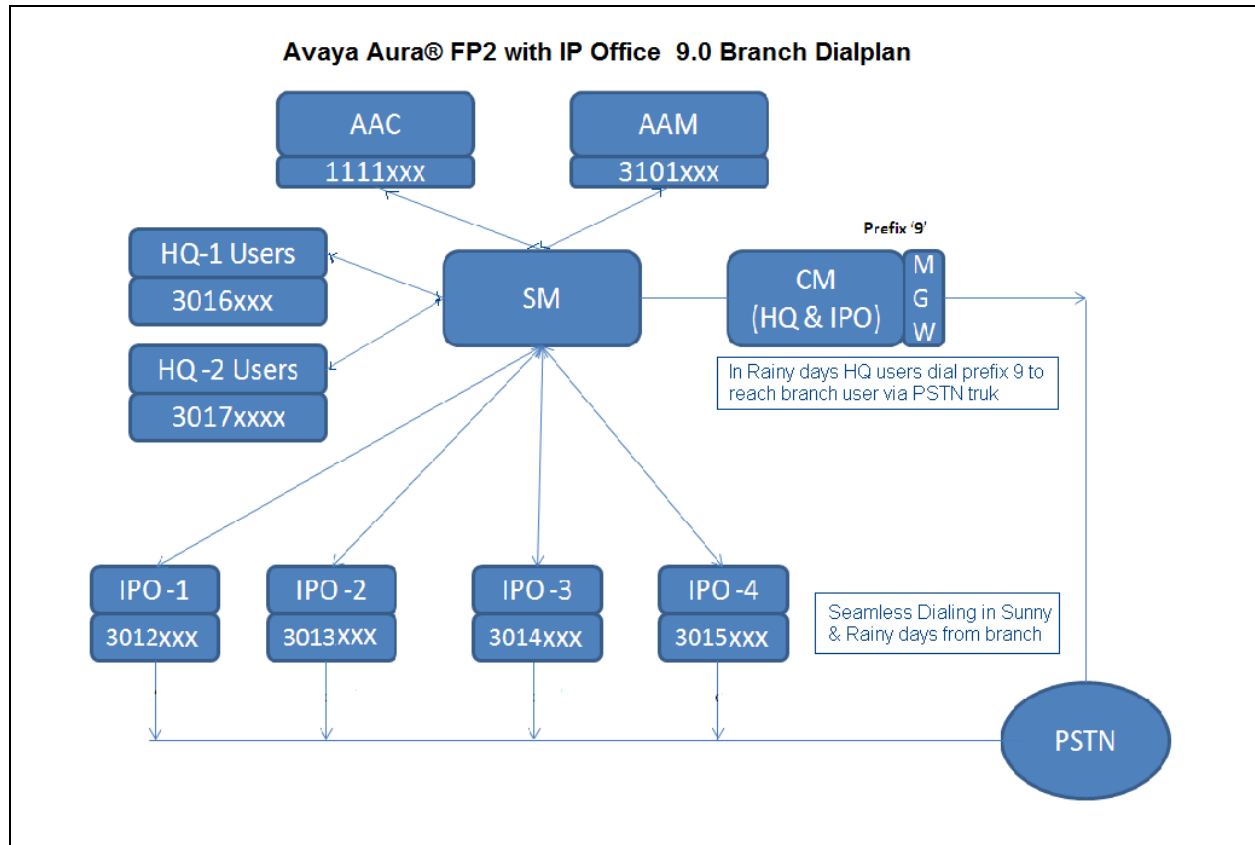


Figure 5: Dialplan Configuration

In Sunny-Day:

- Voice Mail access code from all locations - 3101000
- Bridge Conference access code from all locations - 1111001
- HQ DC-I users access code – 3016xxx
- HQ DC-II users access code – 3017xxx
- Branch 1 users (Centralized SIP & ATA) access code – 3012xxx
- Branch 2 users (Centralized SIP & ATA, H.323 & Digital) access code – 3013xxx
- Branch 3 users (H.323, Digital & Analog) access code – 3014xxx
- Branch 4 users (H.323, Digital & Analog) access code – 3015xxx

In Rainy-Day:

- Voice Mail access code from branch – 3101000
- Bridge Conference access from branch – 1111001
- HQ DC-I users access code from branch – 3016xxx
- HQ DC-II users access code from branch – 3017xxx

- Branch 1 users access code from DC-I & DC-II – 9-3012xxx
- Branch 2 users access code from DC-I & DC-II– 9-3013xxx
- Branch 3 users access code from DC-I & DC-II – 9- 3014xxx
- Branch 4 users access code from DC-I & DC-II – 9-3015xxx

3.4. Signaling and Media Parameters Configuration

Signaling rule “**TLS with SIPS**” was configured on all SIP trunks and users to provide end-to-end signaling level security.

Media Security rule “**Best effort**” was configured on Communication Manager and IP Office branch to provide media security for supported endpoints.

Codec set **G.711A, G.711Mu, and G.729** was configured at endpoints, IP Office, Communication Manager, Messaging, and Conferencing Servers.

4. Equipment and Software Validated

The following components were used for the sample configuration:

Component	Software/Firmware
VMWare ESXi 5.0.1 with vCenter 5.1 OVA	Avaya Aura® System Manager 6.3 (Build No 6.3.3.5.1829)
	Avaya Aura® Session Manager 6.3.2.0.632023
	Avaya Aura® Communication Manager (Evolution Server) R016x.03.0.124.0
Avaya S8800 Server	Avaya Aura® Messaging 6.2 Build MSG-02.0.823.0-109_0202
Avaya S8800 Server	Avaya Aura® Conferencing 7.2
Avaya IP Office IP500 V2	Avaya IP Office 9.0 Build 9.0.0.829
Avaya 96x1 –SIP Series IP Telephones	96x1 SIP Build 6.2.2.16
Avaya 96x1 –H.323 Series IP Telephones	96x1H.323 Build 6.3.r61
one-X® Communicator –SIP at Branch	6.1 Build 6.1.6.18-CI-11
Avaya Flare Experience for Windows	1.1 Build 1.1.1.7
Avaya Flare Experience for iPad	1.1 Build 1.1.9
Avaya 6219 Analog Telephone	-
Avaya 9400 Digital Telephone	-
HTTPS/HTTP Phone Configuration File Server	Windows Server 2003 SP2 for Enterprise

Table 1 – Software/Hardware Version Information

5. Assumptions

It is assumed that Avaya Aura® System Manager, Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, Avaya Aura® Conferencing are installed and configured to work in the above sample Unified Communication solution.

6. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring a skill-enabled hunt group & call routing on Avaya Aura® Communication Manager in the HQ location. The System Access Terminal (SAT) is used to issue the commands.

- Configure System Parameters
- Configure Feature Access Codes
- Configure IP Network Region
- Configure IP Codec Set
- Configure Node-Names
- Configure Signaling Group
- Configure Trunk Group
- Configure Route Pattern
- Configure Automatic Alternate Routing Analysis

6.1. Configure System Parameters

For unlicensed features, contact an authorized Avaya account representative to obtain the licenses.

On Page 2 of the system parameters customer-options form, verify that there are sufficient licenses for SIP trunks.

```
display system-parameters customer-options                               Page  2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 1199
      Maximum Concurrently Registered IP Stations: 18000 41
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414  0
      Max Concur Registered Unauthenticated H.323 Stations: 100  0
      Maximum Video Capable Stations: 18000 6
      Maximum Video Capable IP Softphones: 18000 456
      Maximum Administered SIP Trunks: 24000 4278
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 18
      Maximum Number of DS1 Boards with Echo Cancellation: 522  0
      Maximum TN2501 VAL Boards: 128  1
      Maximum Media Gateway VAL Sources: 250  1
      Maximum TN2602 Boards with 80 VoIP Channels: 128  0
      Maximum TN2602 Boards with 320 VoIP Channels: 128  5
      Maximum Number of Expanded Meet-me Conference Ports: 300  0

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

6.2. Configure Feature Access Codes

This section describes the steps for configuring Feature Access Codes (FAC) for Auto Alternate Route (AAR) for call routing and Automatic Call Distribution (ACD).

Enter **change feature-access-codes** command. Enter FACs that are valid under the provisioned dialplan for the following highlighted fields on Page 1 and Page 5.

change feature-access-codes		Page 1 of 11
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:	*31	
Abbreviated Dialing List2 Access Code:	*32	
Abbreviated Dialing List3 Access Code:	*33	
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:	*30	
Answer Back Access Code:	*14	
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code:	8	
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2:
Automatic Callback Activation:	*18	Deactivation: #18
Call Forwarding Activation Busy/DIA:	All:	Deactivation:
Call Forwarding Enhanced Status:	*21 Act: *11	Deactivation: #11
Call Park Access Code:	*15	
Call Pickup Access Code:	*12	
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation:		Deactivation:
Contact Closure Open Code:		Close Code:

change feature-access-codes		Page 5 of 11
FEATURE ACCESS CODE (FAC)		
Call Center Features		
AGENT WORK MODES		
After Call Work Access Code:	*73	
Assist Access Code:		
Auto-In Access Code:	*72	
Aux Work Access Code:	*71	
Login Access Code:	*88	
Logout Access Code:	*75	
Manual-in Access Code:	*70	
SERVICE OBSERVING		
Service Observing Listen Only Access Code:	*91	
Service Observing Listen/Talk Access Code:	*92	
Service Observing No Talk Access Code:	*93	
Service Observing Next Call Listen Only Access Code:	*99	
Service Observing by Location Listen Only Access Code:		
Service Observing by Location Listen/Talk Access Code:		

6.3. Configure IP Network Region

Enter **change ip-network-region X** command, where **X**, is the available network region.

- **Region:** 1, default network-region
- **Authoritative Domain:** Specify the name or IP address of the SIP domain for this network region. In the sample configuration, domain name is mentioned as **sol001.fst.silpunelab.com**.
- **Name:** Specify network region name (optional)
- **Codec Set:** Specify the codec set number assigned to the region. In the sample configuration, codec set number is set to default value **1**.

Default values can be used for the remaining fields.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1 Authoritative Domain: sol001.fst.silpunelab.com
Name: FP2 Stub Network Region: n
MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes
Codec Set: 1 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? y
UDP Port 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
```

6.4. Configure IP Codec Set

Enter **change ip-codec-set X** command where **X**, is the codec set number mentioned on the IP-Network-Region form in **Section 6.3**

```
change ip-codec-set 1                                     Page 1 of 2

IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression    Per Pkt     Size (ms)
1: G.711A   n                     2           20
2: G.711MU  n                     2           20
3: G.729    n                     2           20
4:          -                     -
5:          -                     -
6:          -                     -
7:          -                     -

Media Encryption
1: 1-srtp-aescm128-hmac80
2: none
3: 
```

6.5. Configure Node-Names

Enter **change node-names ip** command, to configure node name for Avaya Aura® Session Manager IP Address.

```
change node-names ip fp2-sm01                             Page 1 of 2

IP NODE NAMES

Name      IP Address
fp2-sm01  [REDACTED]
fp2-sm02  [REDACTED]
```

Verify that IP Address of '**procr**' is available in the node-name table by default.

```
change node-names ip procr                                Page 1 of 2

IP NODE NAMES

Name      IP Address
procr     [REDACTED]
[REDACTED]
```


6.6. Configure Signaling Group

Enter command **add signaling X**, where **X** is an available signaling group number and configure highlighted details as below. Default values can be used for the remaining fields.

- **Group Type:** sip
- **Transport Method:** tls
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name as defined in **Section 6.5** for Session Manager with IP xx.xx.121.15
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Network Region:** 1
- **Far-end Domain:** sol001.fst.silpunelab.com (SIP Domain) name for which the far-end proxy is responsible (i.e. Authoritative)
- **Initial IP-IP Direct Media:** y

```
change signaling-group 1                                     Page 1 of 2
SIGNALING GROUP
Group Number: 1
IMS Enabled? n
Q-SIP? n
IP Video? y
Peer Detection Enabled? y
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Group Type: sip
Transport Method: tls
Priority Video? y
Enforce SIPS URI for SRTP? y
Peer Server: SM
Near-end Node Name: procr
Near-end Listen Port: 5061
Far-end Node Name: fp2-sm01
Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Secondary Node Name:
Far-end Domain: sol001.fst.silpunelab.com
Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? y
Initial IP-IP Direct Media? y
Alternate Route Timer(sec): 6
Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Enable Layer 3 Test? y
H.323 Station Outgoing Direct Media? n
```

Repeat the above steps to configure **signaling group 2** for the secondary Session Manager.

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group x** command, where **x** is an available trunk group number and fill in the following fields.

- ```
change trunk-group 1 Page 1 of 22
```
- ```
TRUNK GROUP
```
- ```
Group Number: 1 Group Type: sip CDR Reports: y
```
- ```
Group Name: To-SM01 COR: 1 TN: 1 TAC: #001
```
- ```
Direction: two-way Outgoing Display? n Night Service:
```
- ```
Dial Access? n Queue Length: 0
```
- ```
Service Type: tie Auth Code? n
```
- ```
Member Assignment Method: auto
```
- ```
Signaling Group: 1
```
- ```
Number of Members: 255
```

Configure a route pattern corresponding to the newly added SIP trunk group. Use **change route pattern X** command, where **X** is an available route pattern number. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

18 of 59
IPO9AA62FP2UCBR

6.9. Configure Automatic Alternate Routing Analysis

Automatic Alternate Routing (AAR) is used for routing calls with starting dialed digits 301 to Session Manager.

Note: Other methods of routing may be used.

Enter **change aar analysis 3** command and add an entry to specify how to route the calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **301**
- **Total Min:** Minimum number of digits, in this case **7**
- **Total Max:** Maximum number of digits, in this case **8**
- **Route Pattern:** route pattern number configured in the above step
- **Call Type:** aar

change aar analysis 3							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all					Percent Full: 1			
Dialed	Total		Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
301	7	8	1	aar		n		

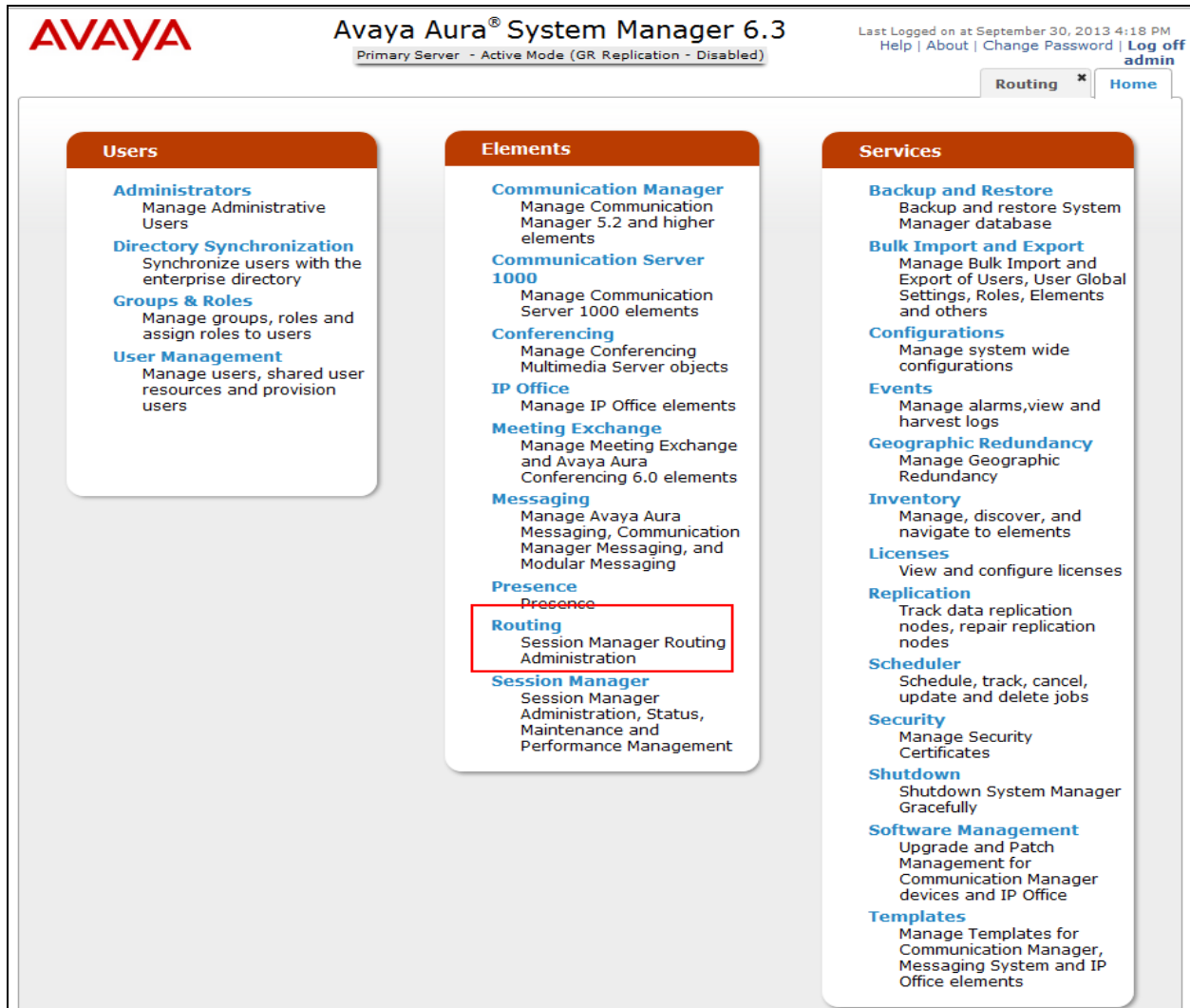
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager as provisioned in the sample configuration.

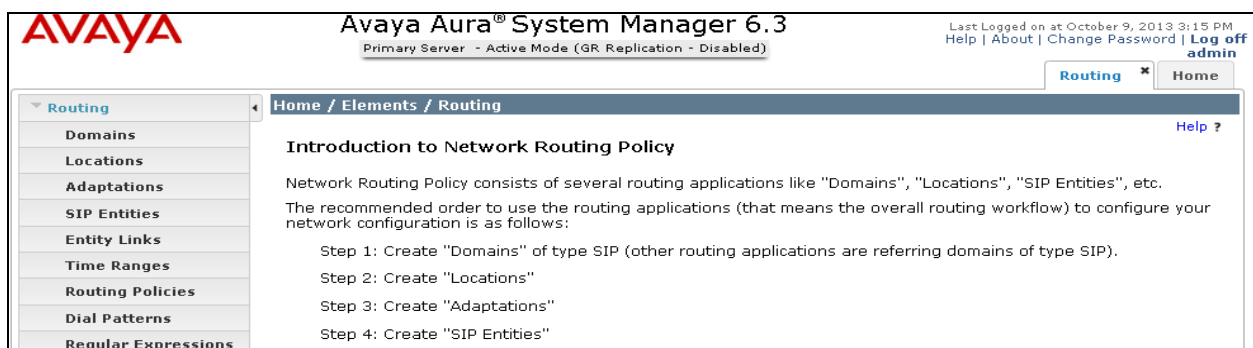
The procedures described in this section include configurations in the following areas:

- Configure SIP domain
- Configure SIP Entities corresponding to the SIP telephony systems including Communication Manager, Avaya IP Office and Session Manager itself
- Configure Entity Links which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Configure Routing Policies which controls call routing between the SIP Entities
- Configure Dial Patterns specifying the dial digit strings for Routing Policies

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL; **http://<ip-address>/SMGR** where <ip-address> is the IP address of System Manager. Log in to the system with valid credentials. The menu shown below is displayed. Select the **Routing** link from the home page of System Manager.



The screenshot shows the Avaya Aura System Manager 6.3 home page. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.3", and status information: "Primary Server - Active Mode (GR Replication - Disabled)". On the right, it shows the last login time "September 30, 2013 4:18 PM" and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there are three main sections: "Users", "Elements", and "Services". The "Elements" section is highlighted with a red box around the "Routing" link, which is labeled "Session Manager Routing Administration".



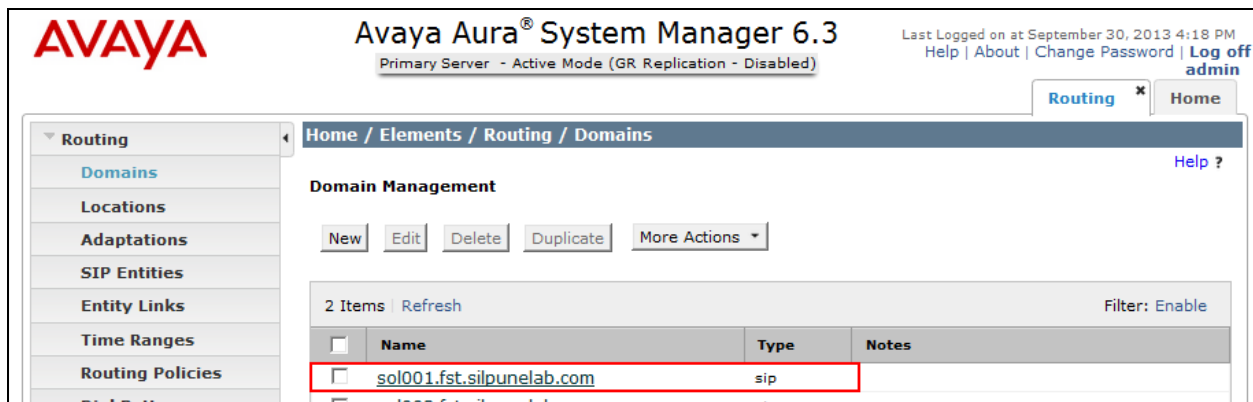
The screenshot shows the "Routing" page in the Avaya Aura System Manager 6.3 GUI. The left sidebar contains a list of navigation links: "Routing", "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", and "Regular Expressions". The main content area is titled "Introduction to Network Routing Policy" and provides an overview of the routing applications. It states: "Network Routing Policy consists of several routing applications like 'Domains', 'Locations', 'SIP Entities', etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:" followed by four steps: "Step 1: Create 'Domains' of type SIP (other routing applications are referring domains of type SIP).", "Step 2: Create 'Locations'", "Step 3: Create 'Adaptations'", and "Step 4: Create 'SIP Entities'".

7.1. Configure SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and click the **New** button on the right. Fill in the following:

- **Name:** The authoritative domain name matching the domain configuration on Communication Manager. This should be same as the authoritative domain name configured in **Section 6.6**
- **Notes:** Descriptive text (optional)

Click **Commit**.



7.2. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for Session Manager and Communication Manager at the HQ and Avaya IP Office branch location. Select **SIP Entities** on the left and click on the **New** button (not shown) on the right.

Under **General**:

- **Name** A descriptive name
- **FQDN or IP Address:** FQDN or IP address of Session Manager or the signaling interface on the telephony system
- **Type:** **Session Manager** for Session Manager;
CM for Communication Manager; **SIP Trunk** for Avaya IP Office
- **Adaptation:** Leave blank

Under **Port** (for adding Session Manager Entity only), click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests. Default TLS port is **5061**. Sample configuration uses a default TCP port.
- **Protocol:** Transport protocol to be used to send SIP requests
- **Default Domain:** Select the SIP Domain configured in **Section 7.1**

Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

The following screen shows the addition of Session Manager. The IP address of the SIP signaling interface is entered for **FQDN or IP Address**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. A red box highlights the 'Name' field (SM-1) and the 'FQDN or IP Address' field (redacted). Below this, the 'Type' is set to 'Session Manager'. The 'Notes' field is empty. Further down, the 'Location' is set to 'All', 'Outbound Proxy' is empty, 'Time Zone' is 'America/Fortaleza', and 'Credential name' is empty. The 'SIP Link Monitoring' section shows 'Link Monitoring Enabled' and monitoring intervals. The 'Entity Links' section shows a table with 4 items found.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
SM-1	TLS	* 5061	Daytona-FST-Bangalore-B5800-IPO-Branch-4	* 5061	trusted	<input type="checkbox"/>
SM-1	TLS	* 5061	Daytona-FST-Hyderabad-Branch2	* 5061	trusted	<input type="checkbox"/>
SM-1	TLS	* 5061	Daytona-FST-Kolkata-Branch-3	* 5061	trusted	<input type="checkbox"/>
SM-1	TLS	* 5061	Daytona-FST-Pune-Branch-1	* 5061	trusted	<input type="checkbox"/>

Repeat the above step to configure **SIP Entity** for the secondary Session Manager.

The following screen shows the results of adding Communication Manager. In this case, **FQDN or IP Address** is the **FQDN** of the PROCR interface of Communication.

Note: the **CM** selection for the field **Type**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. A red box highlights the 'Name' field (CM Duplex Main) and the 'FQDN or IP Address' field (fp2-cm001.sol001.fst.silpunelab.cor). Below this, the 'Type' is set to 'CM'. The 'Notes' field contains 'Main with fallback to ESS'. The 'Adaptation' field is empty, and the 'Location' is set to 'All'.

The following screen shows the results of adding Avaya IP Office for the sample branch. In this case, **FQDN or IP Address** is the IP address assigned to the Avaya IP Office.

Note: the **SIP Trunk** selection for field **Type**.

AVAYA Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled) Last Logg Help | About | Cha

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: Daytona-FST-Pune-Branch-1

* FQDN or IP Address: [Redacted]

Type: SIP Trunk

Notes: [Empty]

Adaptation: [Empty]

Location: Daytona-FST-Pune-Branch-1

7.3. Configure Entity Links

A SIP trunk between Avaya Aura® Session Manager and a telephony system is described by an Entity link. In the sample configuration, an Entity Link is configured between Session Manager and Communication Manger. Another Entity Link is created between Session Manager and Avaya IP Office.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager SIP Entity configured in **Section 7.2**
- **Protocol:** Select **TLS**
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select Communication Manager or the Branch Edition SIP Entity configured in **Section 7.2**
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box

Click **Commit** to save the configuration.

The screen below shows the Entity Link configured between Session Manager and Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Entity Links'. Below this, there's a section for 'Entity Links' with 'Commit' and 'Cancel' buttons. A table lists the configured entity links. The first item is highlighted with a red box:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM-1_CM Duplex M	* SM-1	TLS	* 5061	* CM Duplex Main	* 5061	trusted	<input type="checkbox"/>

Below the table, there's a 'Select : All, None' option. At the bottom right, there are 'Commit' and 'Cancel' buttons.

The screen below shows the Entity Link between Session Manager and Avaya IP Office for the sample branch.

The screenshot shows the Avaya Aura System Manager 6.3 interface, similar to the previous one. The left sidebar is the same. The main content area is titled 'Home / Elements / Routing / Entity Links'. The 'Entity Links' section shows a table with one item highlighted by a red box:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM-1_Daytona-FST	* SM-1	TLS	* 5061	* Daytona-FST-Pune-Branch-1	* 5061	trusted	<input type="checkbox"/>

Below the table, there's a 'Select : All, None' option. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Repeat the above steps to configure **Entity Links** for the secondary Session Manager.

7.4. Configure Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities. To add a routing policy, select **Routing Policies** link on the left pane and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** Enter a descriptive name in and optional text in **Notes**.
- **SIP Entity as Destination:** Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.
- **Notes:** Enter a descriptive text (optional)

Under **Time of Day**:

- Click **Add**, and select the default **24/7** time range.

Defaults can be used for the remaining fields.

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for routing calls from Avaya IP Office to non-SIP phones registered/connected with Communication Manager named **Duplex CM** at the HQ location. This same Routing Policy can also be used for routing PSTN calls to the HQ location where **Duplex CM** would send these calls through the central T1/E1 trunks to the PSTN¹.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Home / Elements / Routing / Routing Policies'. The 'Routing Policy Details' section is active, showing the 'General' tab. The 'Name' field is set to 'To Duplex CM'. The 'SIP Entity as Destination' section shows a table with one entry: 'CM Duplex Main' with FQDN 'fp2-cm001.sol001.fst.silpune1ab.com' and Type 'CM'. The 'Time of Day' section shows a table with one entry: '24/7' with a time range from '00:00' to '23:59'. The 'Dial Patterns' section shows a table with three entries: '301', '3016', and '3017', all with a time range of '7' to '7' and a note 'Duplex CM Core'.

Name	FQDN or IP Address	Type	Notes
CM Duplex Main	fp2-cm001.sol001.fst.silpune1ab.com	CM	Main with fallback to ESS

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
301	7	7	<input type="checkbox"/>	-ALL-	-ALL-	Duplex CM Core
3016	7	7	<input type="checkbox"/>	-ALL-	-ALL-	
3017	7	7	<input type="checkbox"/>	-ALL-	-ALL-	

¹ The standard configuration on Communication Manager and the Avaya Media Gateway for routing calls to the PSTN are out of scope of these Application Notes, and are therefore not included.

The following screen shows the Routing Policy to IP Office at the sample site for routing PSTN calls as well as calls to the branch non-SIP local extensions.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Routing Policies'. It features a 'Routing Policy Details' section with a 'General' tab. The 'General' tab includes fields for 'Name' (Daytona-FST-Pune-Branch-1), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is a 'SIP Entity as Destination' section with a 'Select' button and a table. The table has columns: Name, FQDN or IP Address, Type, and Notes. The first row shows 'Daytona-FST-Pune-Branch-1' as the Name, a redacted FQDN or IP Address, 'SIP Trunk' as the Type, and an empty Notes field. Below the table is a 'Time of Day' section with 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows '1 Item' and a 'Refresh' button. A table below this shows a single item with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The item has a ranking of 0, a name of 24/7, and is active for all days of the week from 00:00 to 23:59. The Notes field for this item is 'Time Range 24/7'. At the bottom, there is a 'Select : All, None' option.

7.5. Configure Dial Patterns

Define a Dial Pattern for matching calls based on dialed digits. A Dial Patterns is then associated with a Routing Policy to direct calls with the matched dialed digit strings to the destinations (SIP Entities as specified in Routing Policies).

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under **General**:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **SIP Domain:** SIP domain specified in **Section 7.1**
- **Notes:** Comment on purpose of dial pattern.

Under **Originating Locations and Routing Policies**:

Click **Add** and then select **ALL** for **Originating Location Name** field and routing policy from the list.

Defaults can be used for the remaining fields.

Click **Commit** to save the Dial Pattern.

AVAYA Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled) Last Logged on at October 1, 2013 4:36 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 3012
* Min: 7
* Max: 15

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: sol001.fst.silpunelab.com
Notes: Daytona-FST-Pune-Branch-1

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Daytona-FST-Pune-Branch-1		<input type="checkbox"/>	Daytona-FST-Pune-Branch-1	

Select : All, None

8. Configure Avaya IP Office

This section provides the procedures for configuring IP Office to be centrally administered via System Manager. The procedures include the following areas:

- Access IP Office ICU (Initial Configuration Utility)
- Configure IP Office Element on System Manager
- Synchronizing IP Office “System Configuration and Users” with System Manager
- Launch IP Office Manager via System Manager
- Verify IP Office Licenses
- Configure Codec Preference
- Configure Voicemail
- Configure SM Line
- Configure short codes
- Configure Incoming Call Route
- Configure Centralized SIP Users for IP Office Branch using System Manager
- Configure H.323 User for IP Office Branch using System Manager

8.1. Access IP Office ICU (Initial Configuration Utility)

Connect a PC/Laptop to the LAN port of IP Office 500 V2 Hardware box. Provide IP address to PC/Laptop of 192.168.42.X range. PC/Laptop should have the latest IPO manager Application installed on it.

Select **Start → Programs → IP Office → Manager** to launch the Manager application. Click on **File→Open Configuration**, a **Select IP Office** window will popup, enter IP Office IP address as 192.168.42.1 (default LAN port IP address of IP Office) and click on search, check the check box provided and the **Initial Configuration Utility** will be displayed.

- **System Type** Select IP Office Standard Mode
- **System Name** A descriptive name for IP Office
- **LAN Interface** Select appropriate LAN port
- **IP address** Enter IP address for IP Office
- **IP Mask** Enter IP mask for the IP range
- **Gateway** Enter gateway IP address for IP Office
- **DHCP Mode** Provides the ability to act as a DHCP server for IP Telephones and other IP endpoints. For the sample configuration DHCP server is disabled.
- **New Security password** Enter security password
- **Under Centralized management** Check the Check box. This field indicates that all the IPO related administration will be done via Avaya Aura® System Manager.
- **System Manager Address** Enter System Manager IP Address
- **SNMP Community** Enter “public”
- **SNMP Device ID** This value will be filled by system itself, leave it blank.
- **Trap Community** Enter “public”
- **Device Certificate Name** This name would be used to generate TLS certificate from System Manager.
- **Certificate Enrollment (SCEP) Password** Enter password for TLS certificate exchange between System Manager and IP Office.

The screenshot shows the 'Avaya IP Office Initial Configuration' window. It contains the following fields and settings:

- System Type:** ☒ Basic Mode, ☐ Server Edition Expansion, ☒ IP Office Standard Mode
- System Name:** IP-Office-42111
- LAN Interface:** ☒ LAN1, ☐ LAN2
- IP Address:** [Redacted] . 42 . 111
- IP Mask:** 255 . 255 . 255 . 0
- Gateway:** [Redacted] . 42 . 1
- DHCP Mode:** ☐ Server, ☐ Client, ☐ DialIn, ☒ Disabled
- New Security Password:** [Redacted]
- Under Centralized Management ?** ☒
- SMGR Address:** [Redacted] . 121 . 13
- SNMP Community:** public
- SNMP Device ID:** [Redacted]
- Trap Community:** public
- Device Certificate Name:** IPOffice42111
- Certificate Enrolment (SCEP) Password:** [Redacted]

Buttons at the bottom: Save, Reset, Close, Help.

After entering the above details click **Save**, and IPO will reboot. Once IP Office comes up again, launch IPO Manager, access IP Office and verify above details are reflected properly on IP Office.

8.2. Configure IP Office Element on System Manager

To add IP Office as an element on System Manager, launch System Manager web page login as Administrator credentials. Go to **Services→Inventory→Manage Elements**, click on **New**.

- **Name** A descriptive name for IP Office
- **Description** Description for IP Office
- **Node** Enter IP Address of IP Office
- **Device Type** Select IP Office from drop down
- **Device Version** Select correct IP Office version from drop down
- **Service Login** The default Service Login is **SMGRB5800Admin**
- **Service Password** The default Password is **SMGRB5800Admin**
- **Confirm Service Password** Re-Enter Service Password

Note: Service login/ password mentioned above is default one this can be changed here and then same should be updated on IP Office under Security Settings.

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The breadcrumb navigation is Home / Services / Inventory / Manage Elements. The page title is 'Edit IP Office Daytona-FST-Pune-Branch'. The 'General' tab is selected, and a red box highlights the configuration fields:

- Name:** Daytona-FST-Pune-Branch
- Description:** IP Office 9.0 Pune Branch
- Node:** 42.111
- Device Type:** IP Office
- Device Version:** 9.0
- Service Login:** SMGRB5800Admin
- Service Password:** (masked with dots)
- Confirm Service Password:** (masked with dots)

Click on **SNMP** tab displayed in above screenshot.

- Select version as “**V1**” and Read Community as “**public**”.

Click on the **Commit** button.

General * SNMP *

SNMP

*Version ☐ None ☒ V1

* Read Community public

Write Community

* Retries 3

* Timeout (ms) 5000

Commit Clear Cancel

8.3. Synchronizing IP Office System Configuration and Users with System Manager

Go to **System Manager**→**Services**→**Inventory**→**Synchronization**→**IP Office**, select **IP Office**. Select the **System Configuration and Users** and click on the **New** button (not shown). Verify that this operation is successful and the **Status** column should get updated with **Completed** status.

AVAYA Avaya Aura® System Manager 6.3

Primary Server - Active Mode (GR Replication - Disabled)

Last Logged on at October 1, 2013 4:36 PM
Help | About | Change Password | Log off admin

IP Office * Inventory * Routing * Home

Home / Services / Inventory / Synchronization / IP Office

Synchronize IP Office System Configuration

Device List

1 Item Found Refresh Show ALL Filter: Disable, Apply, Clear

<input checked="" type="checkbox"/>	Device Name	IP Address	System Type	Last Operation on Device	Status	System Configuration Template	Last Modified Time of System Configuration	Last Backup Time
<input checked="" type="checkbox"/>	Daytona-FST-Pune-Branch	42.111	IP Office	Restore: User(s)	Completed	Daytona-FST-Pune-Branch	October 3, 2013 8:23:36 PM +05:30	September 25, 2013 4:02:36 PM +05:30

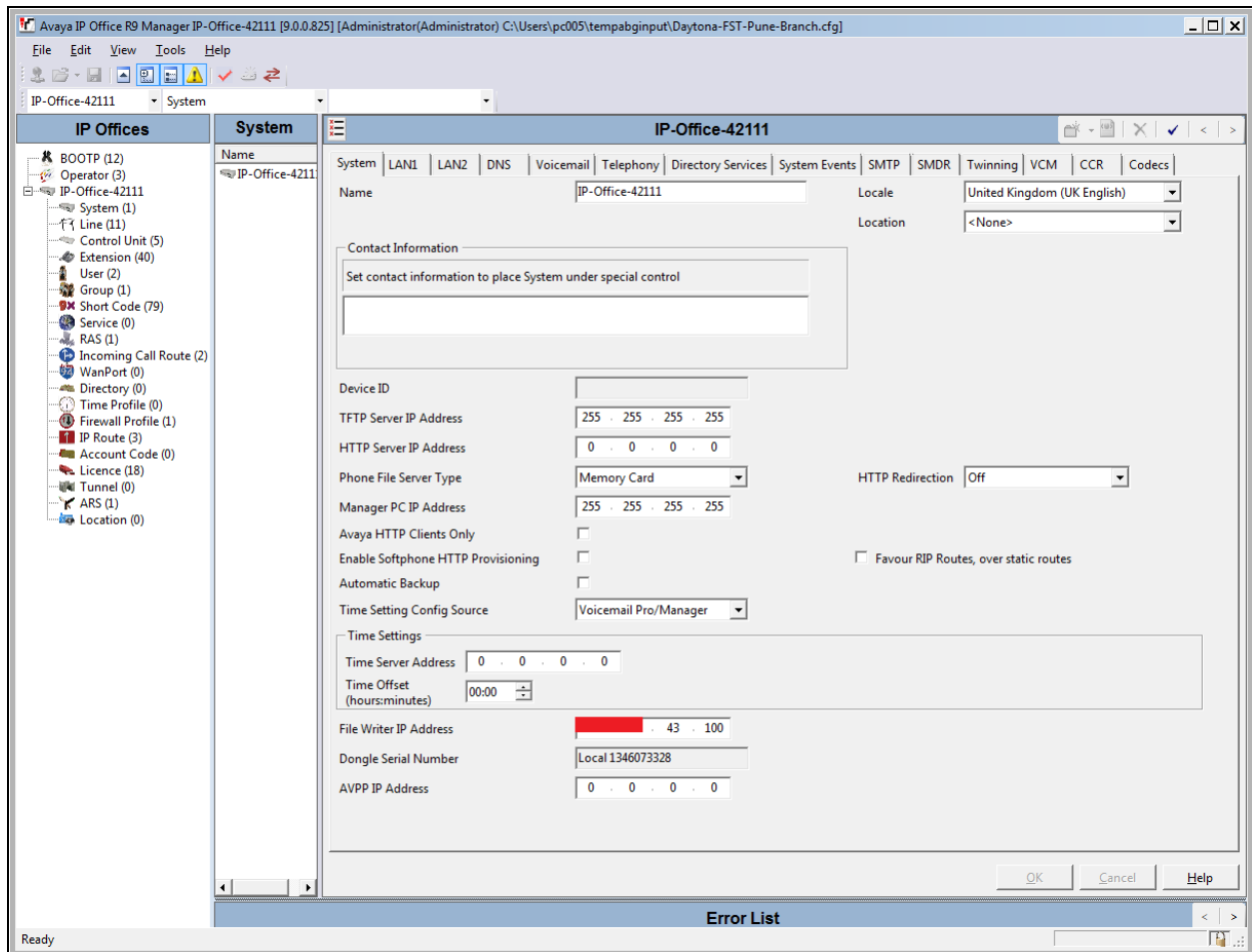
Select : All, None

☐ System Configuration
☐ User
☒ System Configuration and Users

Now Schedule

8.4. Launch IP Office Manager via System Manager

Go to **System Manager**→**Elements**→**IP Office**→**System Configuration**, click on the **Edit** button (not shown). The IP Office manager window will be launched as displayed on screenshot.



8.4.1. IP Office License Configuration

Go to **SMGR**→**Elements**→**IP Office**→**System Configuration**, click on the **Edit** button (not shown). The IP Office manager window will be launched as displayed below. From the configuration tree in the left pane, select **License** and select **Remote Server** tab to configure the following:

- **Enable Remote Server** Check box should be checked if using Centralized License server.
- **Domain name (URL)** Enter <https://xx.xx.xx.13> (In sample configuration SMGR is the centralized WebLM License server).
- **URN** Enter **WebLM/LicenseServerPort Number**
Enter the port for WebLM. By default WebLM uses

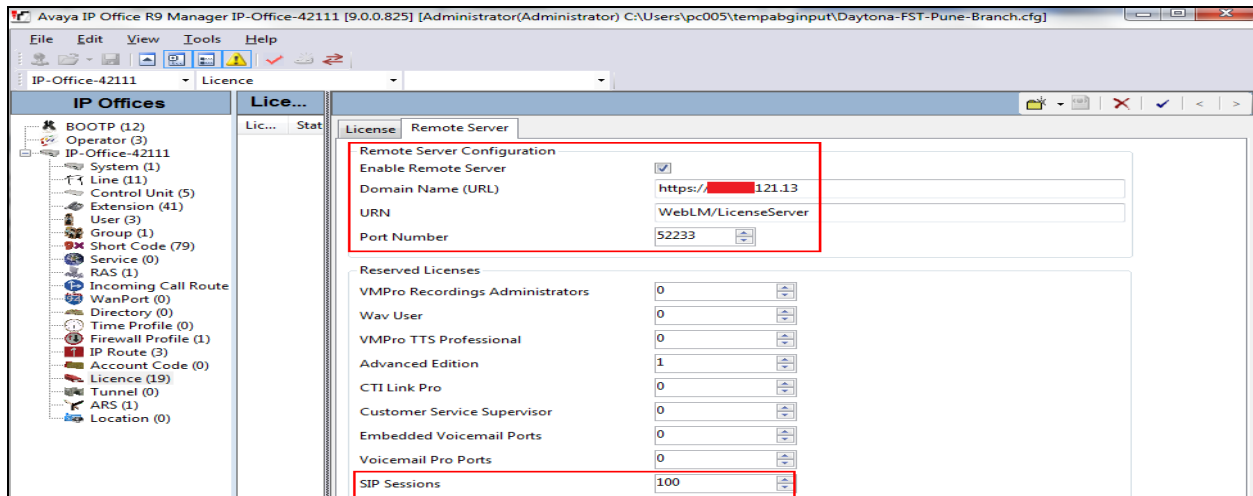
Port **52233**.

- **SIP Session**

Enter value as per licenses on license server.

Maximum value can be **100**.

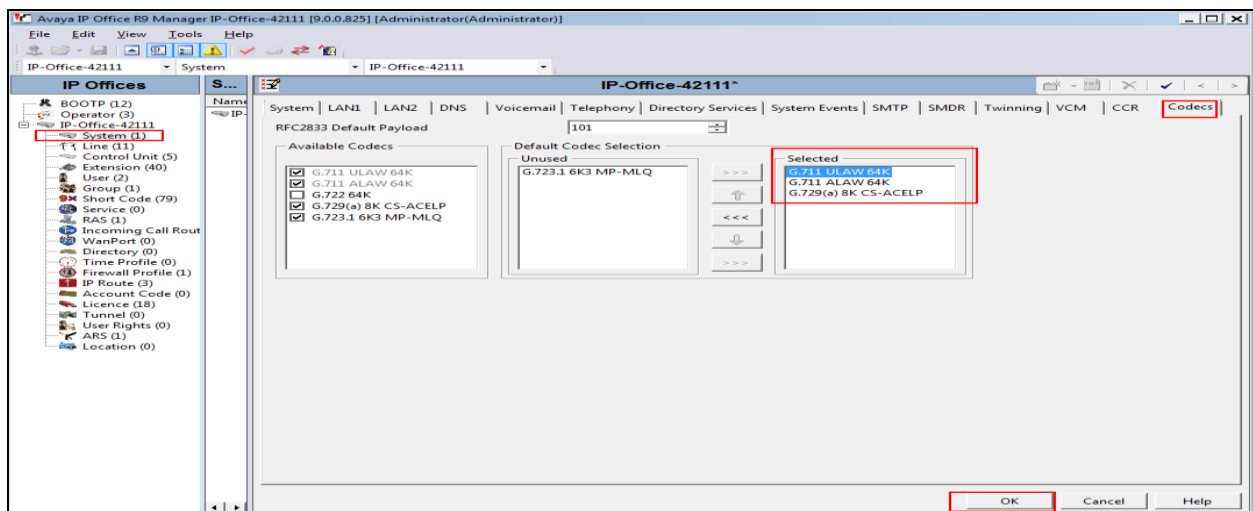
Click on the **OK** button and click **Save** button to save configuration (not shown).



8.4.2. Configure Codec Preference

From the configuration tree in the left pane, select **System** to display the details panes on the right. Select the right-most tab called **Codecs** to specify the IP codec and their preferred order for all calls on Avaya IP Office. In the sample configuration **G.711ALAW**, **G.711ULAW**, **G.729(a)** was selected. This should match the allowed codec on Communication Manager as configured in **section 6.4**.

Click on the **OK** button and click **Save** button to save configuration (not shown).



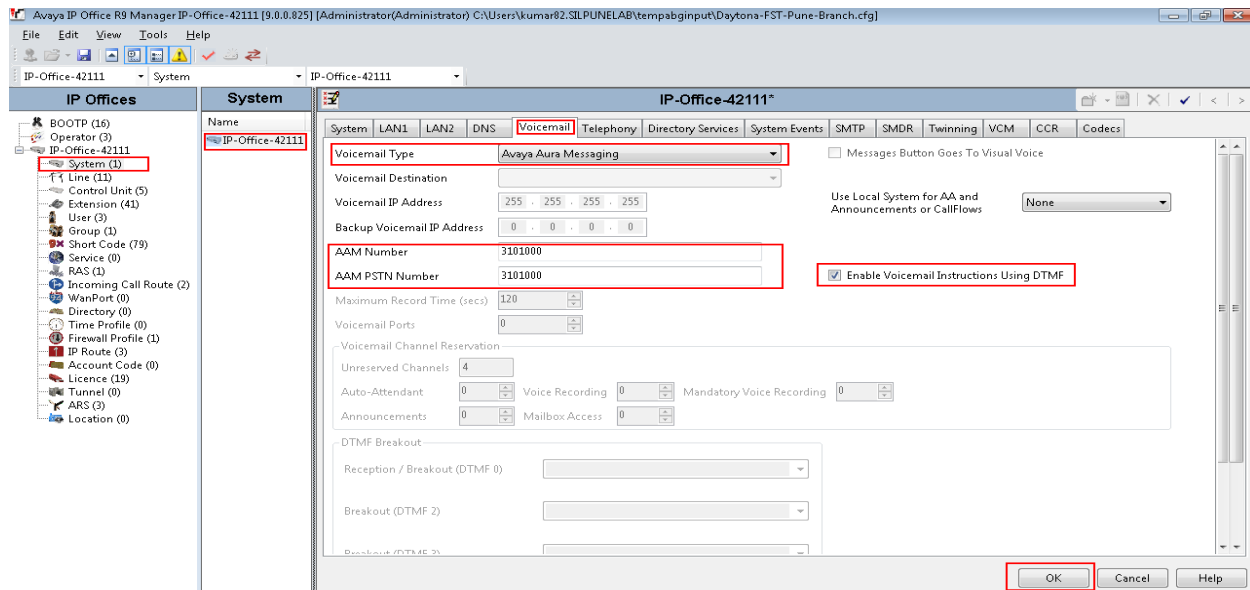
8.4.3. Configure Voicemail

From the configuration tree in the left pane, click on **System** → **Voicemail** to configure voicemail type as Avaya Aura® Messaging.

- **Voicemail Type** Avaya Aura® Messaging.
- **AAM Number** **3101000** Pilot number to reach Voicemail server via SMLine.
- **AAM PSTN Number** **310100** Pilot number to reach Voicemail server via PSTN
- **Enable Voicemail Instructions Using DTMF** Check this box

Retain default values for all other fields.

Click the **OK** button and **Save** button (not shown) to save configurations.



8.4.4. Configure SM Line

Avaya IP Office uses a special type of SIP trunk to communicate with Avaya Aura® Session Manager called an **SM Line**. From the configuration tree in the left pane, right-click on **Line** and select **New SM Line** to add an instance.

In the **Session Manager** tab the following information is entered.

- **Line Number:** **111**. 349 is maximum value.
- **In Service:** Enable check box to make trunk In Service
- **SM Domain Name:** **silpunelab.com**. SIP domain used in Session Manager under section 6.1.
- **SM Address:** **xx.xx.121.15**. IP address of the SIP signaling interface.

- **Outgoing GroupID:** **98888**. While this value is not adjustable it should be noted as it will be used for routing calls to Session Manager via Short Codes.
- **Max Calls:** **128** was used in the reference configuration. This entry should not exceed licensed value.
- **URI Type:** **SIPS** was used in reference configuration.
- **Layer 4 Protocol:** **TLS**.
- **Session Timer (Seconds):** **On Demand**. This field is kept as On Demand to negotiate the session refresh timer sent by Communication Manager.

Avaya IP Office R9 Manager IP-Office-42111 [9.0.0.825] [Administrator/Administrator]

File Edit View Tools Help

IP-Office-42111 Line

IP Offices	Line	Line Number	Line Type	Line SubType
BOOTP (12)				
Operator (3)				
IP-Office-42111				
System (1)				
Line (11)				
Control Unit (5)				
Extension (40)				
User (2)				
Group (1)				
Short Code (79)				
Service (0)				
RAS (1)				
Incoming Call Rout				
WanPort (0)				
Directory (0)				
Time Profile (0)				
Firewall Profile (1)				
IP Route (3)				
Account Code (0)				
Licence (18)				
Tunnel (0)				
User Rights (0)				
ARS (1)				
Location (0)				

SM Line - Line 111

Session Manager | VoIP | T38 Fax

Line Number: 111 ☒ In Service

SM Domain Name: sol001.fst.silpunelab.com

SM Address: . 121 . 15

Outgoing Group ID: 98888

Prefix:

Max Calls: 128

URI Type: SIPS

Media Connection Preservation: Enabled

Network Configuration

Layer 4 Protocol: TLS

Send Port: 5061

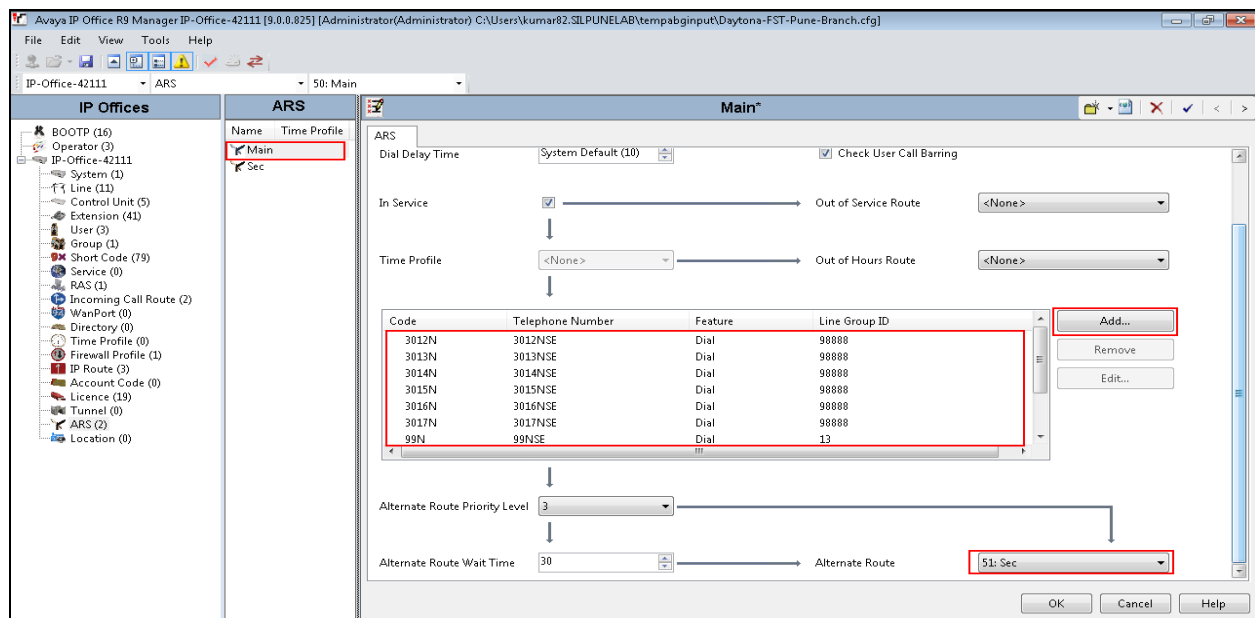
Listen Port: 5061

Session Timer (seconds): On Demand

OK Cancel Help

8.4.5. Configure ARS for SM Line

From the configuration tree in the left pane, right click on ARS and click on **New** (not shown).



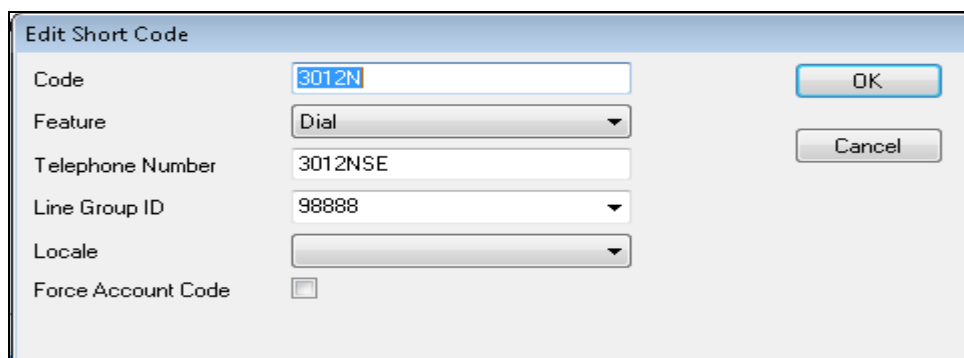
In the **ARS** tab the following information is entered.

- **Name:** Enter a descriptive name for primary ARS (not shown).

Click on the **Add** Button to create short code. The Edit Short Code window will be launched as displayed on screenshot. The following information is entered.

- **Code:** 3012N
- **Telephone number:** 3012NSE
- **Line Group ID:** 98888. Group ID mentioned in Section 8.4.3 to route calls to Session Manager via SM Line

Click the **OK** button.



Repeat above steps to create secondary ARS routing for PSTN trunk

On main ARS window select the secondary ARS route from the **Alternate Route** drop down box.

Code	Telephone Number	Feature	Line Group ID
3012N	3012NSE	Dial	98888
3013N	3013NSE	Dial	98888
3014N	3014NSE	Dial	98888
3015N	3015NSE	Dial	98888
3016N	3016NSE	Dial	98888
3017N	3017NSE	Dial	98888
99N	99NSE	Dial	13

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: 51: Sec

8.4.6. Configure Incoming Call Route

From the configuration tree in the left pane, right click on **Incoming Call Route** and click on **New** (not shown).

- Retain the default for values for the fields on the **Standard** tab

Avaya IP Office R9 Manager IP-Office-42111 [9.0.0.825] [Administrator/Administrator]

File Edit View Tools Help

IP-Office-42111 Incoming Call Route 0

IP Offices Incoming ...

Line Group ID Ind

0 13

Standard Voice Recording Destinations

Bearer Capability Any Voice

Line Group ID 0

Incoming Number

Incoming Sub Address

Incoming CLI

Locale

Priority 1 - Low

Tag

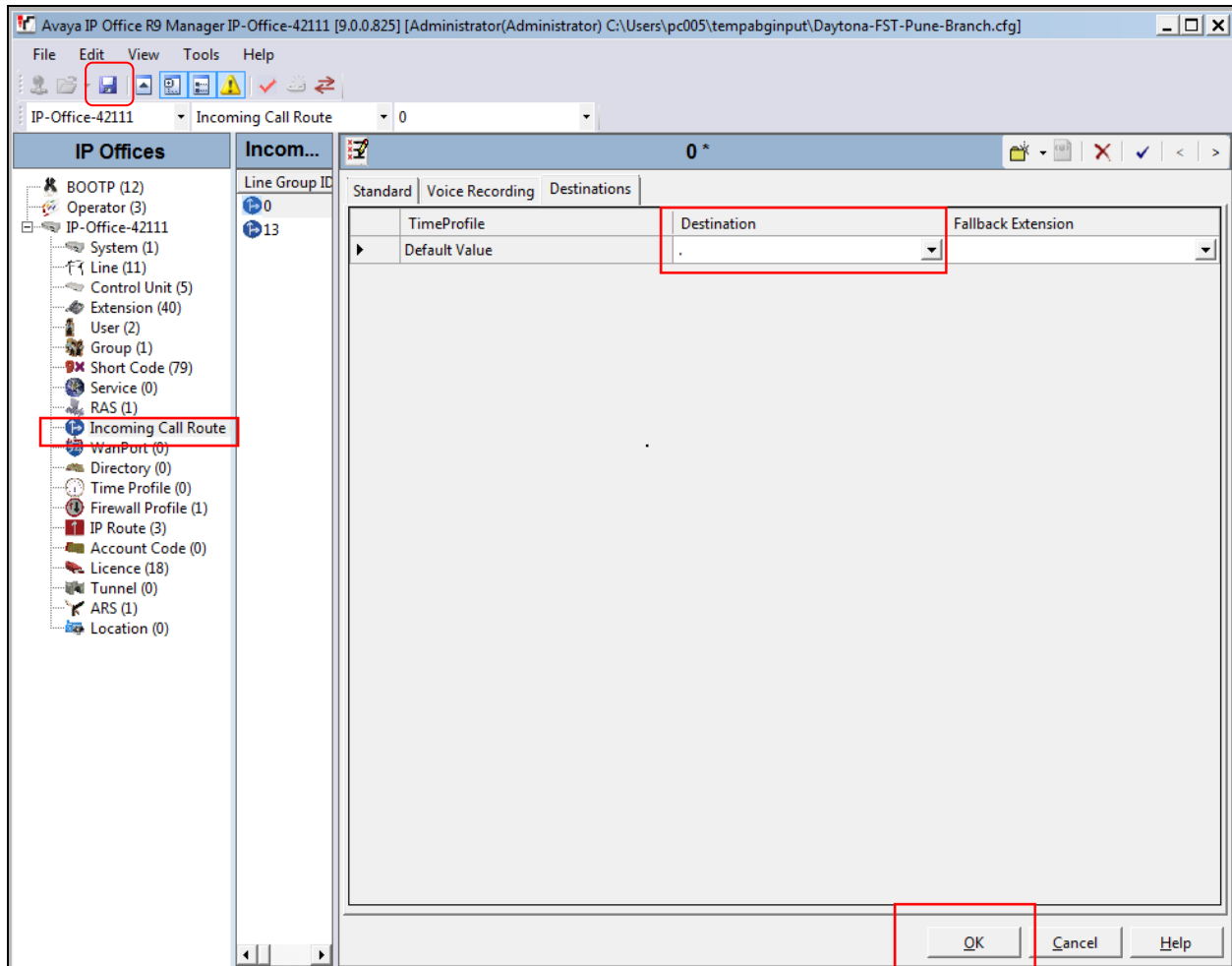
Hold Music Source System Source

Ring Tone Override None

OK Cancel Help

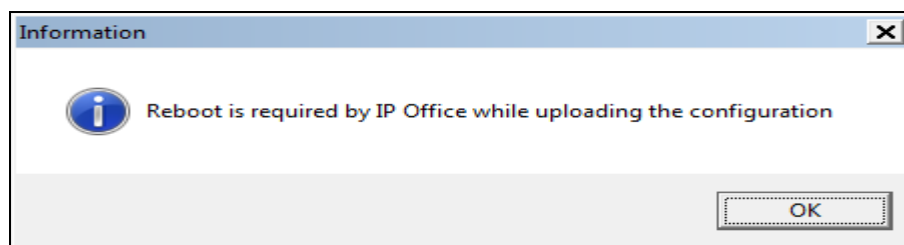
Click on **Destination** tab and put “.” in the destination text box, to allow all calls to Avaya IP Office.

Click **OK**.



Now click on the **Save** button as highlighted in the previous screen shot at the top menu bar. The **Information** window will appear as shown below to indicate a reboot is required.

Click **OK**.



After above operation IP Office Manager Application will be closed and System Configuration page will occur on System Manager. Click on the **Commit** button to send reboot command to Avaya IP Office on the IP Office tab on System Manager, as highlighted below.

Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled)

Last Logged on at October 4, 2013 2:52 PM
Help | About | Change Password | Log off admin

IP Office x Home

Home / Elements / IP Office / System Configuration

IP Office System Configuration Edit

Device List

Device Name	IP Address	System Type	Version	System Configuration Template
Daytona-FST-Pune-Branch	42.111	IP Office	9.0	Daytona-FST-Pune-Branch

Commit Schedule Cancel

Verify that after IP Office reboot is completed. Select **System and Configuration** from the left hand menu and verify the status at IP Office System Configuration screen should be displayed as **Completed** as displayed in below screenshot.

Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled)

Last Logged on at October 4, 2013 2:52 PM
Help | About | Change Password | Log off admin

IP Office x Home

Home / Elements / IP Office / System Configuration

IP Office System Configuration

Device List

View Edit

4 Items Found Refresh Show ALL Filter: Disable, Apply, Clear

Device Name	IP Address	System Type	Last Operation on Device	Status	System Configuration Template	Last Modified Time of System Configuration	Last Backup Time
Daytona-FST-Pune-Branch	42.111	IP Office	Edit: System Configuration	Completed	Daytona-FST-Pune-Branch	October 6, 2013 6:04:53 PM +05:30	September 25, 2013 4:02:36 PM +05:30
Daytona-FST-Kolkata-Branch	44.111	IP Office	Restore: User(s)	Completed	Daytona-FST-Kolkata-Branch	September 30, 2013 4:23:22 PM +05:30	August 8, 2013 11:13:12 PM +05:30

8.5. Configure Centralized SIP Users for IP Office Branch Using System Manager

Creating Avaya IP Office SIP endpoints in centralized branch model requires administration of an Avaya IP Office SIP Extension and User for each endpoint via System Manager.

To create Avaya IP Office SIP extension for SIP, log in to System Manager webpage with administrator credentials as described in **Section 7**.

Click **User Management** → **Manage Users** and click the **New** button (not shown).

Enter the following information:

Last Name:	Enter new user last name
First Name:	Enter new user first name
Login Name:	Enter new user login name
Authentication Type:	Select Basic from the drop down box
Password:	Enter new user password
Confirm Password:	Confirm new user password

AVAYA Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled)

Last Logged on at October 6, 2013 5:48 PM
Help | About | Change Password | Log off admin

User Management * Home

Home / Users / User Management / Manage Users

Help ?

New User Profile Commit & Continue Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity

* Last Name: Vijay

* First Name: Burman

Middle Name:

Description:

* Login Name: 3012788@sol001.fst.slp

* Authentication Type: Basic

Password:

Confirm Password:

Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.

Identity * Communication Profile * Membership Contacts

Communication Profile

Communication Profile Password:

Confirm Password:

On the same page, scroll down and under **Communication Address** click **New**. Select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Add**.

Communication Address ▼

<input type="checkbox"/>	Type	Handle	Domain
No Records found			

Type: Avaya SIP ▼

*** Fully Qualified Address:** 3012788 @ sol001.fst.silpunelab.com ▼

The Communication Address is now displayed.

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	3012788	sol001.fst.silpunelab.com

Select : All, None

Continue to scroll down on the same page and select the following information relevant to the implementation:

- **Primary Session Manager** Primary Session Manager SIP Entity from **Section 7.2**
- **Secondary Session Manager:** Secondary Session Manager SIP Entity from **Section 7.2**
- **Origination Application Sequence;** Select Origination Application Sequence relevant for implementation
- **Termination Application Sequence:** Select Termination Application Sequence relevant for implementation
- **Home Location** Select Home Location relevant to the implementation.

☒ **Session Manager Profile** ▼

SIP Registration

*** Primary Session Manager** SM-1 ▼

Secondary Session Manager SM-1 ▼

Survivability Server Daytona-FST-Pune-Branch-1 ▼

Max. Simultaneous Devices 1 ▼

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence CM Duplex Core ▼

Termination Sequence CM Duplex Core ▼

Call Routing Settings

*** Home Location** Daytona-FST-Pune-Branch-1 ▼

Conference Factory Set (None) ▼

Primary	Secondary	Maximum
96	8	101

supports 16 Communication Profile(s).

Scroll down to the page to the **CM Endpoint Profile** section.

- **System:** Select Communication Manager SIP Entity created from **Section 7.2** from the drop down box.
- **Profile Type:** Select the appropriate template type for the implementation. The sample configuration used **9641SIP_DEFAULT_CM_6_3** from the drop down box.
- **Extension:** Enter an available extension number.
- **Port:** Confirm **IP** is configured.

Click **Commit and Continue** (not shown here) before Configuring IP Office related parameters.

☒ **CM Endpoint Profile**

* **System**

CMduplex

* **Profile Type**

Endpoint

Use Existing Endpoints

☐

* **Extension**

3012788

Endpoint Editor

Template

9641SIP_DEFAULT_CM_6_3

Set Type

9641SIP

Security Code

Port

IP

Voice Mail Number

Preferred Handle

(None)

Enhanced Callr-Info display for 1-line phones

☐

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

☒

Scroll down to the page to the **IP Office** section.

- **System:** Select the IP Office System SIP Entity created in **Section 7.2** from the drop down list.
- **Template:** Select **Default Centralized SIP Template** from the drop down list.
- **Extension:** This value is populated automatically.
- **Set Type:** This value is populated automatically.

Click **Commit** (not shown here).

The screenshot shows the 'IP Office Endpoint Profile' configuration form. It includes fields for 'System' (Daytona-FST-Pune-Branch), 'Template' (Default Centralized SIP Tem), 'Extension' (3012788), 'Module-Port' (Select), and 'Set Type' (SIP). There are also checkboxes for 'Use Existing Extension' and 'Delete Extension On User Delete'. Red boxes highlight the System and Template fields, and the Extension, Module-Port, and Set Type fields.

☒ **IP Office Endpoint Profile**

* **System** Daytona-FST-Pune-Branch
Centralized User is supported by selected IP Office.

* **Template** Default Centralized SIP Tem
Selected template is a Centralized User template.

Use Existing Extension ☐

* **Extension** 3012788 Endpoint Editor

Module-Port Select

Set Type SIP

Delete Extension On User Delete ☒

8.6. Configure H.323 User for IP Office branch using System Manager

Creating Avaya IP Office H.323 endpoints requires administration of an Avaya IP Office SIP Extension and User for each endpoint via System Manager.

To create Avaya IP Office H.323 extension, log in to System Manager webpage with administrator credentials as described in **Section 7**.

Navigate to **User Management** → **Manage Users** and click the **New** button (not shown).

Enter the following information:

Last Name:	Enter new user last name
First Name:	Enter new user first name
Login Name:	Enter new user login name
Authentication Type:	Select Basic from the drop down box
Password:	Enter new user password
Confirm Password:	Confirm new user password

Home / Users / User Management / Manage Users [Help ?](#)

User Profile Duplicate

[Commit & Continue](#) [Commit](#) [Cancel](#)

Identity * **Communication Profile** * **Membership** **Contacts**

Identity ▾

* **Last Name:**

* **First Name:**

Middle Name:

Description:

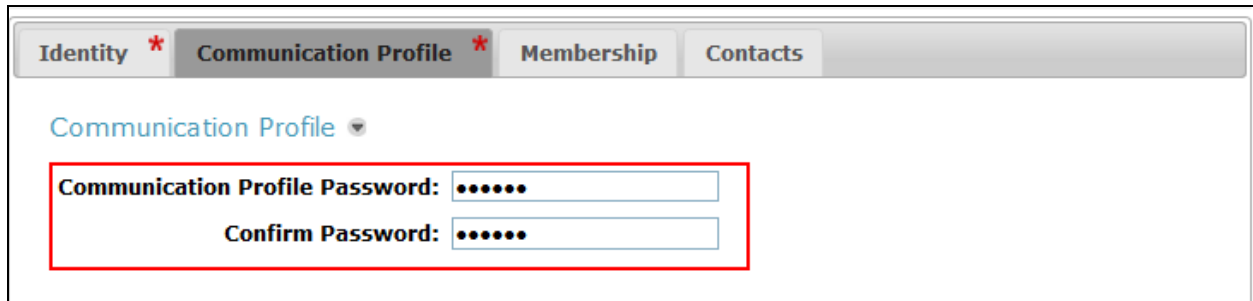
* **Login Name:**

* **Authentication Type:**

Password:

Confirm Password:

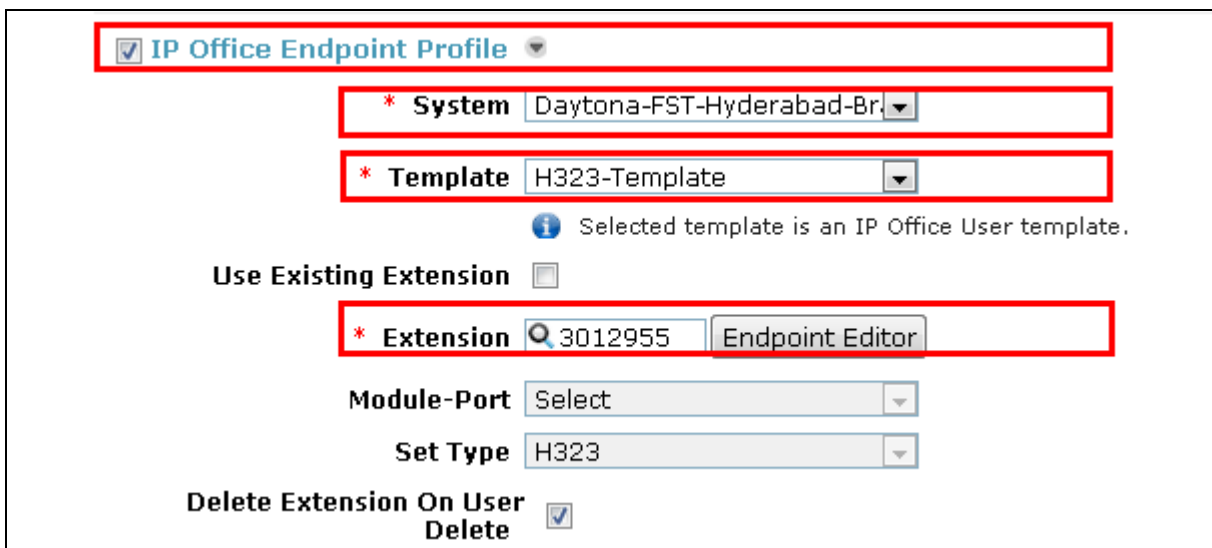
Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.



Scroll down to the page to the **IP Office** section.

- **System:** Select the IP Office System SIP Entity created in **Section 7.2** from the drop down list.
- **Template:** Select **H323-Template** from the drop down list.
- **Extension:** This value is populated automatically.
- **Set Type:** This value is populated automatically.

Click **Commit** (not shown here).



9. Configure Avaya Aura® Messaging

This section provides the procedures for configuring Avaya Aura® Messaging as provisioned in the sample configuration. Assumption is that Messaging is already installed, configured and integrated with Avaya Aura® System Manager.

The procedures described in this section include configurations in the following areas:

- Configure Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern
- Configure Messaging profile for Users

9.1. Configure Entity

The following screen shows the results of adding the Avaya Aura® Messaging. In this case, **FQDN or IP Address** is the IP address assigned to Avaya Aura® Messaging.

Select **Modular Messaging** for **Type** field.

Click **Commit**.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: AAM

* FQDN or IP Address: 172.16.121.232

Type: Modular Messaging

9.2. Configure Entity Links

In the sample configuration, an Entity Link is configured between Avaya Aura® Session Manager and Avaya Aura® Messaging.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the SIP Entity link for Session Manager that was created in **Section 7.2**
- **Protocol:** Select **TLS**
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the SIP Entity link for **Messaging** that was configured in **Section 9.1**

- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box

Click **Commit**.

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
SM-1_AAM	SM-1	TLS	5061	AAM	5061	trusted

Select : All, None

9.3. Configure Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities. To add a routing policy, select **Routing Policies** link on the left pane and click on the **New** button (not shown) on the right. The Routing Policies details screen is displayed.

Under **General** section fill in the following:

Name: Enter a descriptive name

Notes: Optional text.

Scroll down to **SIP Entity as Destination**. Click **Select** and select the appropriate SIP entity for Avaya Aura® Messaging configured in **Section 9.1**.

Scroll down to **Time of Day**. Click **Add** and select the default **24/7** time range.

Defaults can be used for the remaining fields.

Click **Commit** to save the Routing Policy definition.

Routing Policy Details

Commit Cancel

General

* Name: To AAM Voicemail

Disabled: ☐

* Retries: 0

Notes: To AAM Voicemail

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AAM	172.16.121.232	Modular Messaging	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

9.4. Configure Dial Pattern

Define a Dial Pattern for call routing to Avaya Aura® Messaging.
Associate Dial Patterns with a Routing Policy created under **Section 9.3**

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under **General**:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **SIP Domain:** SIP domain specified in **Section 7.1**
- **Notes:** Descriptive text (optional)

Under **Originating Locations and Routing Policies**:

Click **Add** and then select **ALL** for **Originating Location Name** field and routing policy from the list. Select **Routing Policy** of **Messaging** created under **Section 9.3**

Defaults can be used for the remaining fields.

Click **Commit** to save the Dial Pattern.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 310

* Min: 7

* Max: 7

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To AAM ViuceMail 3101000

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input checked="" type="checkbox"/>	-ALL-		To AAM ViuceMail		<input type="checkbox"/>	AAMCluster	To AAM ViuceMail

9.5. Configure Messaging Profile to User

Adding a Messaging Profile to user enables Voice mail and Messaging features for the end user. Avaya endpoints require administration for users that need Messaging capabilities.

To add a Messaging Profile to an existing extension, log in to System Manager webpage with administrator credentials as described in **Section 7**.

Click **User Management** → **Manage Users**. Select the applicable user. Click **Edit** button. Select the **Communication Profile** tab.

Scroll down to the **Messaging Profile** section. Select the **Messaging Profile** check box.

- **System:** Select the **AvayaAuraMessaging** from the drop down list.
- **Mailbox Number:** Enter the applicable mailbox number.
- **Template:** Select **DEFAULT_AURAMESSAGING_TEMPLATE** from the drop down list.
- **Password:** Configure a password in the **Password** and **Confirm Password** fields.

Click **Commit** to save the configuration.

☒ **Messaging Profile**

* **System** AvayaAuraMessaging

Use Existing Subscriber on System ☐

* **Mailbox Number** 3011902 Messaging Editor

* **Template** DEFAULT_AURAMESSAGING_TEMPLATE

* **Password**

Delete Subscriber on Unassign of Subscriber from User or on Delete User ☒

10. Configure Avaya Aura® Conferencing

This section provides the procedures for configuring Avaya Aura® Conferencing as provisioned in the sample configuration. Assumption is that Avaya Aura® Conferencing is already installed, configured and integrated with Avaya Aura® System Manager.

The procedures described in this section include configurations in the following areas:

- Configure Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern
- Configure Conferencing Profile for User

10.1. Configure Entity

The following screen shows the results of adding the Avaya Aura® Conferencing. In this case, **FQDN or IP Address** is the IP address assigned to Avaya Aura® Conferencing.

Select **Conferencing** from the drop down list for **Type** field.

AVAYA Avaya Aura® System Manager 6.3
Primary Server - Active Mode (GR Replication - Disabled)

Last Logged on at October 7, 2013 7:35 PM
Help | About | Change Password | Log off admin

Routing * User Management * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: AAC7

* FQDN or IP Address: 121.38

Type: Conferencing

Notes: AAC 7 - Jan 23, 2013

Commit Cancel

10.2. Configure Entity Links

In the sample configuration, an Entity Link is configured between Avaya Aura® Session Manager and Avaya Aura® Conferencing.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the Session Manager SIP Entity configured in **Section 7.2**
- **Protocol:** Select **TLS**
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the SIP Entity **Conferencing 7** configured in **Section 10.1**
- **Port:** Port number on which the other system receives SIP requests

- **Trusted:** Check this box

Click **Commit** to save the configuration.

10.3. Configure Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities. To add a routing policy, select **Routing Policies** link on the left pane and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)

Under **SIP Entity as Destination**:

- Click **Select** and then select the appropriate SIP entity for **Avaya Aura® Conferencing** created under **Section 10.1** this routing policy applies.

Under **Time of Day**:

- Click **Add** and select the default **24/7** time range.

Defaults can be used for the remaining fields.

Click **Commit** to save the Routing Policy definition.

10.4. Configure Dial Pattern

Define a Dial Pattern for call routing to Avaya Aura® Conferencing.

Associate Dial Patterns with a Routing Policy created under **Section 10.3**.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown). Fill in the following, as shown in the screens below:

Under **General**:

- **Pattern:** Dialed number or prefix
- **Min:** Minimum length of dialed number
- **Max:** Maximum length of dialed number
- **SIP Domain:** SIP domain specified in **Section 7.1**
- **Notes:** Descriptive text (optional)

Under **Originating Locations and Routing Policies**:

Click **Add** and then select **ALL** for **Originating Location Name** field and routing policy from the list. Select Routing Policy of Conferencing created under **Section 10.3**

Defaults can be used for the remaining fields. Click **Commit** to save the Dial Pattern.

The screenshot shows the 'Dial Patterns' configuration page. On the left is a navigation menu with 'Dial Patterns' selected. The main area is titled 'Dial Pattern Details' and contains two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** 1111
- Min:** 7
- Max:** 8
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** -ALL-
- Notes:** Dial To Conferencing

Originating Locations and Routing Policies Section:

Buttons: Add, Remove

1 Item | Refresh Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To Conferencing		<input type="checkbox"/>	AAC7	To Conferencing

Select : All, None

10.5. Configure Conferencing profile to user

Adding a Conferencing profile to a user enables conferencing features for the end user. Avaya SIP endpoints registered to Session Manager require administration of a Conferencing Profile for users that need Ad-Hoc conferencing capabilities

To add Conferencing profile to an existing extension log in to System Manager webpage with administrator credentials as described in **Section 7**.

Click **User Management** → **Manage Users**. Select the applicable user. Click **Edit** button. Select the **Communication Profile** tab.

Scroll down to the **Conferencing Profile** section. Select the **Conferencing Profile** check box.

- **Location:** Select the applicable Location from the drop down list.
- **Template:** Select the appropriate template based on user conferencing need, in the sample configuration **desktop_user_collab_code_with_video_rec** that will enable user to perform Audio, Video and Collaboration with recording.

Defaults can be used for the remaining fields. Click **Commit** to save the configuration.

<input checked="" type="checkbox"/> Conferencing Profile	
Select Auto-generated Code Length	6
Auto Generate Participant Collaboration Code	<input checked="" type="checkbox"/>
Auto Generate Moderator Collaboration Code	<input checked="" type="checkbox"/>
Auto Generate Participant Pass code	<input checked="" type="checkbox"/>
Auto Generate Moderator Pass code	<input checked="" type="checkbox"/>
Location	HQ-1
* Template	desktop_user_collab_code_wi
Video Enabled	Yes
Recording Enabled	Yes
Priority Class	Medium (default)
Collaboration Class	desktop_user_collab_code
Maximum Number Of Participants	50
Allow Dial Out To Participants	Yes
Video Conferencing Class	hi_bandwidth_d
Maximum Bandwidth (kbps)	150000
Bandwidth Per Participant (kbps)	3000
Conference Class	Class D
Maximum Resolution	1080p-30
Aspect Ratio	16:9

11.3. Verify Registrations of SIP Endpoints

Go to **Elements** → **Session Manager** → **System Status** → **User Registrations** to verify the SIP endpoints have successfully registered with at least one Session Manager.

For example, the screen below highlights one Centralized SIP user from Branch 1 who has successfully registered with both Session Manager servers.

User Registrations												
Select rows to send notifications to devices. Click on Details column for complete registration status.												
View ▾ Default Force Unregister AST Device Notifications: Reboot Reload ▾ Failback As of 5:32 PM Customize ▾ Advanced Search ▾												
1 Item Found Refresh Show ALL ▾ Filter: Disable, Apply, Clear												
Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
										Prim	Sec	Surv
► Show	3012002@sol001.fst.silpunelab.com	premi	poonawala	Daytona-FST-Pune-Branch-1	192.178.42.206:5061	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

11.4. Verify IP Office System Status

Launch IP Office System Status application and go to **System** → **VoIP Trunks** → **Line: 111**. In sample configuration **111** is line Trunk number for Session Manager.

Verify **Number of Administered Channels**, **SIP Trunk Channel License** value are same as configured and should not be **0**. Current Status of channel is **Idle**.

Avaya IP Office System Status - IP-Office-42111 (192.178.42.111) - IP500 V2 9.0.0.0 build 825

AVAYA

IP Office System Status

Help Snapshot LogOff Exit About

System

Memory Cards

Control Unit (IP500 V)

VoIP Trunks (3)

Line: 17

Line: 111

Line: 112

H.323 Extensions

Alarms (22)

Extensions (19)

Trunks (10)

Lines: 1 - 4

Line: 9

Line: 13

Line: 14

Line: 17

Line: 111

Line: 112

Active Calls

Resources

Time

Licenses

Directory

Control Unit Audit

Voicemail

Mailboxes

IP Networking

IP Routes

SSL VPN

Locations

StatusUtilization SummaryAlarms

SM Trunk Summary

Resolved Address: 172.16.121.15

Line Number: 111

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: G711 A, G711 Mu, G729 A, G7231

Silence Suppression: Off

Media Stream: RTP

Layer 4 Protocol: TLS

SIP Trunk Channel Licenses: 100

SIP Trunk Channel Licenses in Use: 0

SIP Device Features: REFER (Incoming and Outgoing)

Precedence: Primary

0%

Channel Number	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Los...	Transmit Jitter	Transmit Packet Los...
1		Idle	1 day 10:0...											
2		Idle	1 day 10:0...											
3		Idle	1 day 10:0...											
4		Idle	1 day 10:0...											
5		Idle	1 day 10:0...											
6		Idle	1 day 10:0...											
7		Idle	1 day 10:0...											
8		Idle	1 day 10:0...											
9		Idle	1 day 10:0...											
10		Idle	1 day 10:0...											

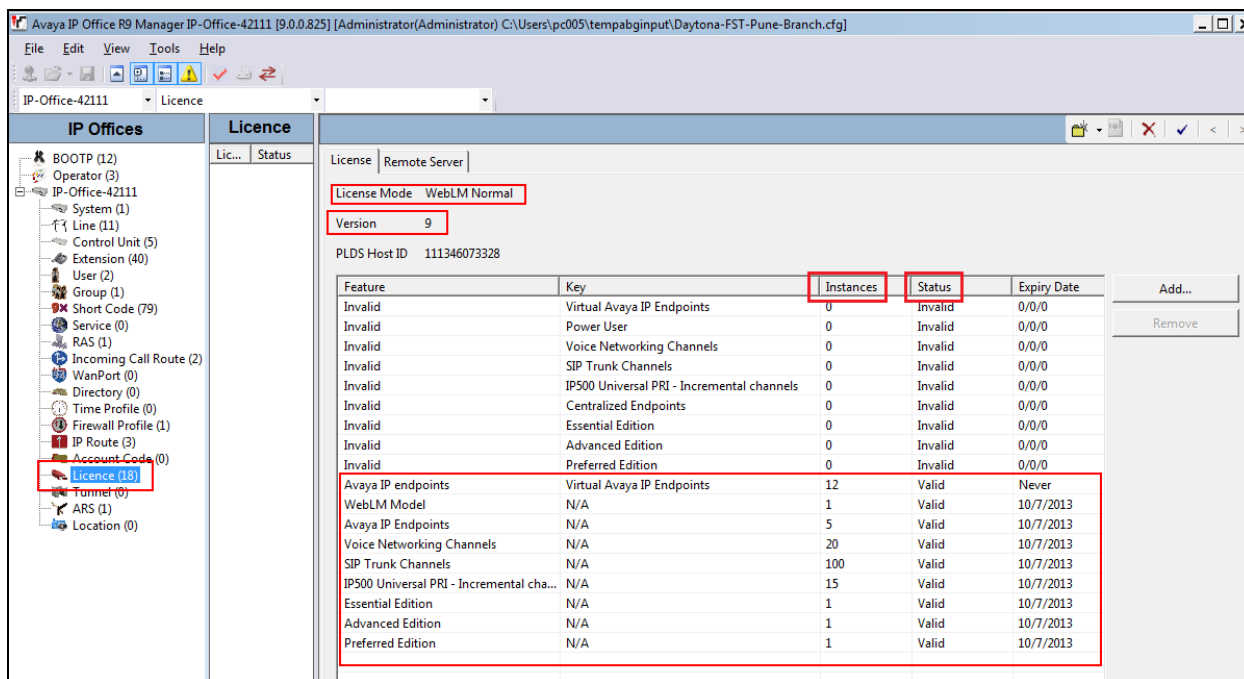
TraceTrace AllPausePingCall DetailsPrint...Save As...

5:56:54 PMOnline

11.5. Verify IP Office WebLM Connectivity

Go to **System Manager** → **Elements** → **IP Office** → **System Configuration**, click on **View** button, IP Office manager window will be launched as displayed below. From the configuration tree in the left pane, select **License** and select

- **License Mode** Should show **WebLM Normal** mode
- **Version** 9
- **Instance** value should be as per the license applied on WebLM License Server (In sample configuration it is SMGR)
- License **Status** should show status as **Valid**



11.6. Verify Call Scenarios

Verification scenarios for the configuration described in these Application Notes included the following call scenarios.

Sunny-Day scenarios:

- Place a call from a SIP telephone at the HQ location which is registered to Session Manager to a H.323 station on IP Office and verify the 2-way talk path.
- Place a call from Analog station on IP Office to an H.323 station at the HQ location that is registered with Communication Manager and verify talk path.
- Place a call from Branch Centralized SIP phone to another branch H.323 phone and verify if the call goes to voice mail when the H.323 phone does not answer call.
- Place a call to Audio Conferencing (1111001) bridge from Branch H.323 phone and verify caller gets connected to Conference Bridge based on participation code.

- Place a video call from HQ SIP Flare Experience on Windows 7 PC registered to Session Manager to another HQ SIP Flare Experience on iPad registered user and verify 2-way video calls works.
- Dial Voicemail access code (3101000) and verify voicemail server plays prompt to access messages.

Rainy-Day scenarios:

- Disconnect WAN connectivity of Branch and verify the Centralized SIP and ATA phones failover and register to IP Office.
- Dial voicemail access code (3101000) and verify voicemail server plays prompt to access messages using PSTN trunk.
- Place a call to Audio Conferencing Bridge (1111001) from Branch H.323 Phone and verify caller gets connected to Conference Bridge based on participation code using PSTN trunk.
- Place a call from HQ SIP telephone registered to Session Manager to a H.323 station registered with IP Office using prefix “9” and verify the 2-way talk path using PSTN trunk.

12. Conclusion

IP Office 9.0 deployed in Centralized, Mixed, Distributed Mode deployed with Avaya Aura® 6.2 FP2 works fine for Centralized administration, maintenance & telephony as well as Unified Communication Solution.

In case of branch WAN outage IP Office serves as Survivable server for branch Centralized SIP and ATA phones under Centralized and Mixed Mode.

13. Additional References

All references listed below can be downloaded from the following URL unless otherwise noted:
<http://support.avaya.com>

Avaya IP Office R9.0:

Extensive on-line help for IP-Office is available at the following URL	http://marketingtools.avaya.com/knowledgebase/
Solution Description for Avaya IP Office in a Branch Environment	https://downloads.avaya.com/css/P8/documents/100174429
Reference Configuration for Avaya IP Office in a Branch Environment	https://downloads.avaya.com/css/P8/documents/100174430
Deploying IP Office as an Enterprise Branch with Avaya Aura® Session Manager	https://downloads.avaya.com/css/P8/documents/100174874
Deploying IP Office as a Distributed Enterprise branch in a CS 1000 Environment with Avaya Aura® Session Manager	https://downloads.avaya.com/css/P8/documents/100174875
Administering Centralized Users for an IP Office Enterprise Branch	https://downloads.avaya.com/css/P8/documents/100174873
Migrating an IP Office or B5800 Branch Gateway to an IP Office Enterprise Branch	https://downloads.avaya.com/css/P8/documents/100174885

Avaya Aura® Session Manager R6.2 FP2:

Avaya Aura® Session Manager Overview and Specification	https://downloads.avaya.com/css/P8/documents/100168154
Installing and Configuring Avaya Aura® Session Manager	https://downloads.avaya.com/css/P8/documents/100168155
Maintaining and Troubleshooting Avaya Aura® Session Manager	https://downloads.avaya.com/css/P8/documents/100168156
Administering Avaya Aura® Session Manager:	https://downloads.avaya.com/css/P8/documents/100168166

Avaya Aura® Communication Manager R6.2 FP2:

Avaya Aura® Communication Manager Overview	https://downloads.avaya.com/css/P8/documents/100171719
Installing and Configuring Avaya	Installing:

Aura® Communication Manager	https://downloads.avaya.com/css/P8/documents/100171634
Configuring	https://downloads.avaya.com/css/P8/documents/100171658
Maintaining and Troubleshooting Avaya Aura® Communication Manager	Avaya Aura® Communication Manager Server Alarms: https://downloads.avaya.com/css/P8/documents/100171664 Avaya Aura® Communication Manager Denial Events: https://downloads.avaya.com/css/P8/documents/100175354 Avaya Aura® Communication Manager Security Design https://downloads.avaya.com/css/P8/documents/100171723

Avaya Aura Call Center Elite 6.2:

Administering Avaya Aura® Call Center Elite	https://downloads.avaya.com/css/P8/documents/100171609
Programming Call Vectoring Features in Avaya Aura® Call Center Elite	https://downloads.avaya.com/css/P8/documents/100171603
Planning for an Avaya Aura® Call Center Elite Implementation	https://downloads.avaya.com/css/P8/documents/100171604
Avaya Aura® Call Center Elite Overview and Specification	https://downloads.avaya.com/css/P8/documents/100171605

Avaya Aura® Experience Portal R.6.0:

Avaya Aura® Experience Portal Overview	https://downloads.avaya.com/css/P8/documents/100176098
--	---

©2014 Avaya Inc. All Rights Reserved.

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

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