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.

©2014 Avaya Inc. All Rights Reserved

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

©2014 Avaya Inc. All Rights Reserved

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

©2014 Avaya Inc. All Rights Reserved

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.

©2014 Avaya Inc. All Rights Reserved

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.

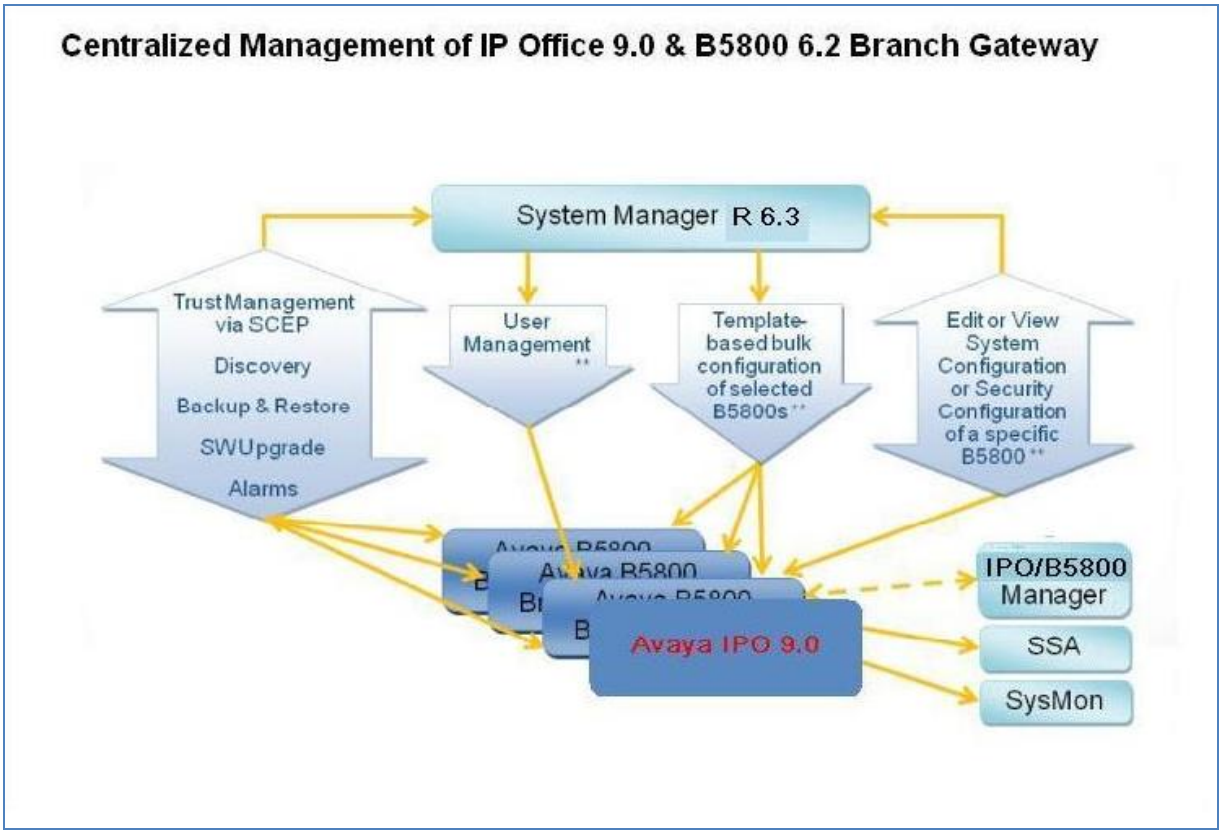


Figure 1: Centralized Management Configuration

- 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

©2014 Avaya Inc. All Rights Reserved

- 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.

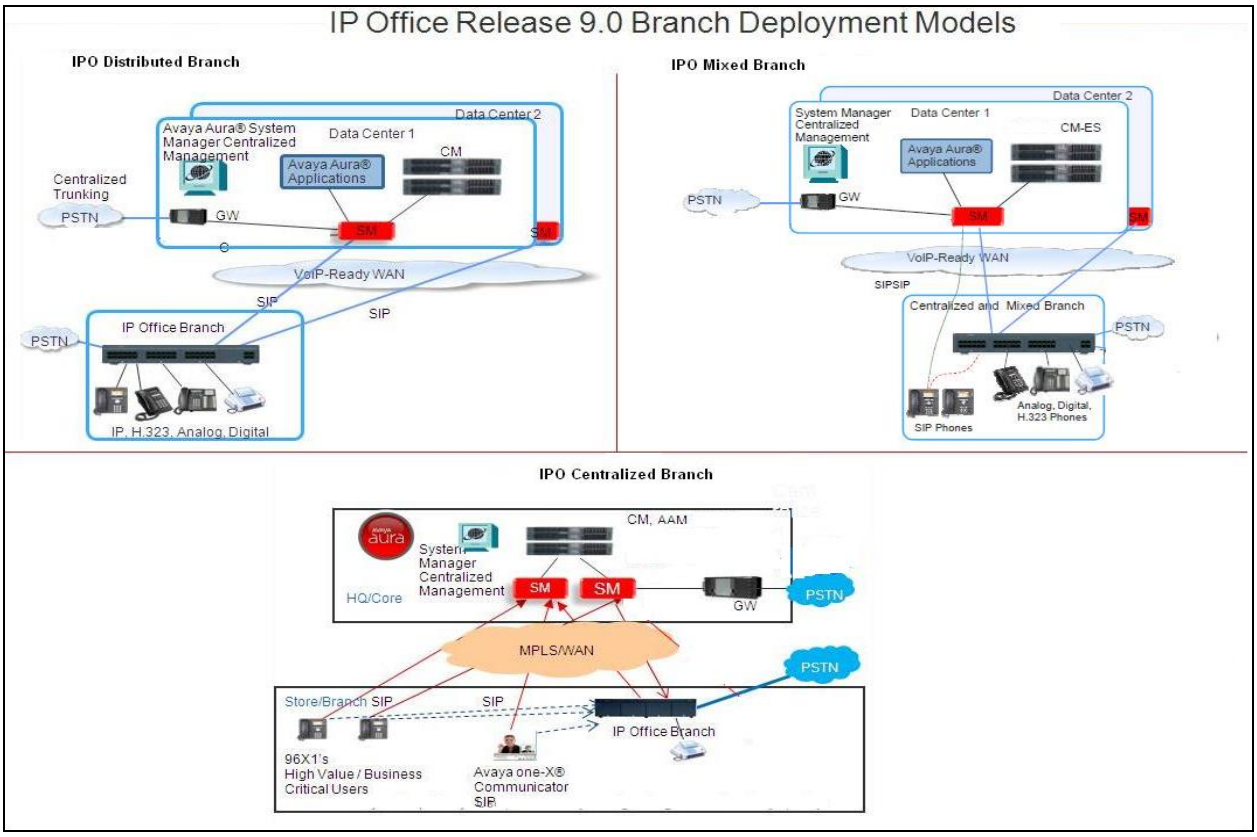


Figure 2: UC Branch Deployment Configuration Models

- 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.

©2014 Avaya Inc. All Rights Reserved

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.

©2014 Avaya Inc. All Rights Reserved

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.

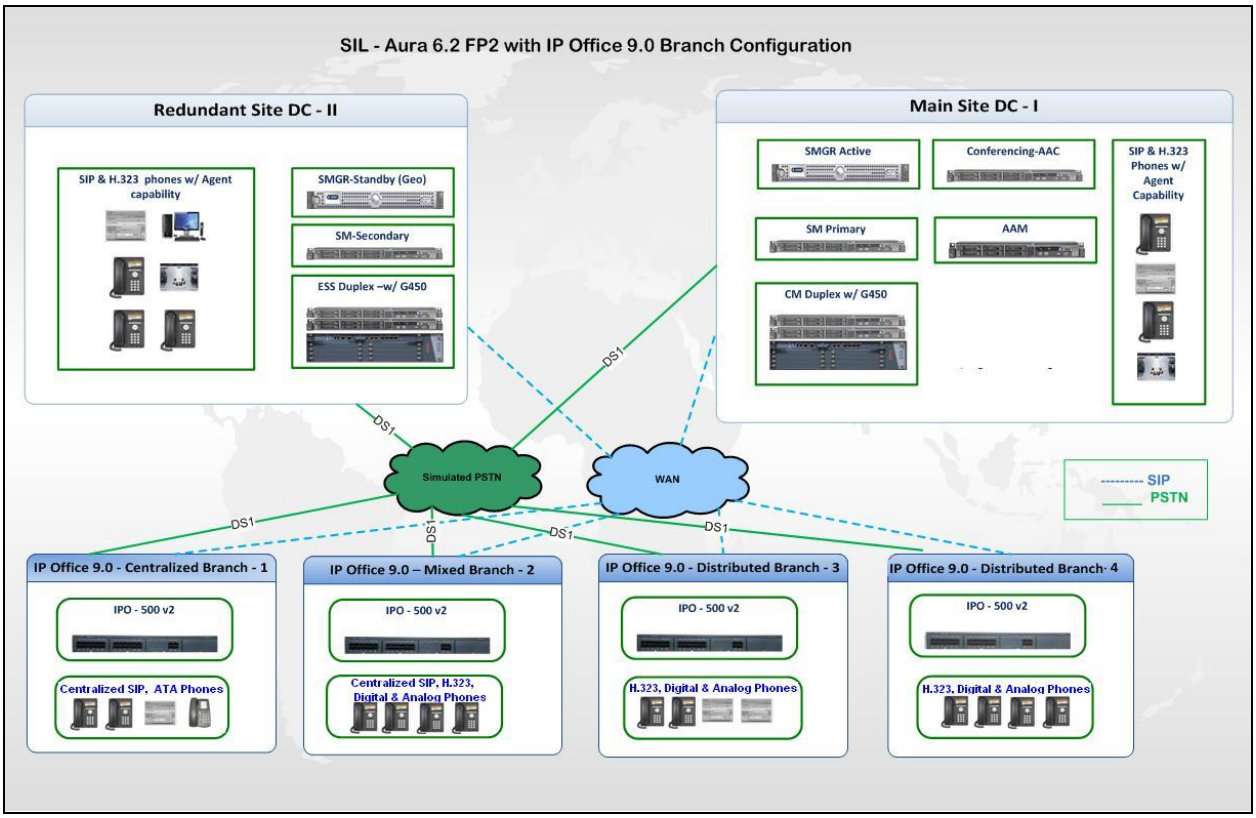


Figure 3: Solution Configuration

©2014 Avaya Inc. All Rights Reserved

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.

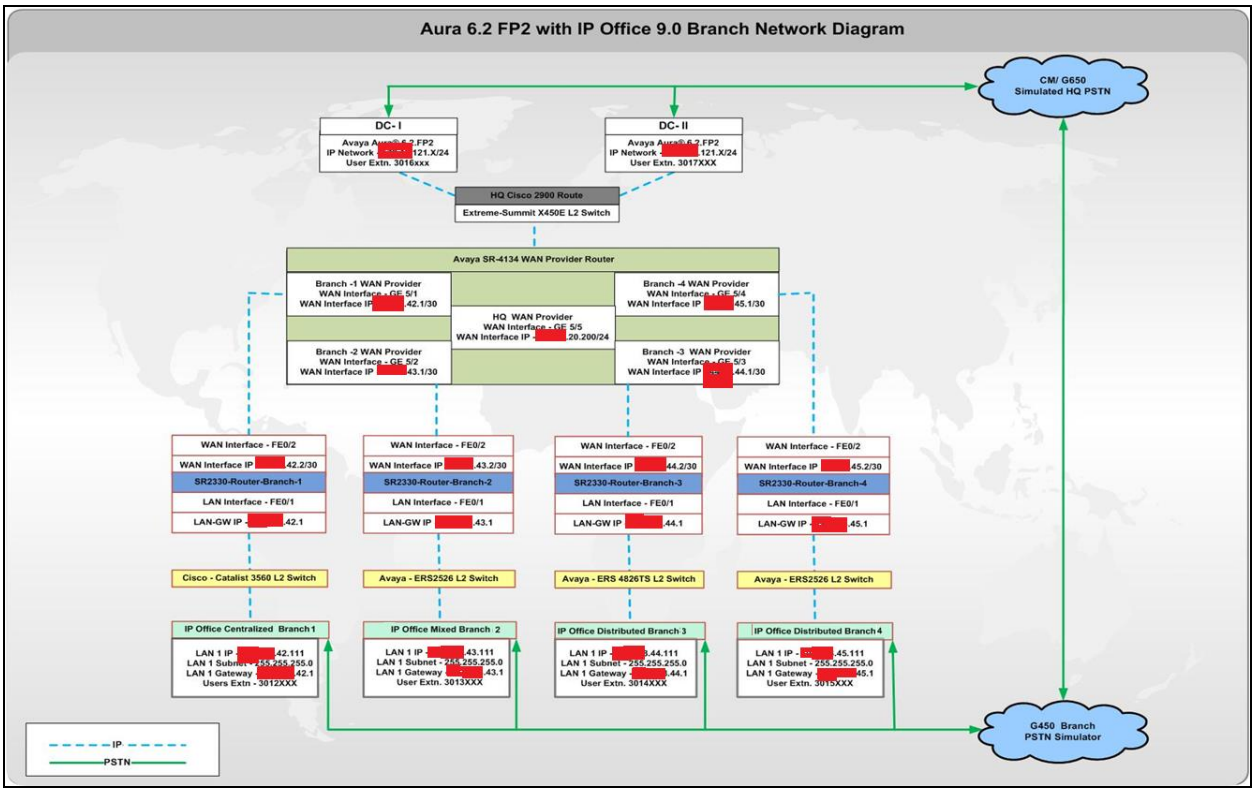


Figure 4: Network Configuration

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.

©2014 Avaya Inc. All Rights Reserved

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.

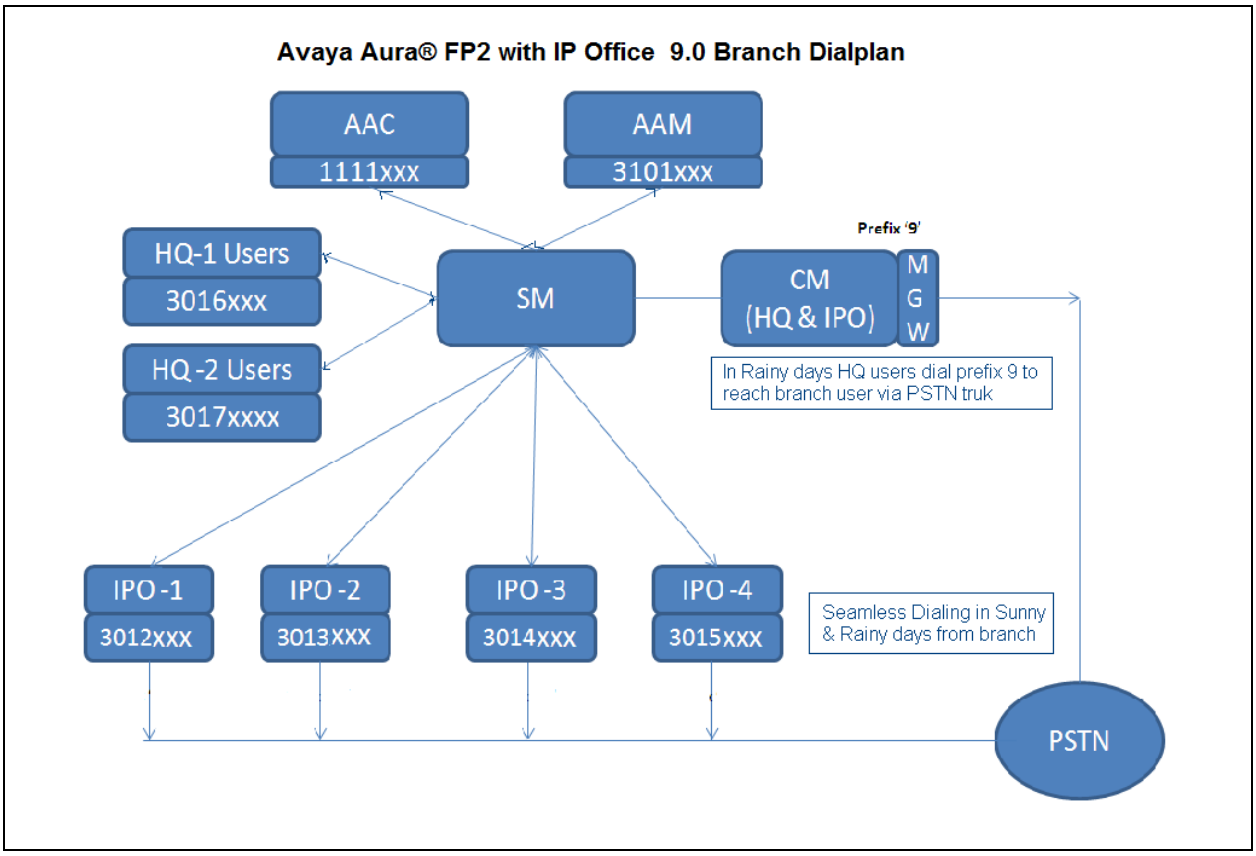


Figure 5: Dialplan Configuration

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

©2014 Avaya Inc. All Rights Reserved

- 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.

©2014 Avaya Inc. All Rights Reserved

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.

©2014 Avaya Inc. All Rights Reserved

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.)
```


©2014 Avaya Inc. All Rights Reserved

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/DA:     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:
```


©2014 Avaya Inc. All Rights Reserved

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
```


©2014 Avaya Inc. All Rights Reserved

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]
```


©2014 Avaya Inc. All Rights Reserved

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              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        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: fp2-sm01
 Near-end Listen Port: 5061                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
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                   IP Audio Hairpinning? y
         Enable Layer 3 Test? y                Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

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

©2014 Avaya Inc. All Rights Reserved

6.7. Configure Trunk Group

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.

- **Group Type:** sip
- **Group Name:** A descriptive name
- **TAC:** An available trunk access code i.e. #**001**
- **Service Type:** tie
- **Signaling Group:** signaling group number added in the **section 6.6**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks available from licensed verified **in Section 6.1**).

```
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
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n
                                        Member Assignment Method: auto
                                                  Signaling Group: 1
                                                Number of Members: 255
```

Repeat the above steps to configure **trunk group 2** for Secondary Session Manager.

6.8. Configure Route Pattern

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.

```
change route-pattern 1                                        Page   1 of   3
                     Pattern Number: 1       Pattern Name: RP1
                                  SCCAN? n      Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/  IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                                 Dgts                               Intw
 1: 1   0                                                            n    user
 2: 2   0                                                            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
 3: y y y y y n   n           rest                                            none
 4: y y y y y n   n           rest                                            none
 5: y y y y y n   n           rest                                            none
 6: y y y y y n   n           rest                                            none
```


©2014 Avaya Inc. All Rights Reserved

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

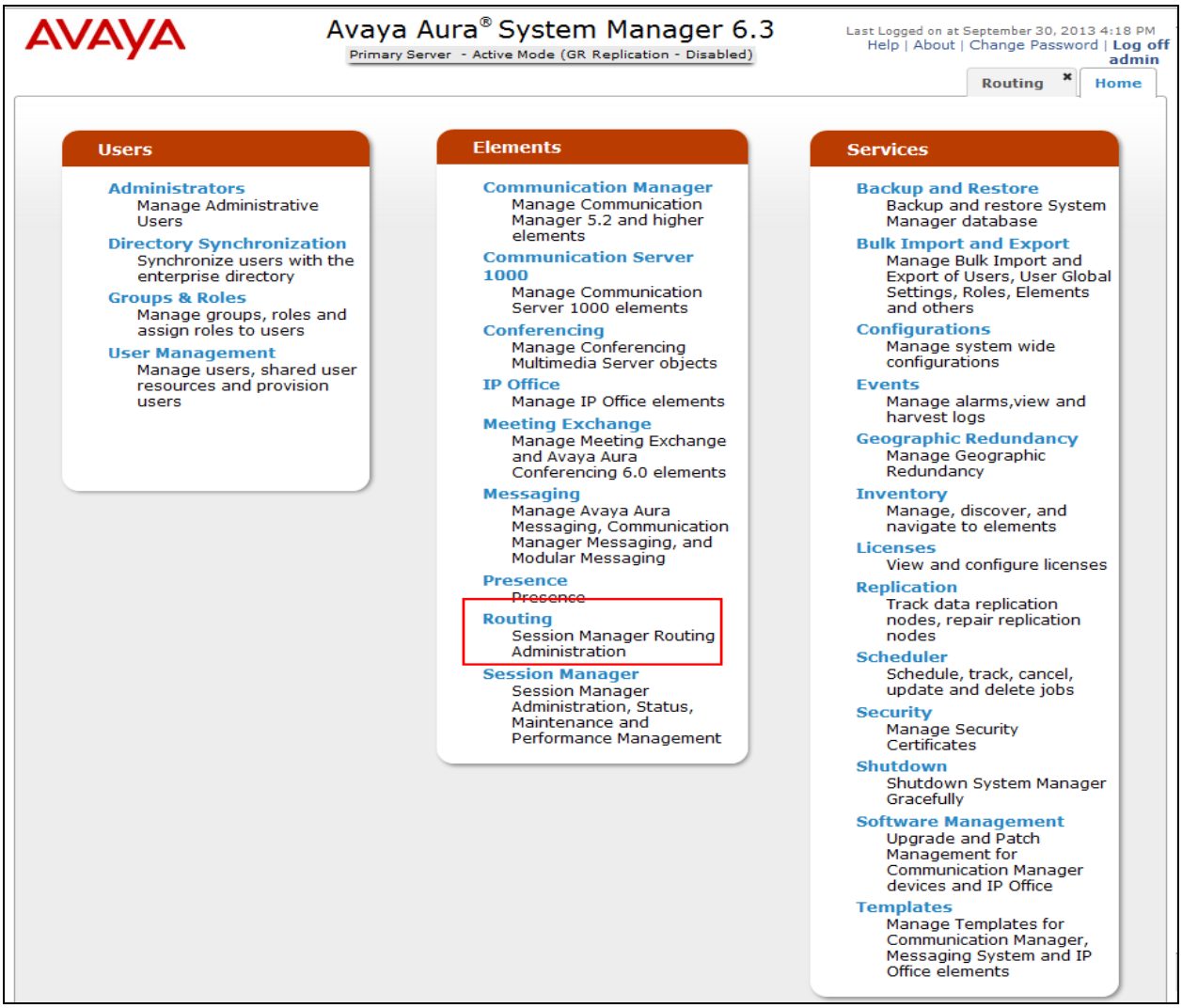
This section provides the procedures for configuring Avaya Aura® Session Manager as provisioned in the sample configuration.

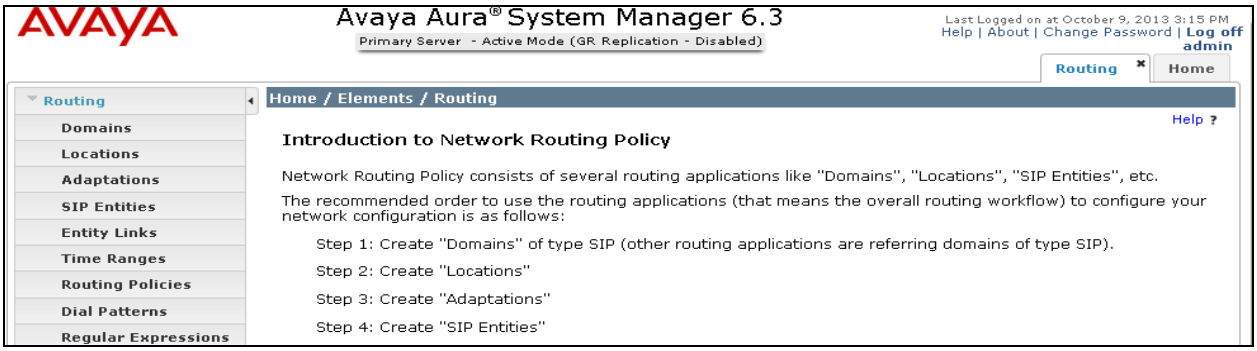
The procedures described in this section include configurations in the following areas:

- 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

©2014 Avaya Inc. All Rights Reserved

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.





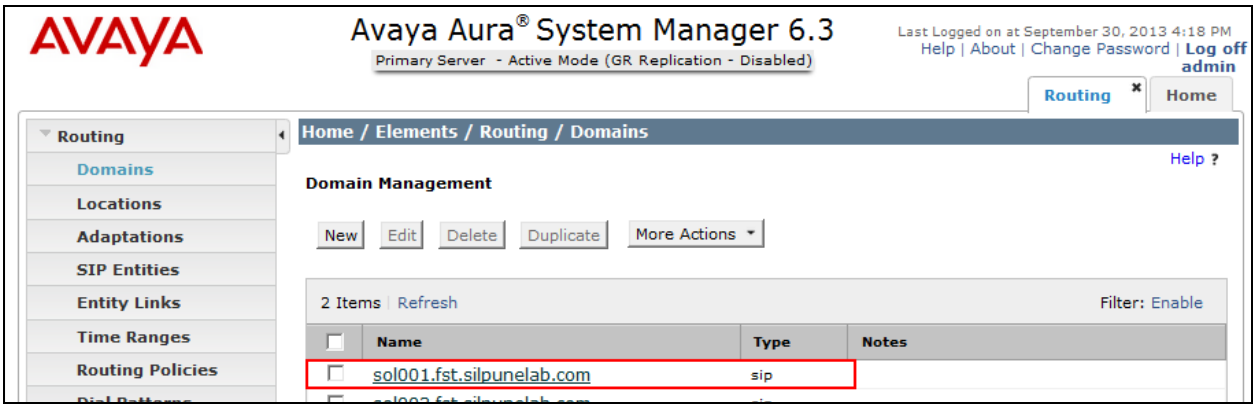
©2014 Avaya Inc. All Rights Reserved

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

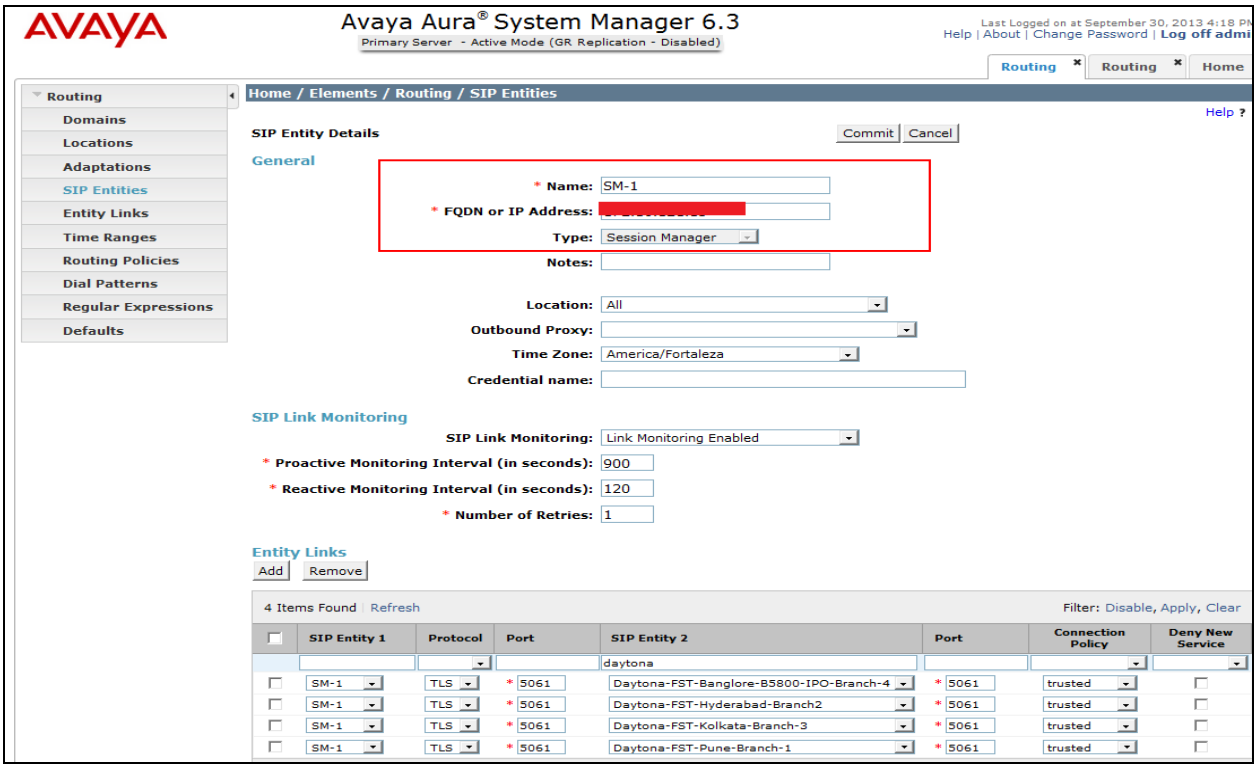
Under **Port** (for adding Session Manager Entity only), click **Add**, and then edit the fields in the resulting new row as shown below:

- **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**

©2014 Avaya Inc. All Rights Reserved

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

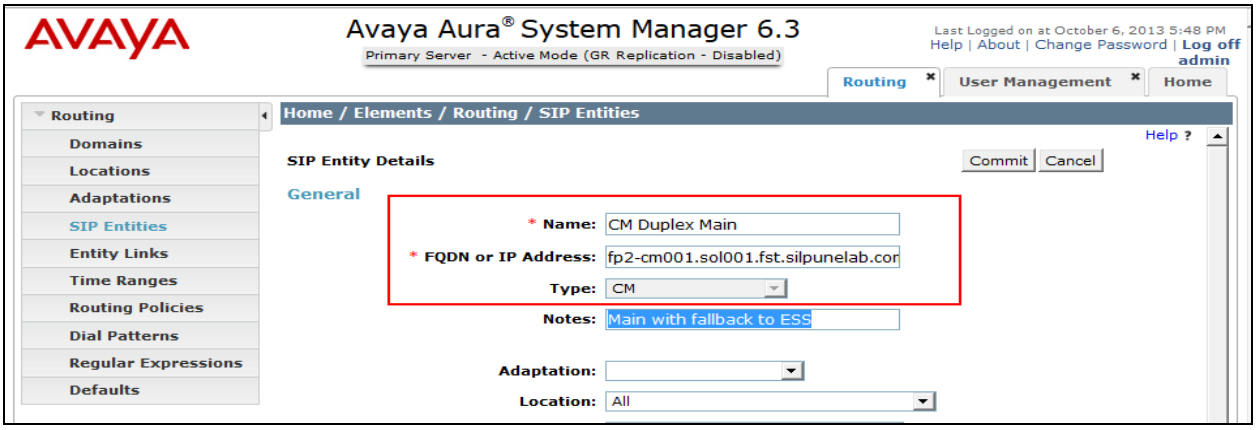
The following screen shows the addition of Session Manager. The IP address of the SIP signaling interface is entered for **FQDN or IP Address**.



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.

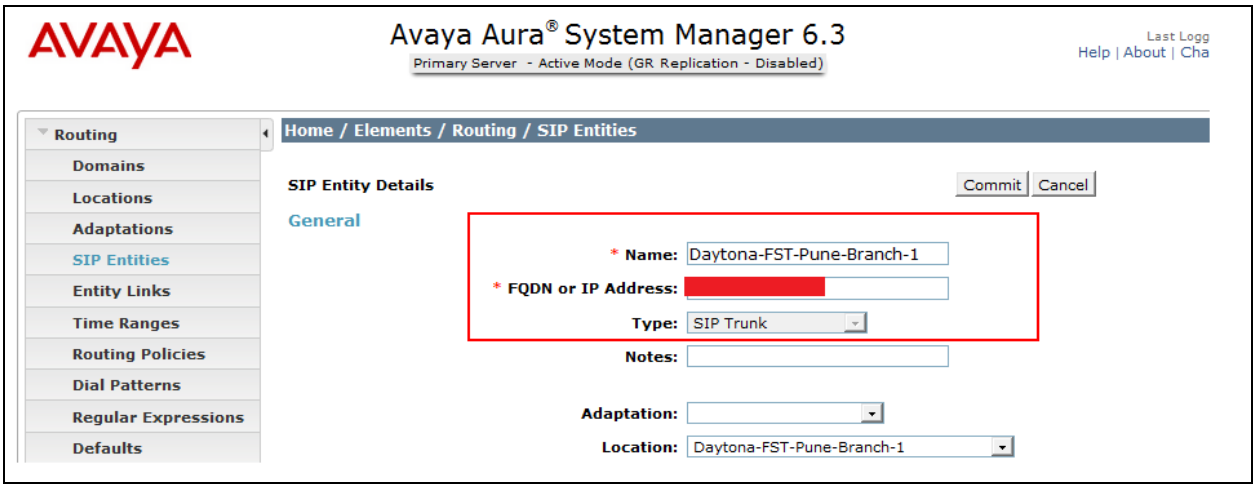
Note: the **CM** selection for the field **Type**.



©2014 Avaya Inc. All Rights Reserved

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**.



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.

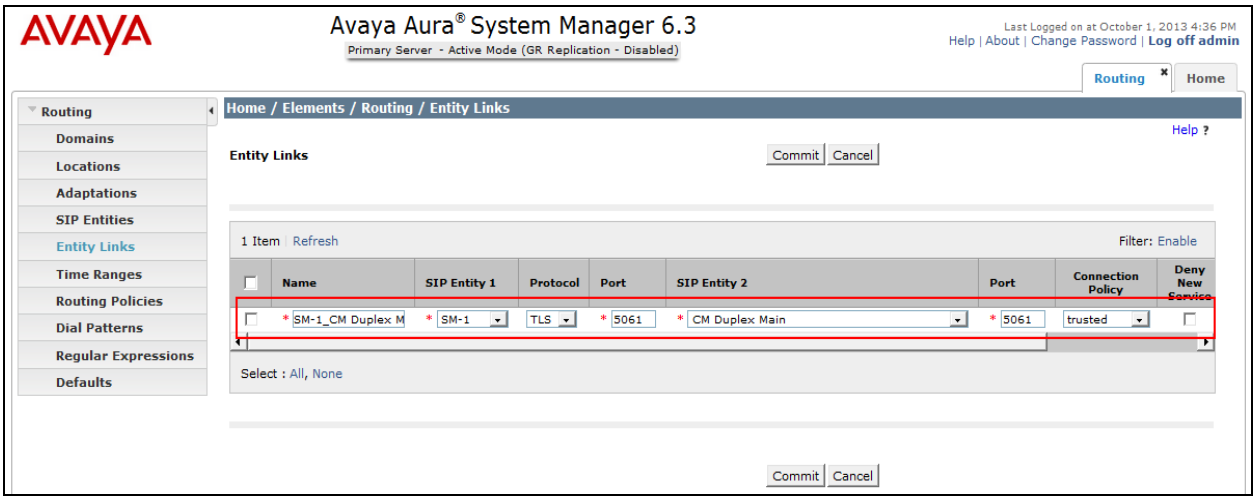
To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **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

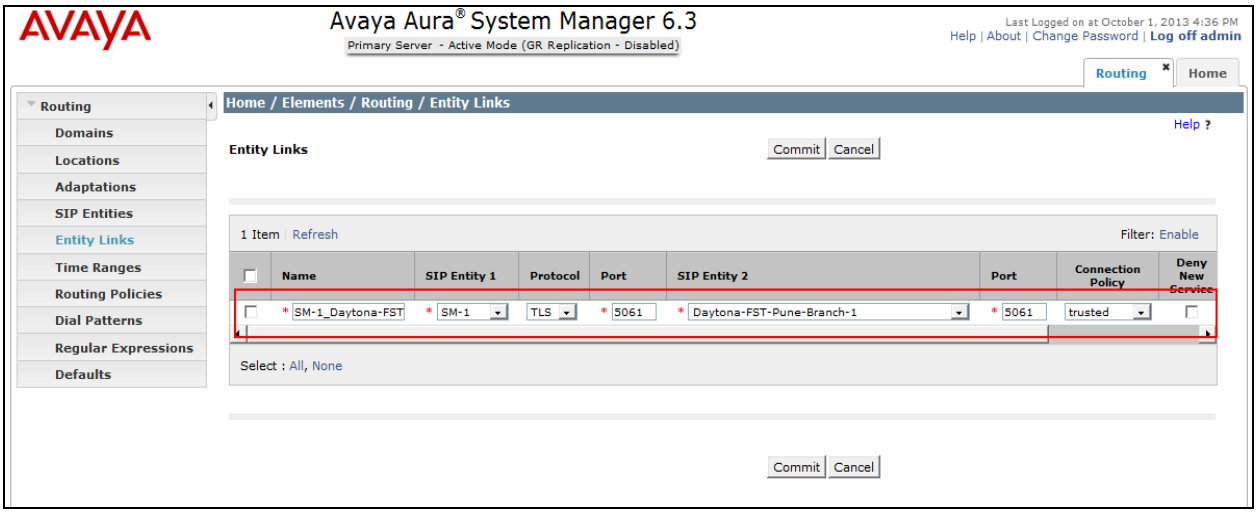
Click **Commit** to save the configuration.

©2014 Avaya Inc. All Rights Reserved

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



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



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

©2014 Avaya Inc. All Rights Reserved

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)

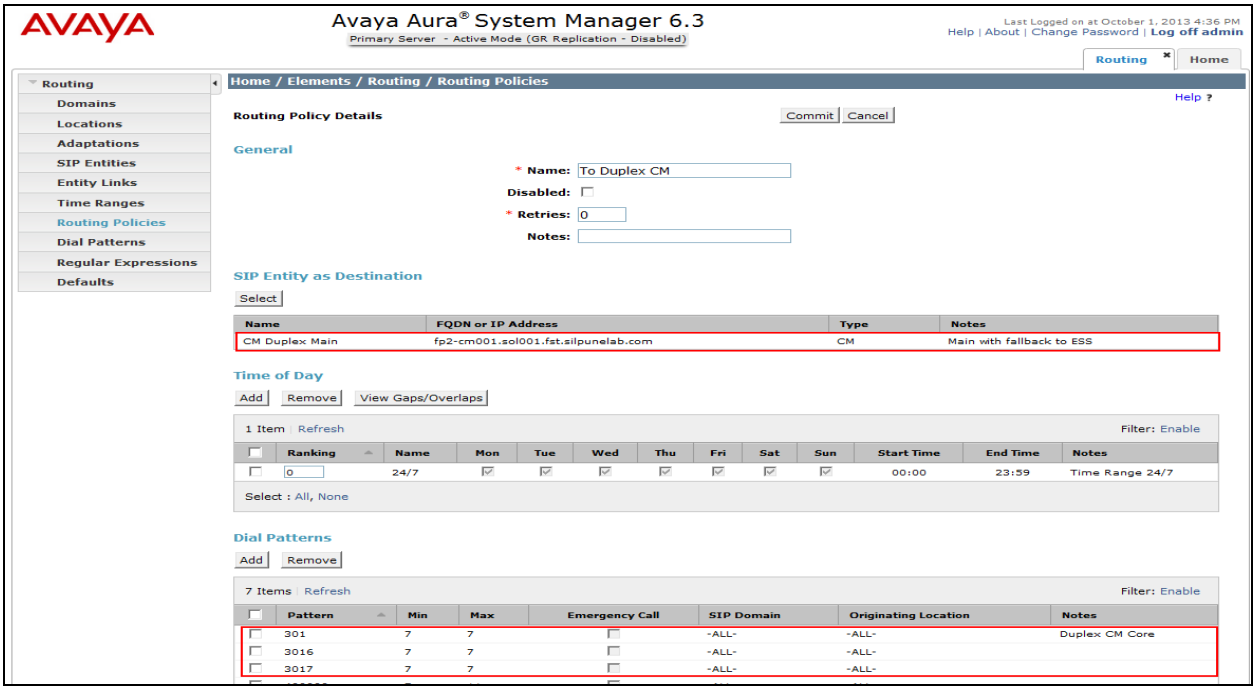
Under **Time of Day**:

- 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.

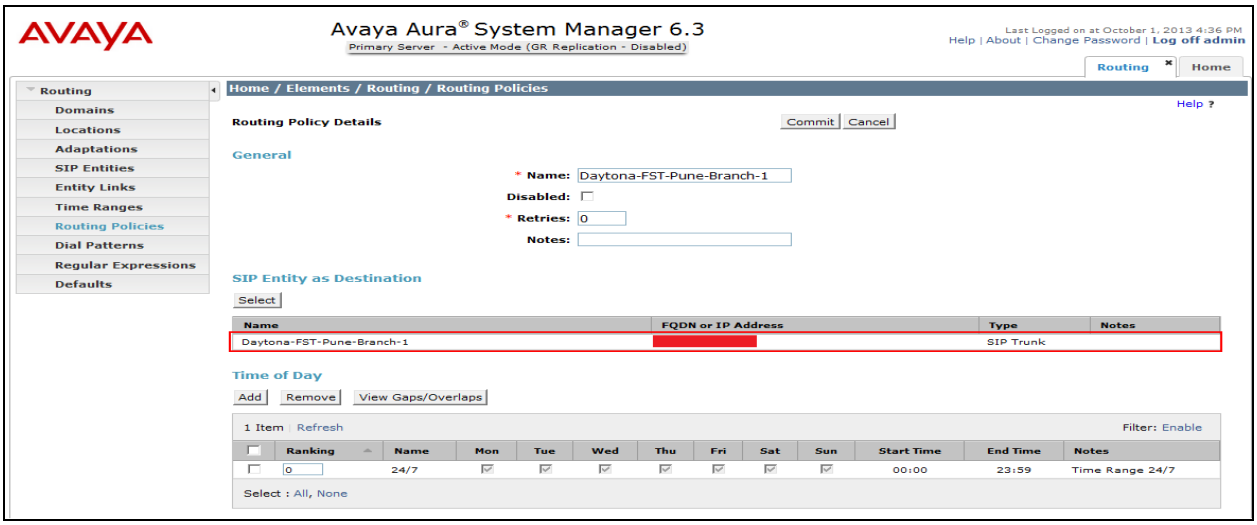
The following screen shows the Routing Policy for routing calls from Avaya IP Office to non-SIP phones registered/connected with Communication Manager named **Duplex CM** at the HQ location. This same Routing Policy can also be used for routing PSTN calls to the HQ location where **Duplex CM** would send these calls through the central T1/E1 trunks to the PSTN[1].



[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.

©2014 Avaya Inc. All Rights Reserved

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.



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 stings 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**:

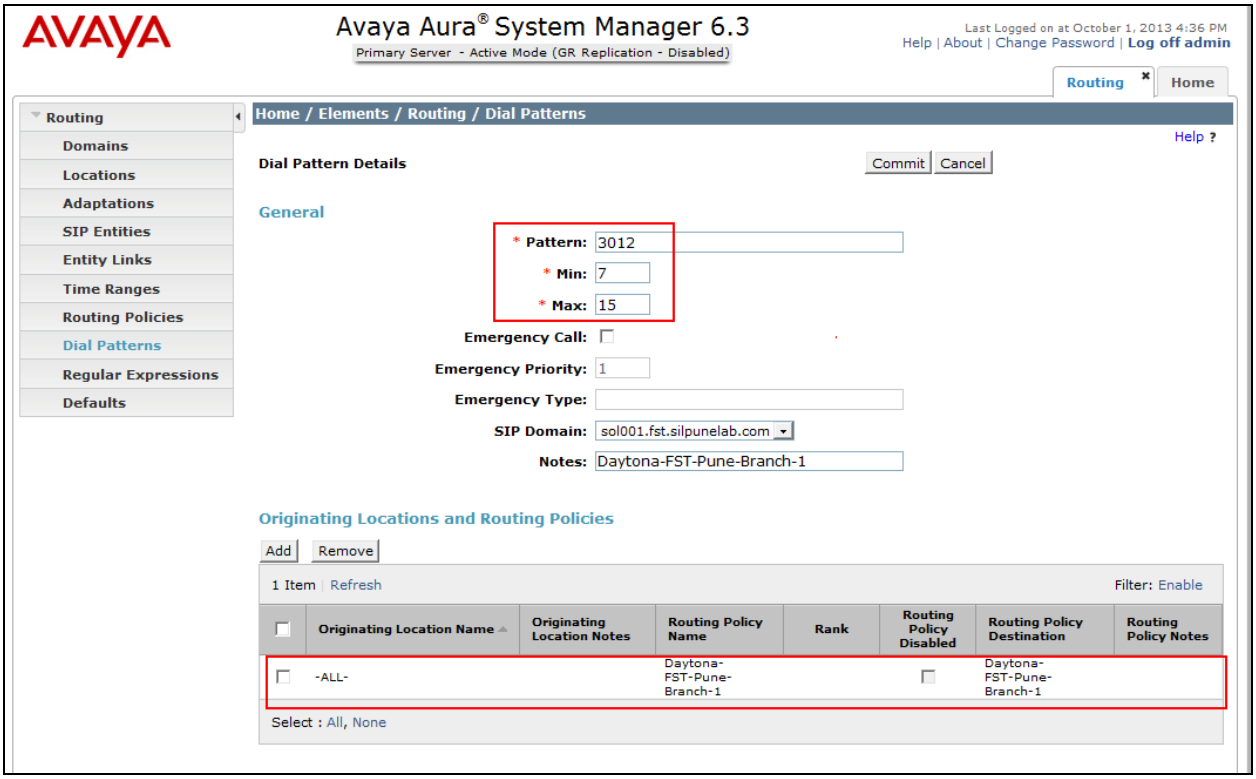
- **Pattern**: Dialed number or prefix
- **Min**: Minimum length of dialed number
- **Max**: Maximum length of dialed number
- **SIP Domain**: SIP domain specified in **Section 7.1**
- **Notes**: Comment on purpose of dial pattern.

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.

©2014 Avaya Inc. All Rights Reserved

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



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

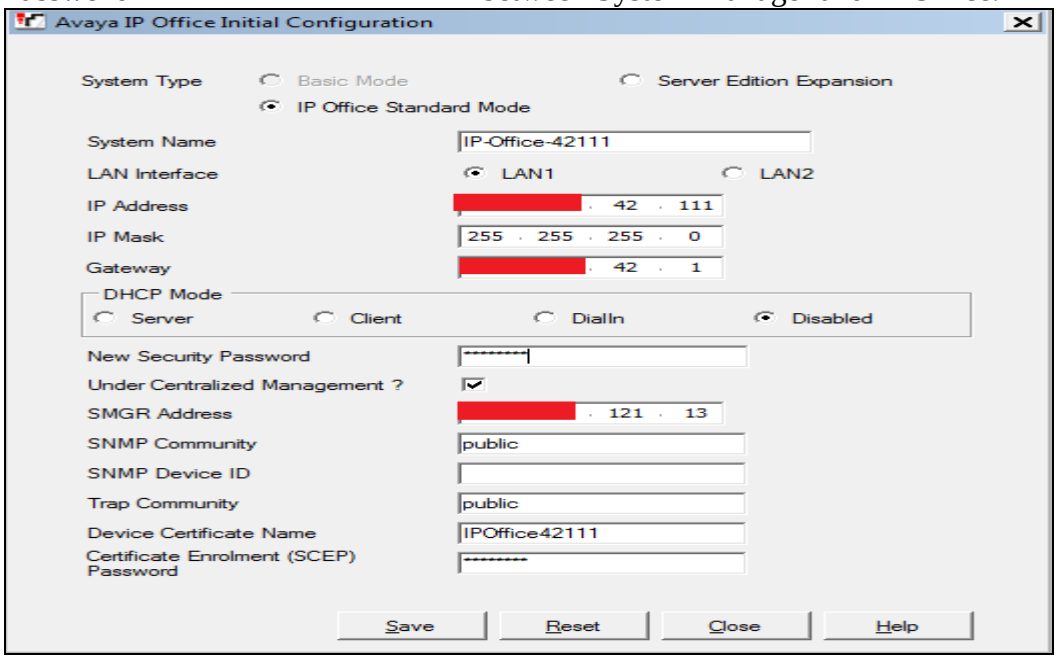
8.1. Access IP Office ICU (Initial Configuration Utility)

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.

©2014 Avaya Inc. All Rights Reserved

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.



©2014 Avaya Inc. All Rights Reserved

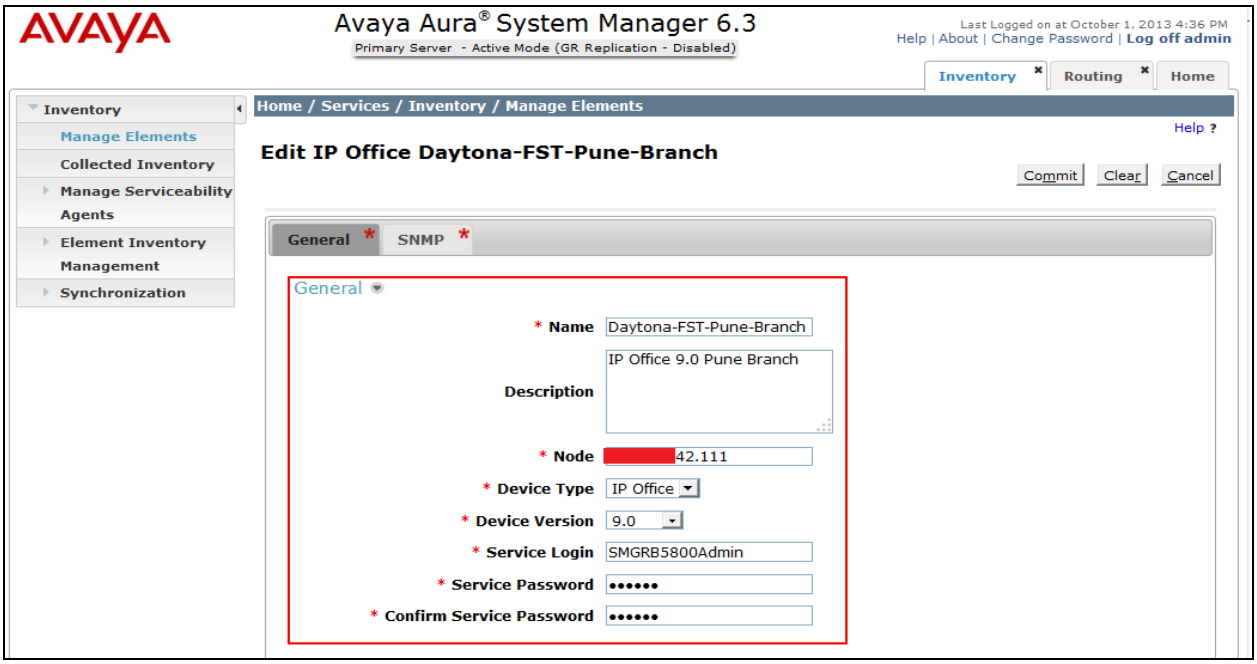
After entering the above details click **Save**, and IPO will reboot. Once IP Office comes up again, launch IPO Manager, access IP Office and verify above details are reflected properly on IP Office.

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.

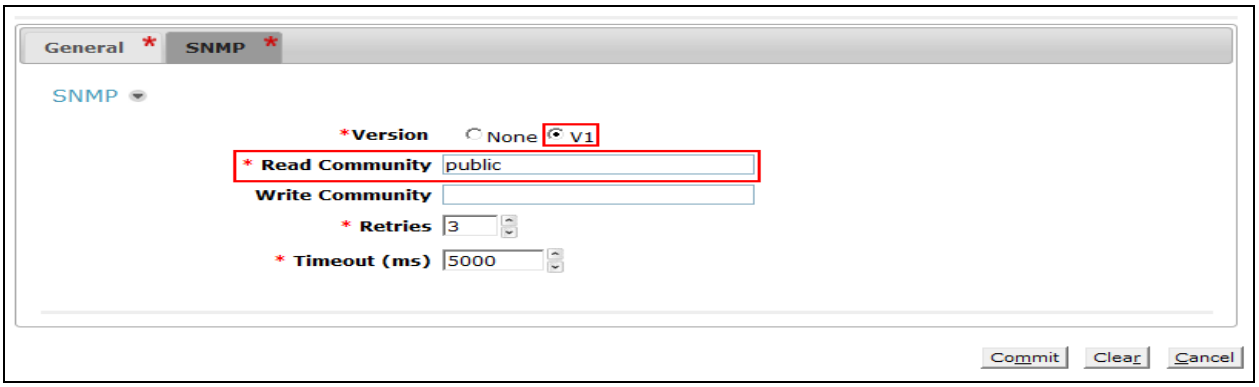


©2014 Avaya Inc. All Rights Reserved

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

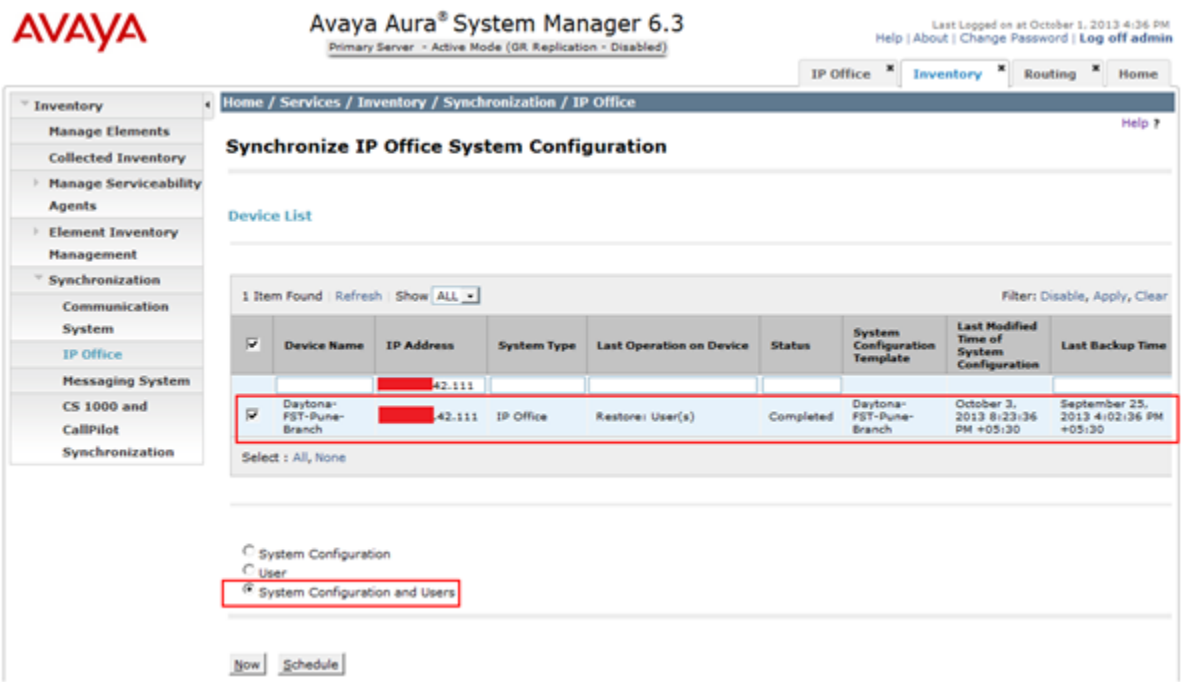
- Select version as "**V1**" and Read Community as "**public**".

Click on the **Commit** button.



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

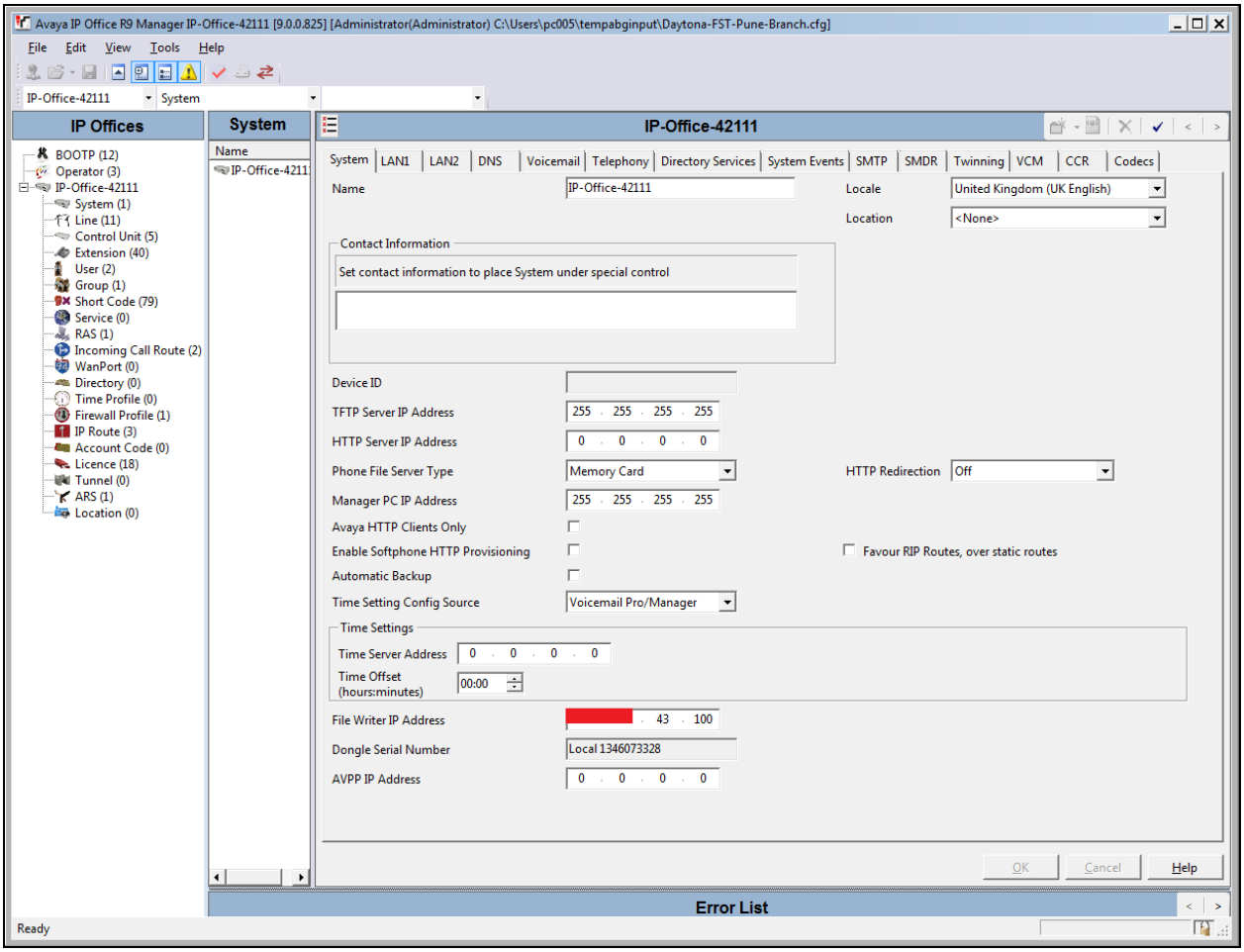
Go to **System Manager→Services→Inventory→Synchronization→IP Office**, select **IP Office**. Select the **System Configuration and Users** and click on the **New** button (not shown). Verify that this operation is successful and the **Status** column should get updated with **Completed** status.



©2014 Avaya Inc. All Rights Reserved

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

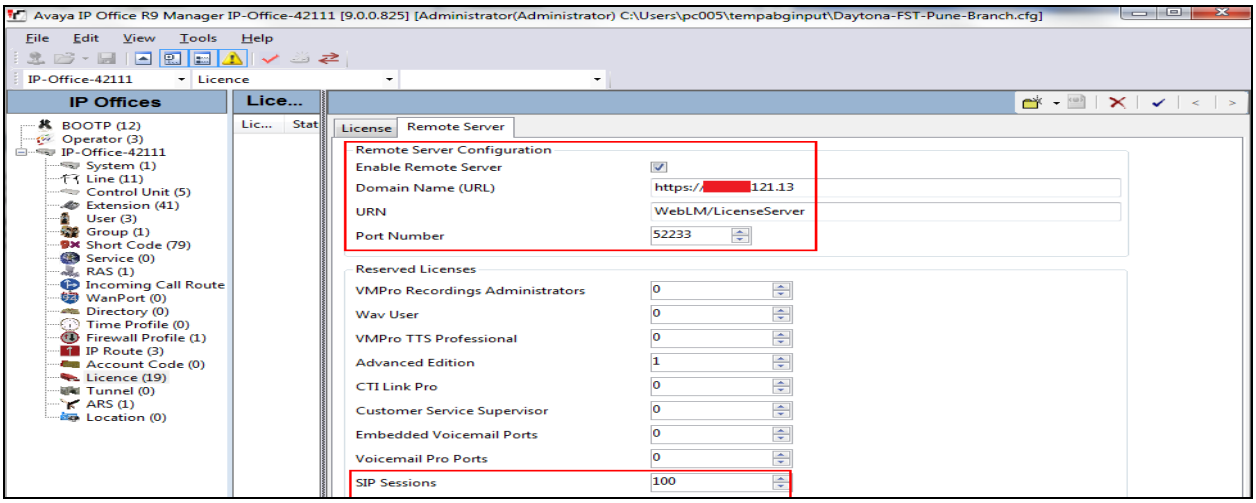
Go to **SMGR→Elements→IP Office→System Configuration**, click on the **Edit** button (not shown). The IP Office manager window will be launched as displayed below. From the configuration tree in the left pane, select **License** and select **Remote Server** tab to configure the following:

- **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

©2014 Avaya Inc. All Rights Reserved

	Port **52233**.
• **SIP Session**	Enter value as per licenses on license server. Maximum value can be **100**.

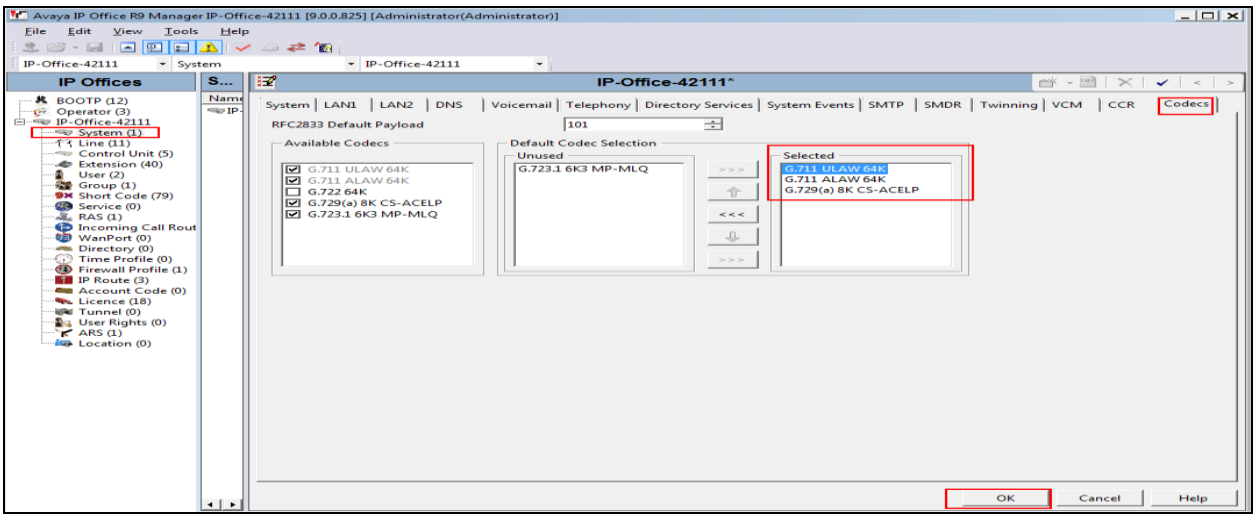
Click on the **OK** button and click **Save** button to save configuration (not shown).



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).



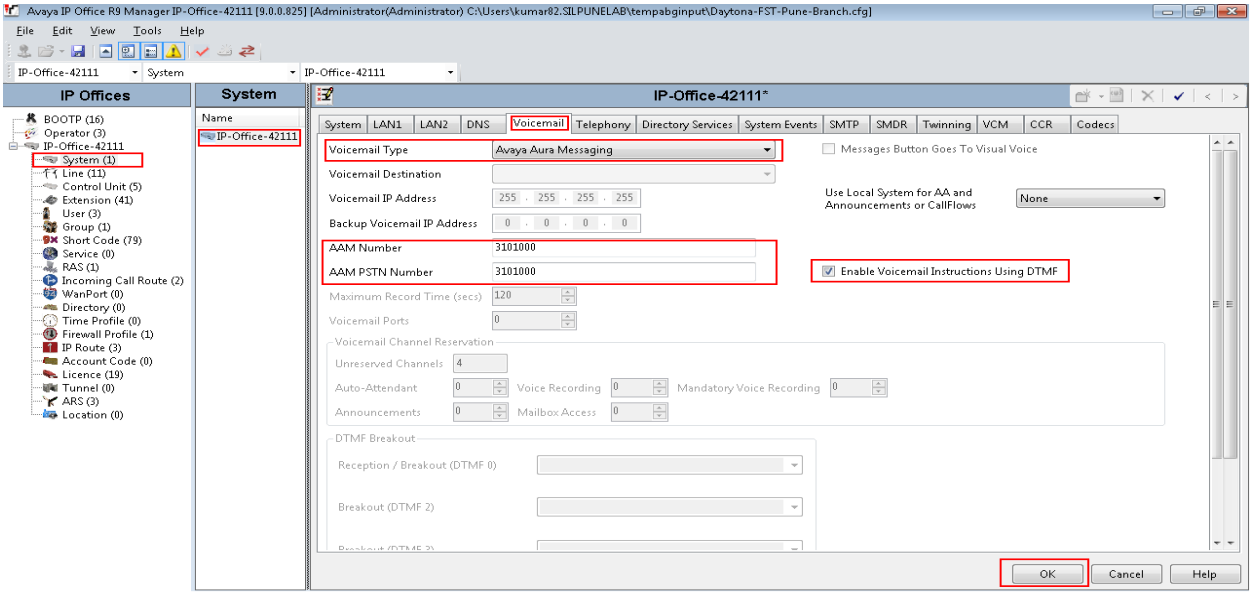
©2014 Avaya Inc. All Rights Reserved

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

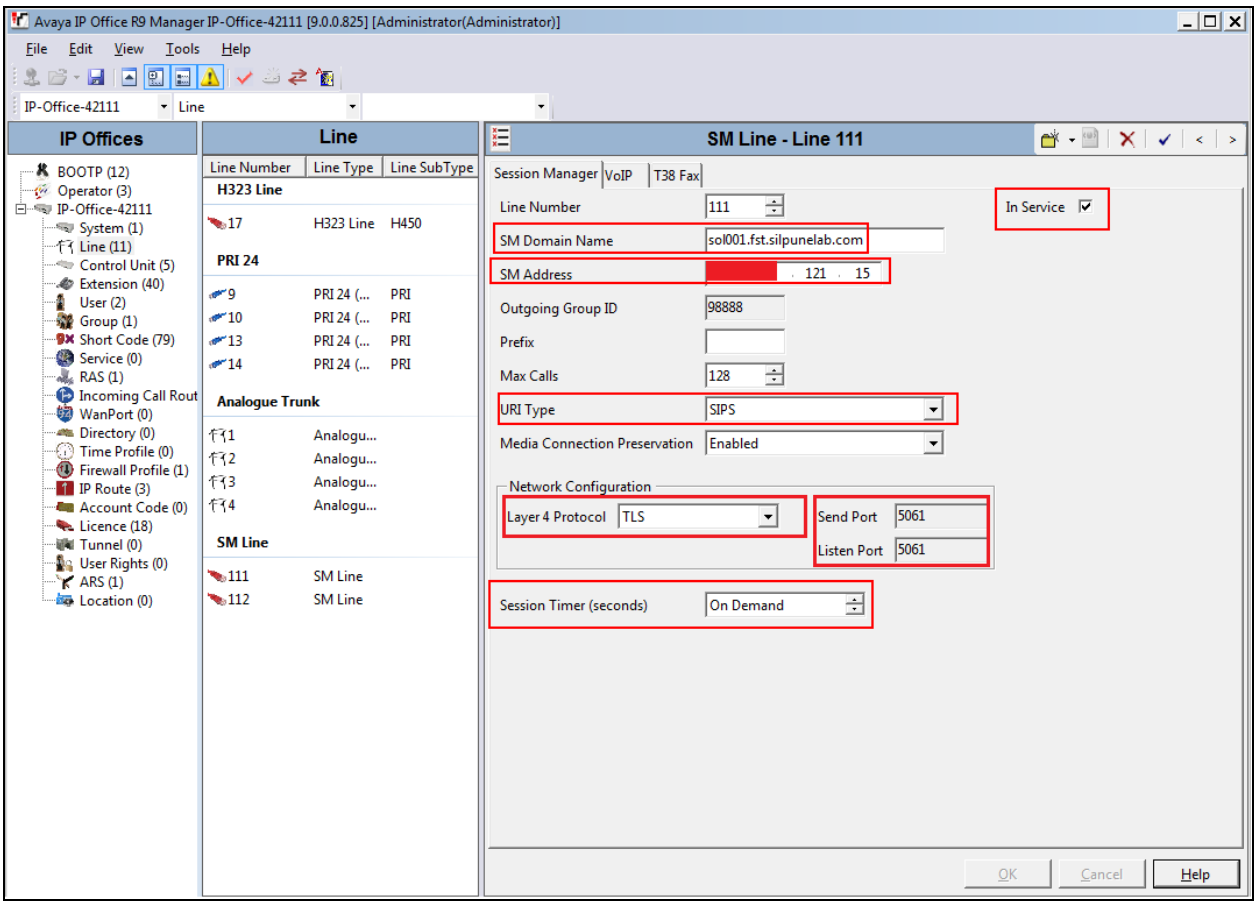
Avaya IP Office uses a special type of SIP trunk to communicate with Avaya Aura® Session Manager called an **SM Line**. From the configuration tree in the left pane, right-click on **Line** and select **New SM Line** to add an instance.

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.

©2014 Avaya Inc. All Rights Reserved

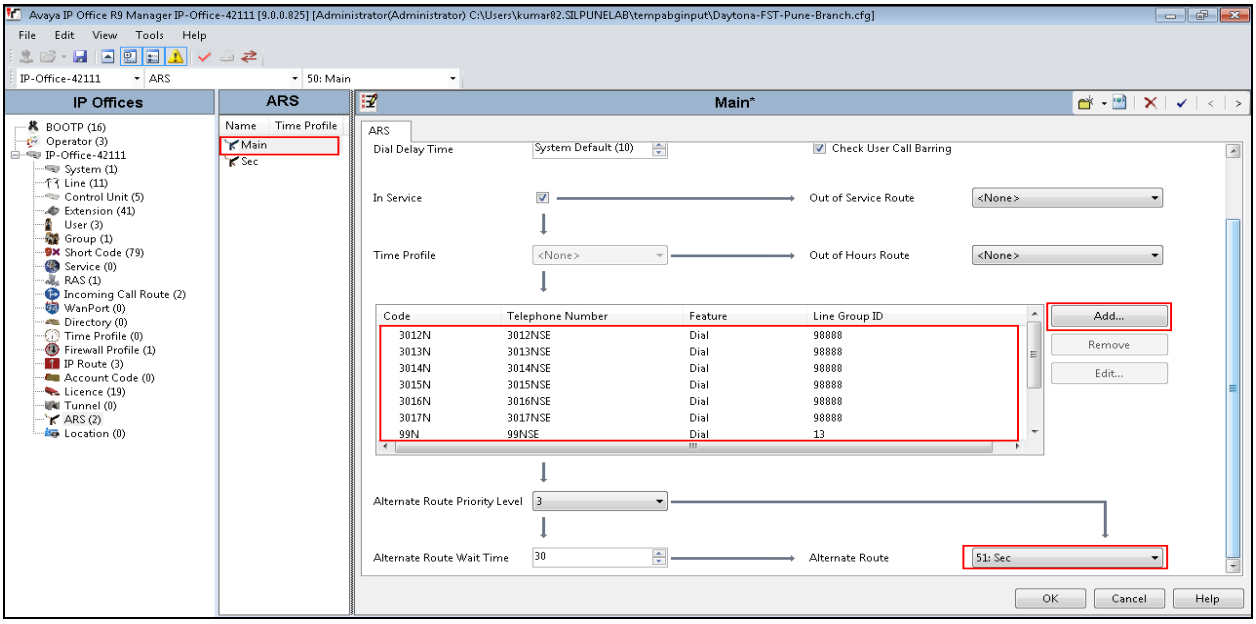
- **Outgoing GroupID:** **98888**. While this value is not adjustable it should be noted as it will be used for routing calls to Session Manager via Short Codes.
- **Max Calls:** **128** was used in the reference configuration. This entry should not exceed licensed value.
- **URI Type:** **SIPS** was 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.



©2014 Avaya Inc. All Rights Reserved

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)**.**



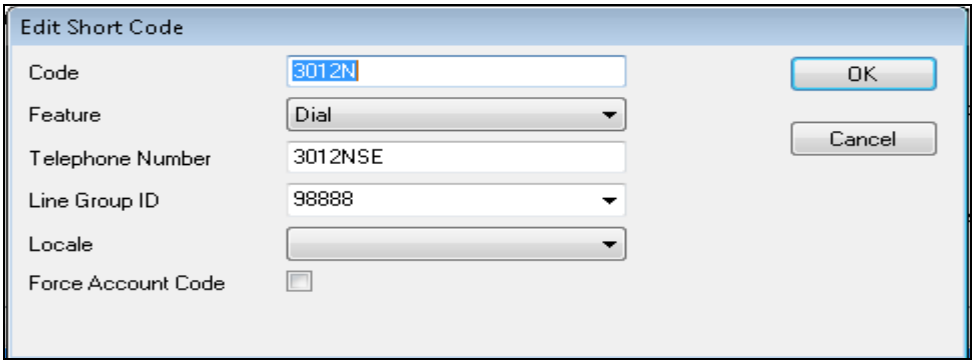
In the **ARS** tab the following information is entered.

- **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

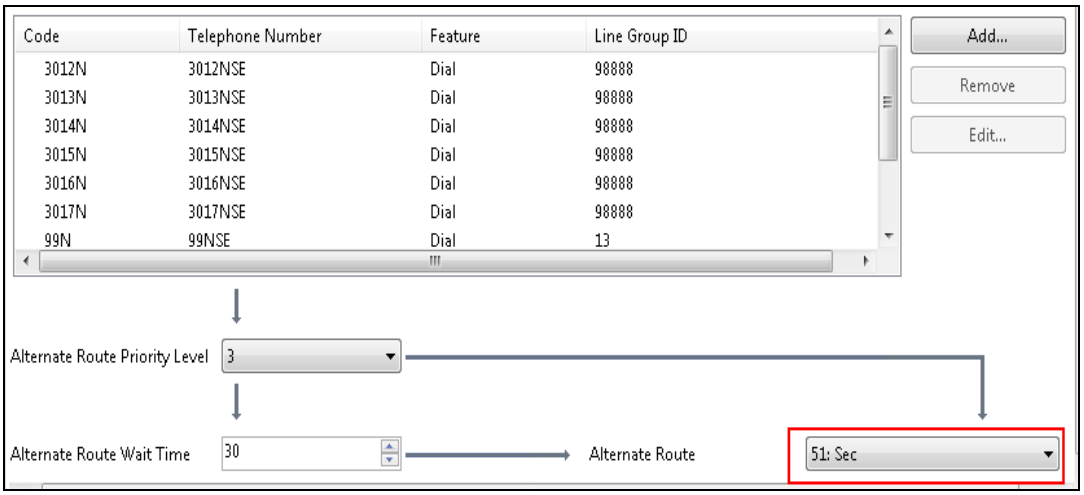
Click the **OK** button.



©2014 Avaya Inc. All Rights Reserved

Repeat above steps to create secondary ARS routing for PSTN trunk

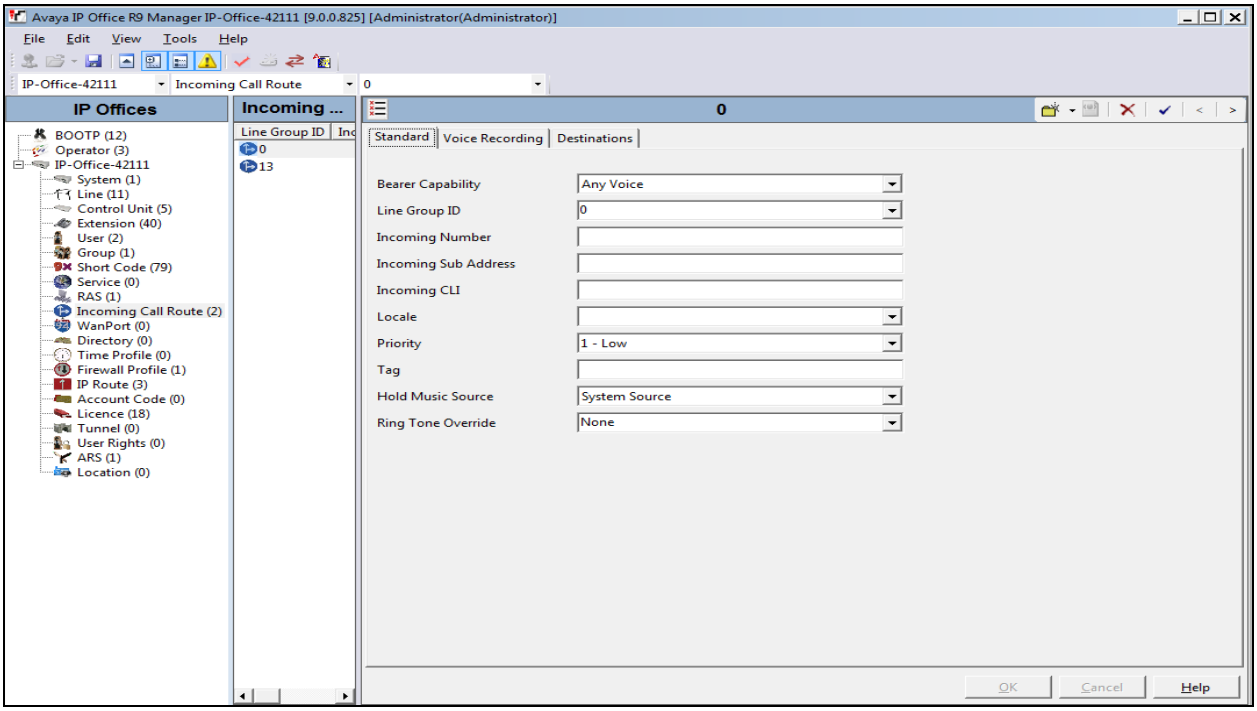
On main ARS window select the secondary ARS route from the **Alternate Route** drop down box.



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).

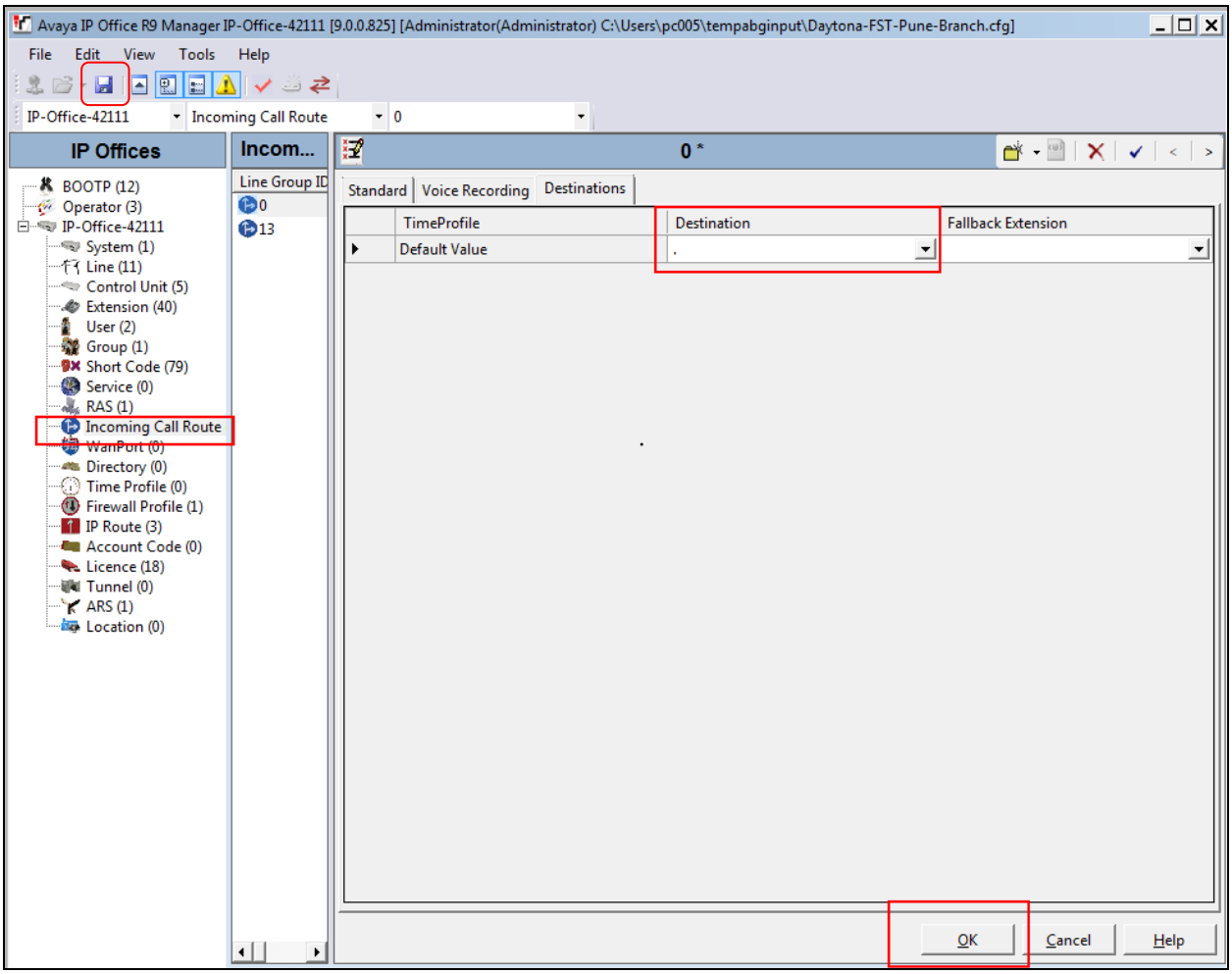
- Retain the default for values for the fields on the **Standard tab**



©2014 Avaya Inc. All Rights Reserved

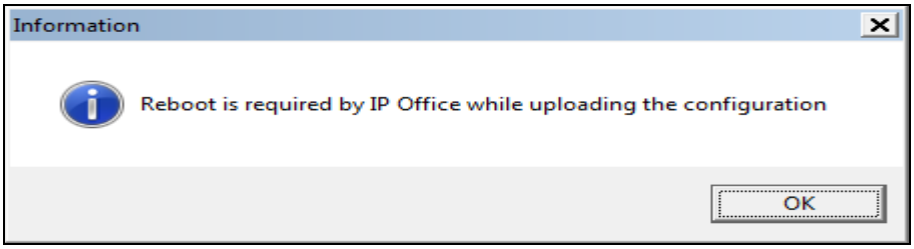
Click on **Destination** tab and put "**.**" in the destination text box, to allow all calls to Avaya IP Office.

Click **OK**.



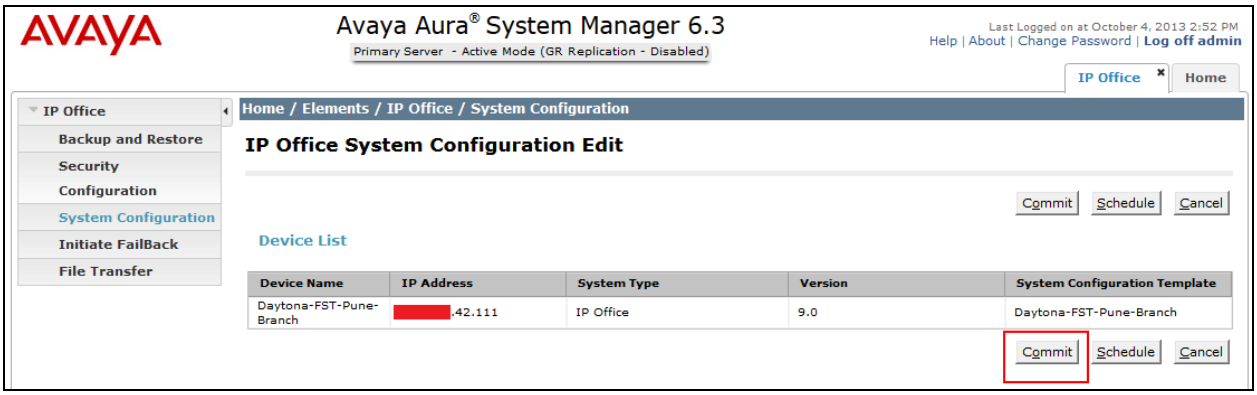
Now click on the **Save** button as highlighted in the previous screen shot at the top menu bar. The **Information** window will appear as shown below to indicate a reboot is required.

Click **OK**.

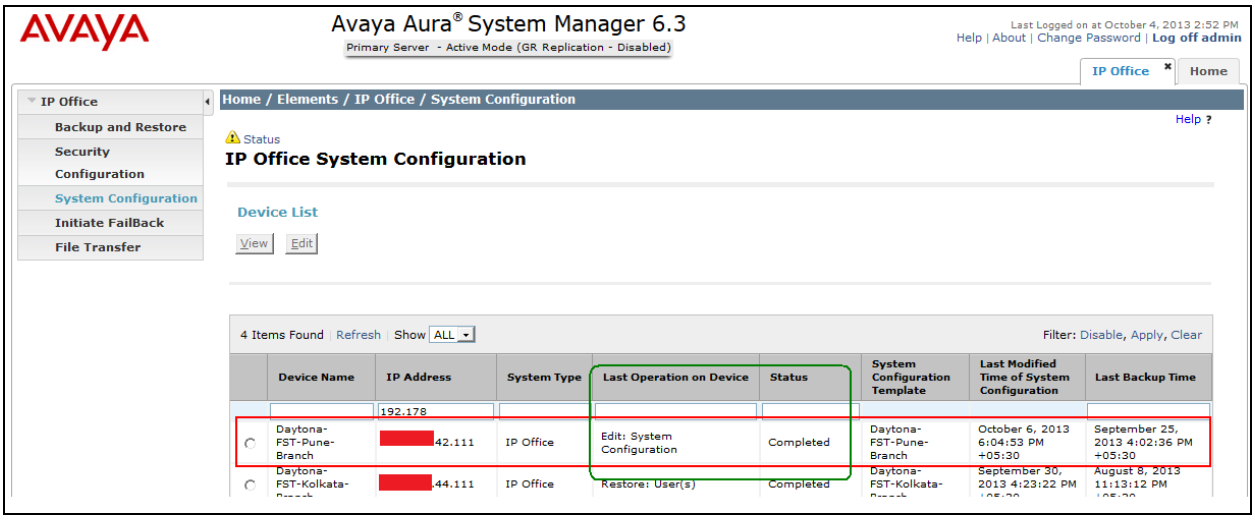


©2014 Avaya Inc. All Rights Reserved

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.



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.



©2014 Avaya Inc. All Rights Reserved

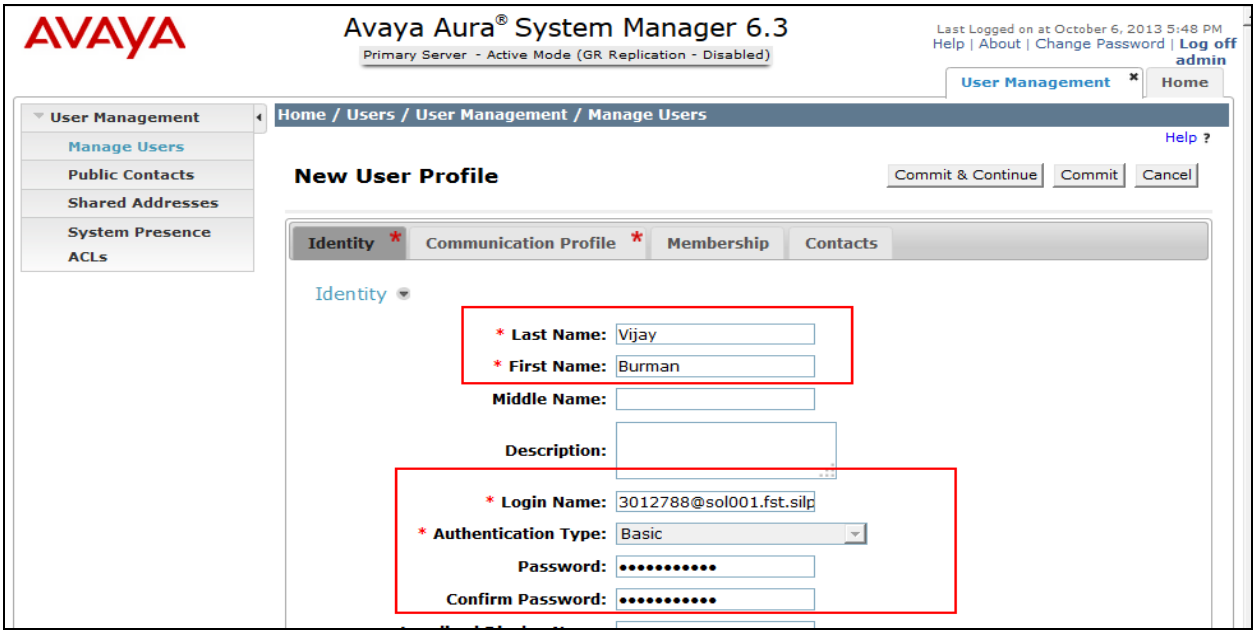
8.5. Configure Centralized SIP Users for IP Office Branch Using System Manager

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.

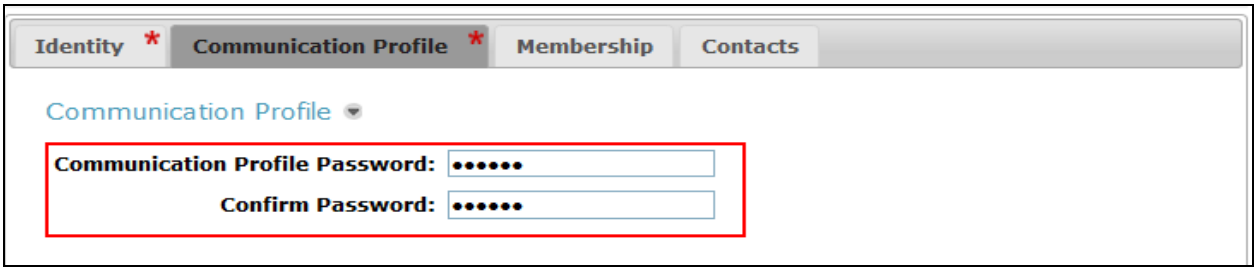
To create Avaya IP Office SIP extension for SIP, log in to System Manager webpage with administrator credentials as described in **Section 7**.

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

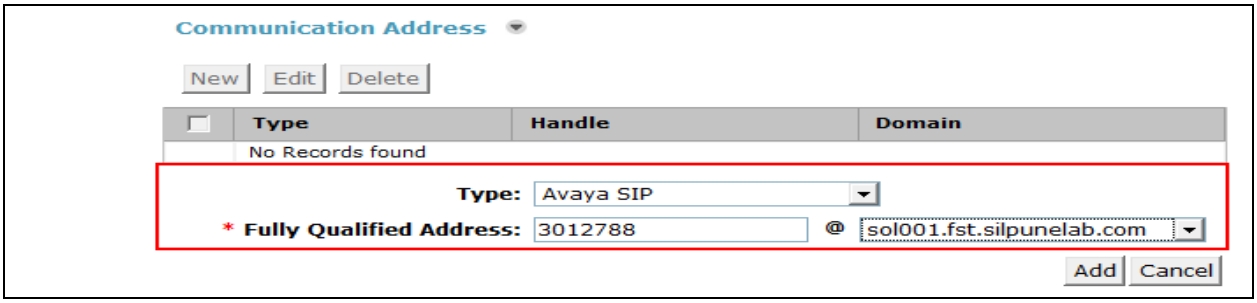


Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.

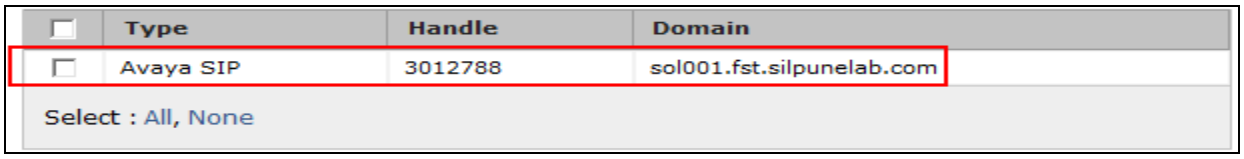


©2014 Avaya Inc. All Rights Reserved

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

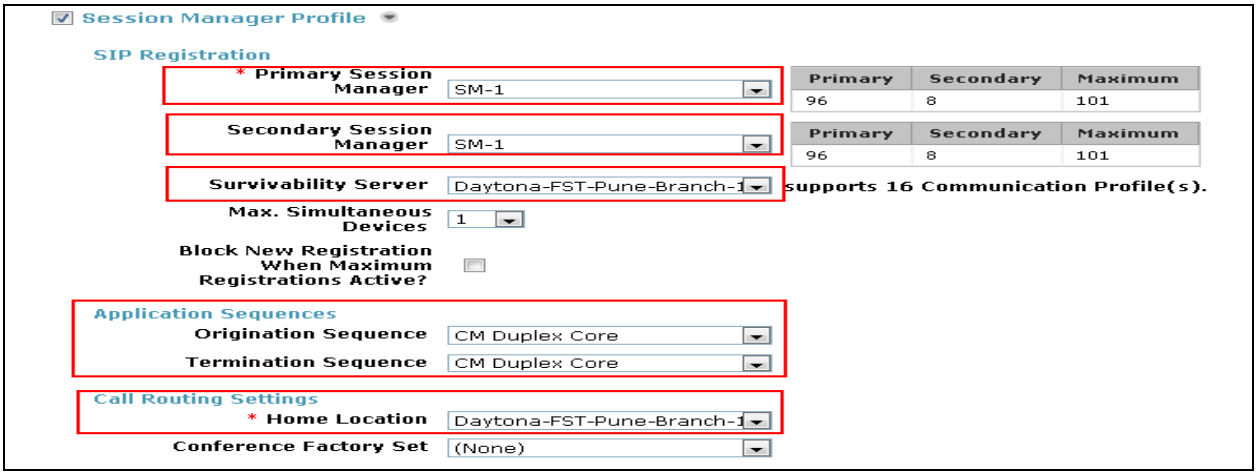


The Communication Address is now displayed.



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.

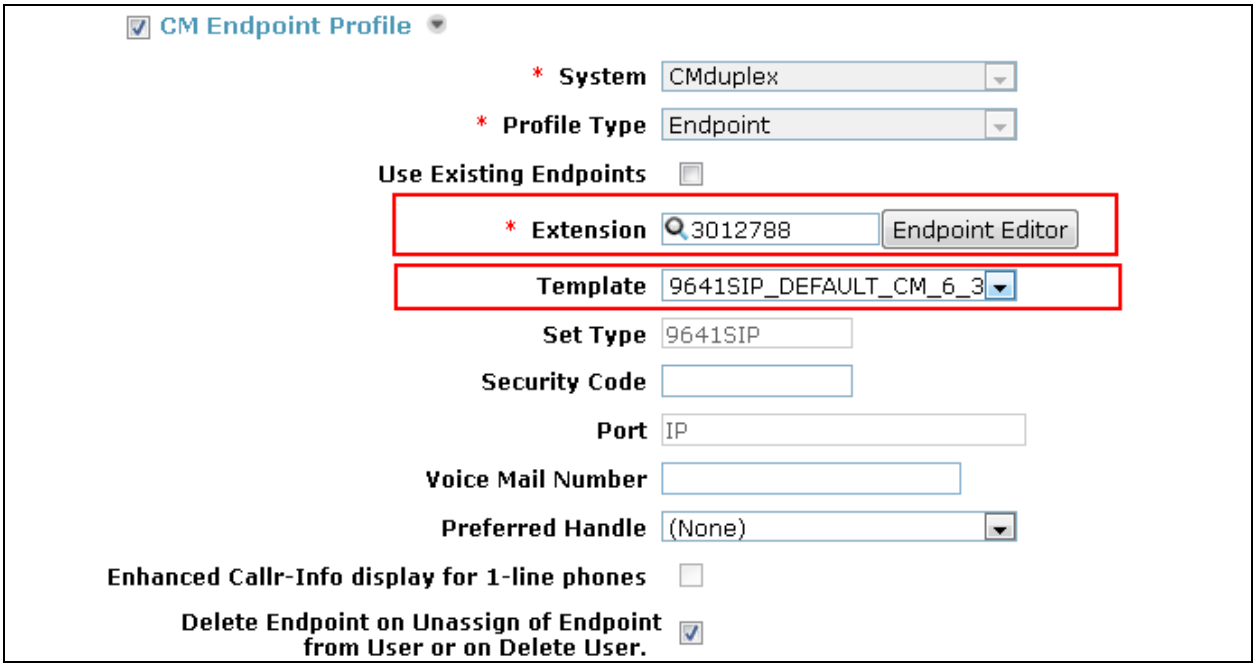


©2014 Avaya Inc. All Rights Reserved

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.

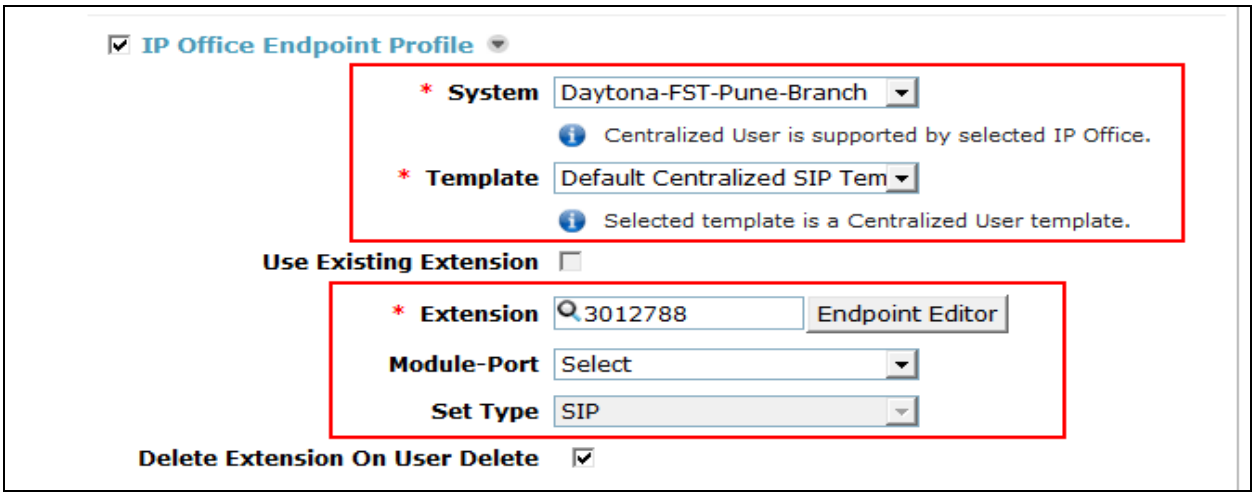


©2014 Avaya Inc. All Rights Reserved

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).



©2014 Avaya Inc. All Rights Reserved

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

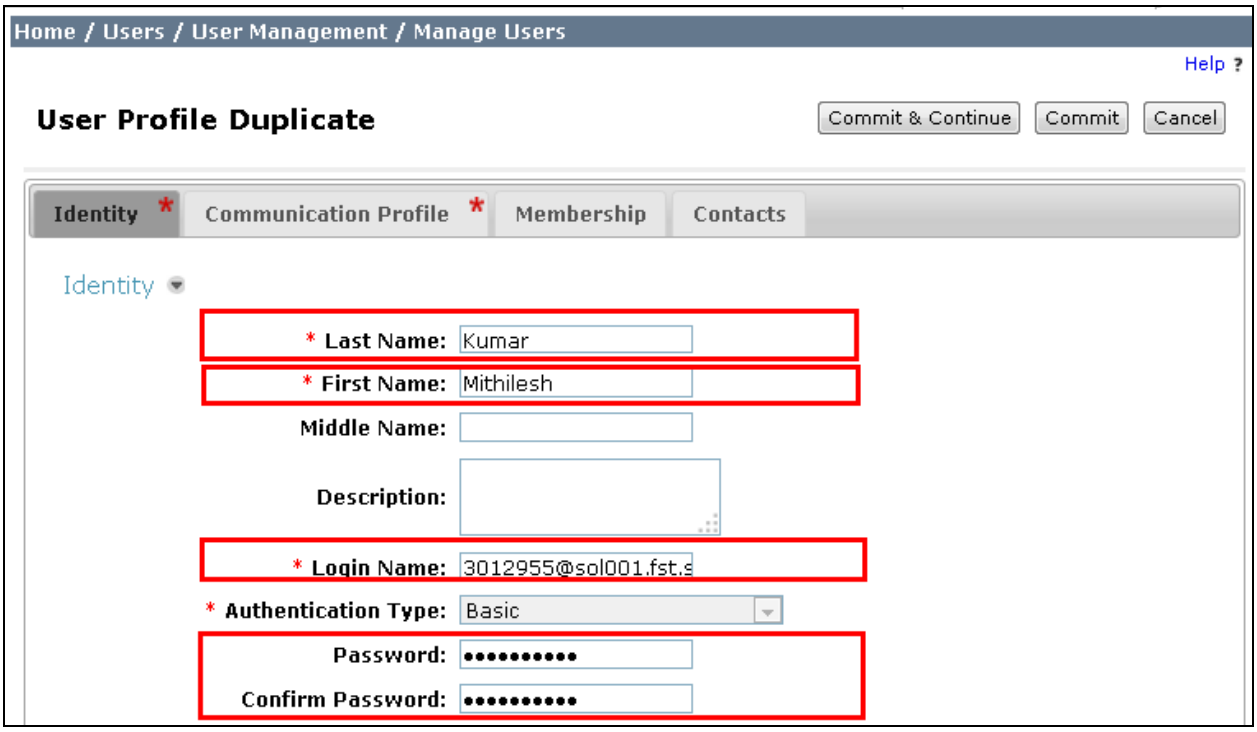
Creating Avaya IP Office H.323 endpoints requires administration of an Avaya IP Office SIP Extension and User for each endpoint via System Manager.

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).

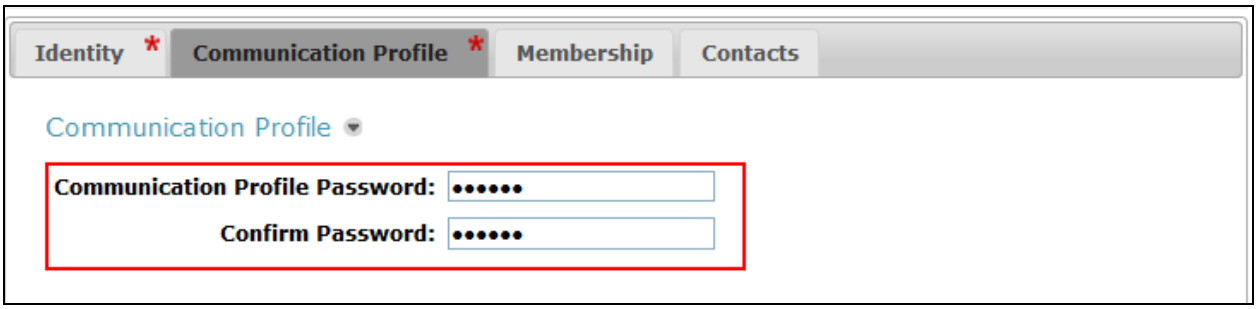
Enter the following information:

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



©2014 Avaya Inc. All Rights Reserved

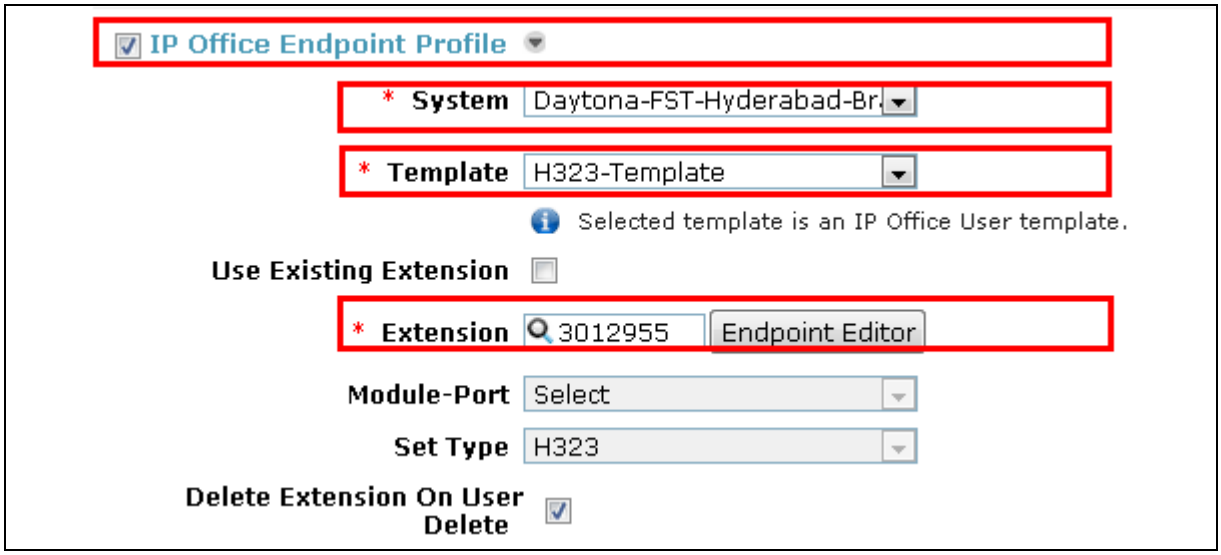
Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint.



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).



©2014 Avaya Inc. All Rights Reserved

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:

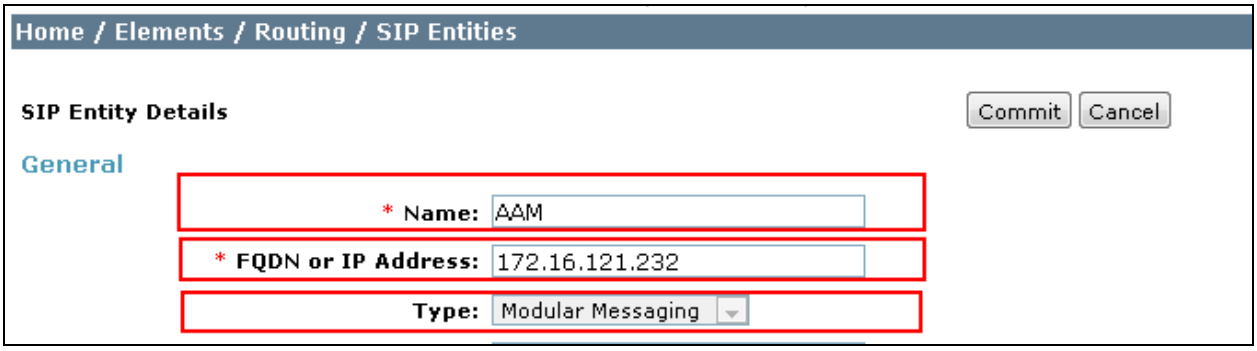
- Configure Entity
- Configure Entity Link
- Configure Routing Policy
- Configure Dial Pattern
- Configure Messaging profile for Users

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**.



9.2. Configure Entity Links

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

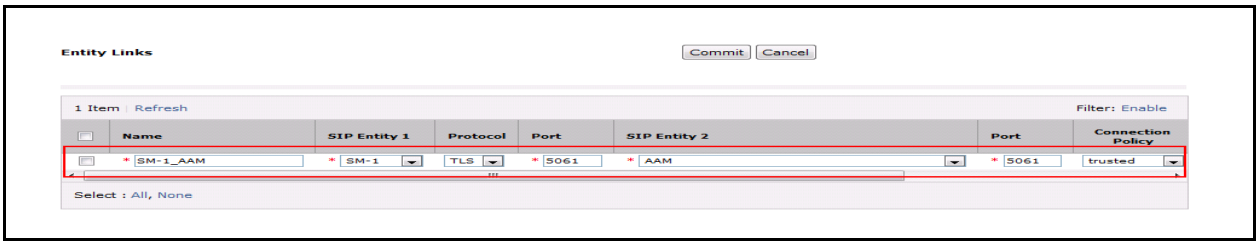
To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **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**

©2014 Avaya Inc. All Rights Reserved

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

Click **Commit**.



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:

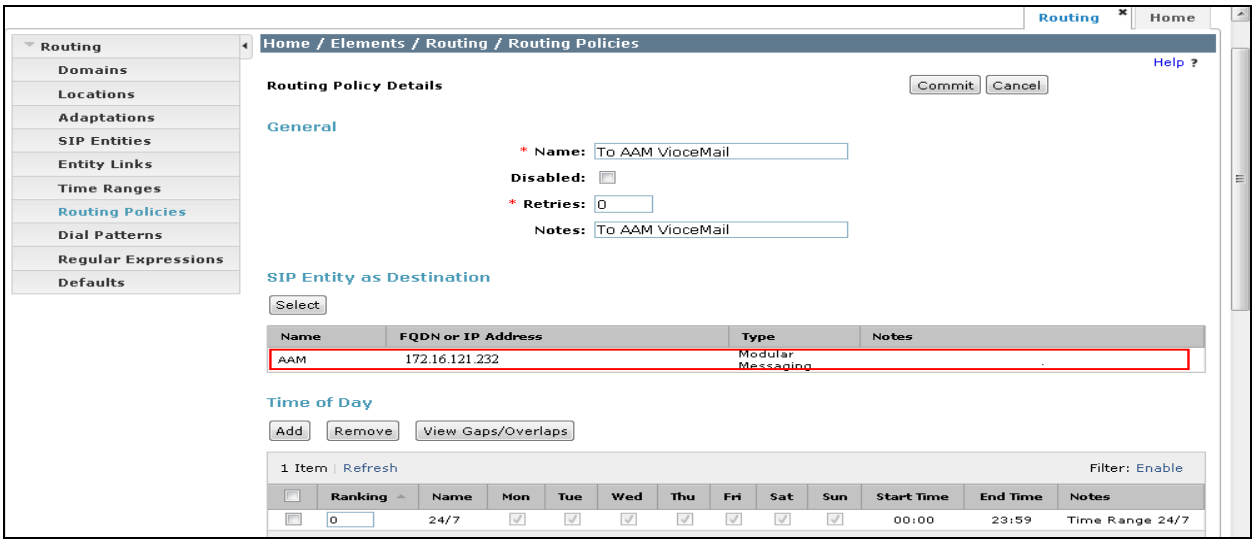
Name: Enter a descriptive name
Notes: Optional text.

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.



©2014 Avaya Inc. All Rights Reserved

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**

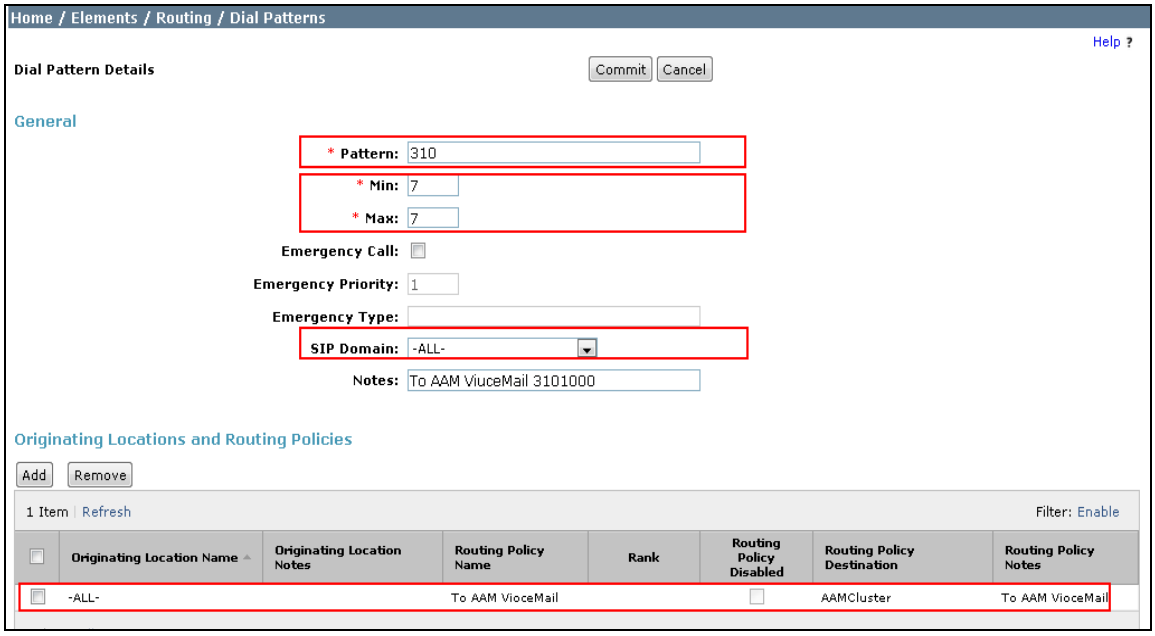
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

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.



©2014 Avaya Inc. All Rights Reserved

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.

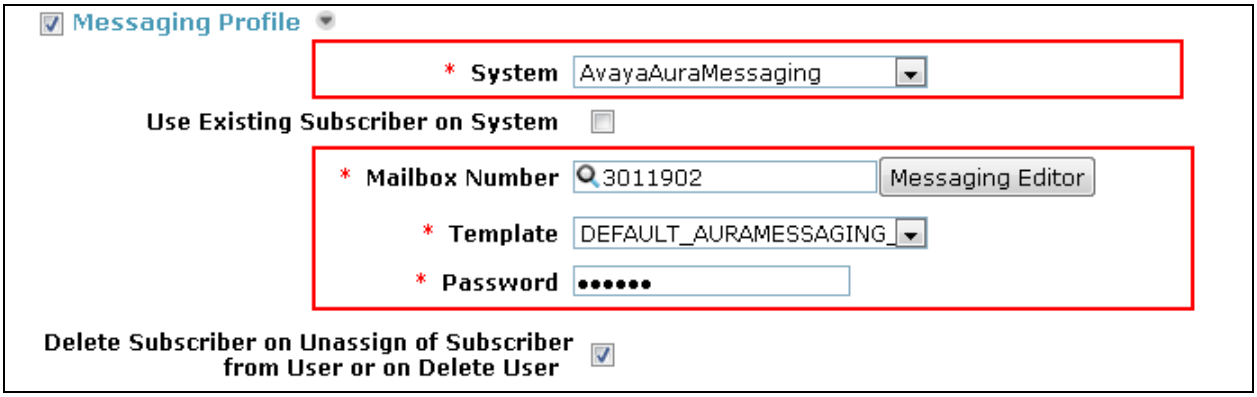
To add a Messaging Profile to an existing extension, log in to System Manager webpage with administrator credentials as described in **Section 7**.

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.



©2014 Avaya Inc. All Rights Reserved

10. Configure Avaya Aura® Conferencing

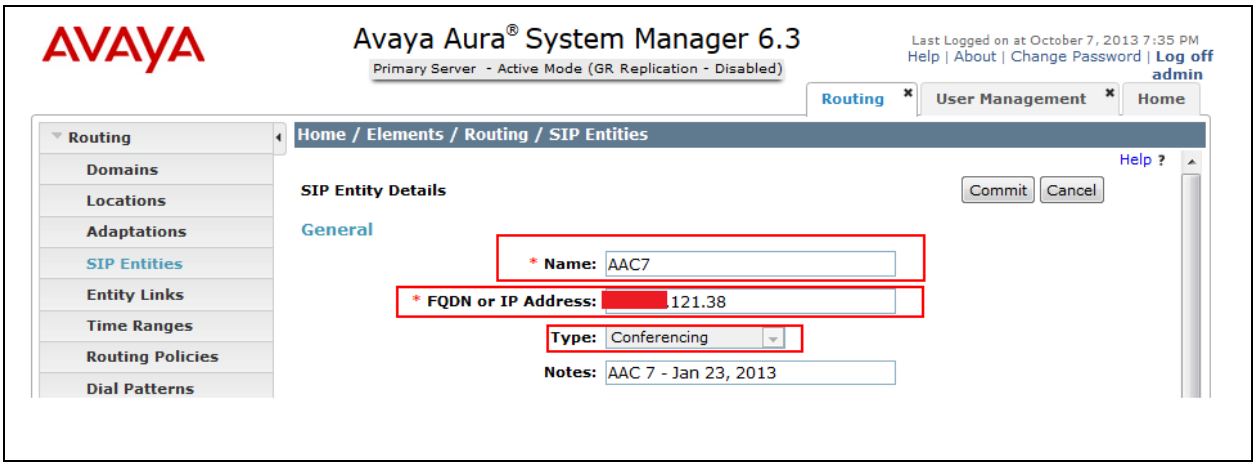
This section provides the procedures for configuring Avaya Aura® Conferencing as provisioned in the sample configuration. Assumption is that Avaya Aura® Conferencing is already installed, configured and integrated with Avaya Aura® System Manager.

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.



10.2. Configure Entity Links

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

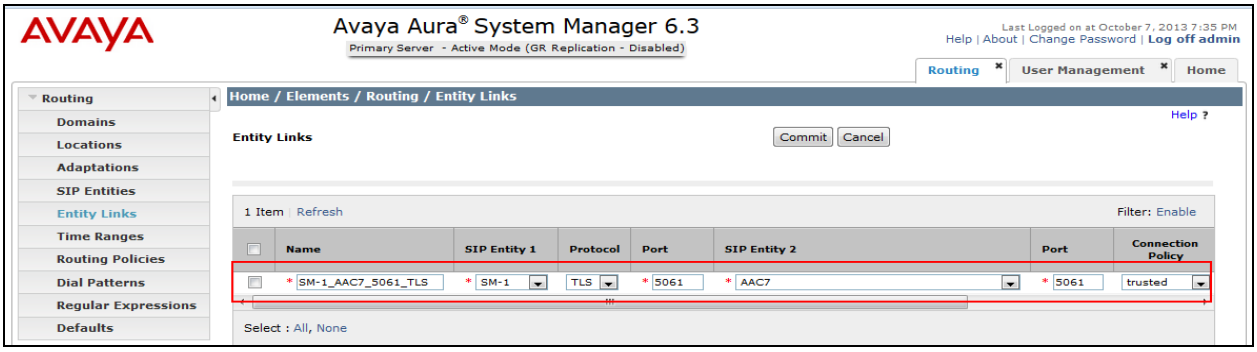
To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **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

©2014 Avaya Inc. All Rights Reserved

- **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)

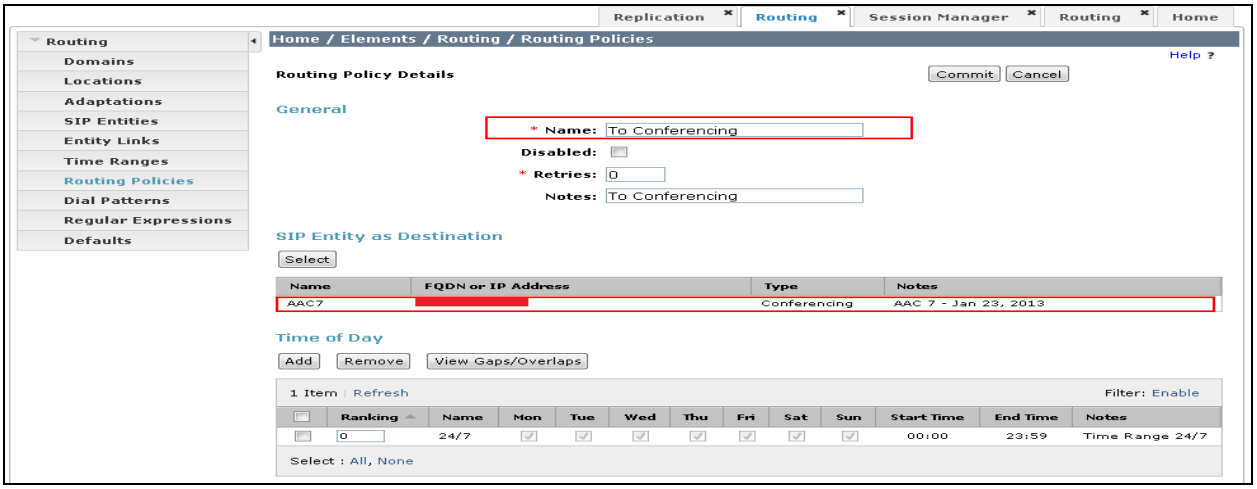
Under **SIP Entity as Destination**:

- 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.



©2014 Avaya Inc. All Rights Reserved

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**.

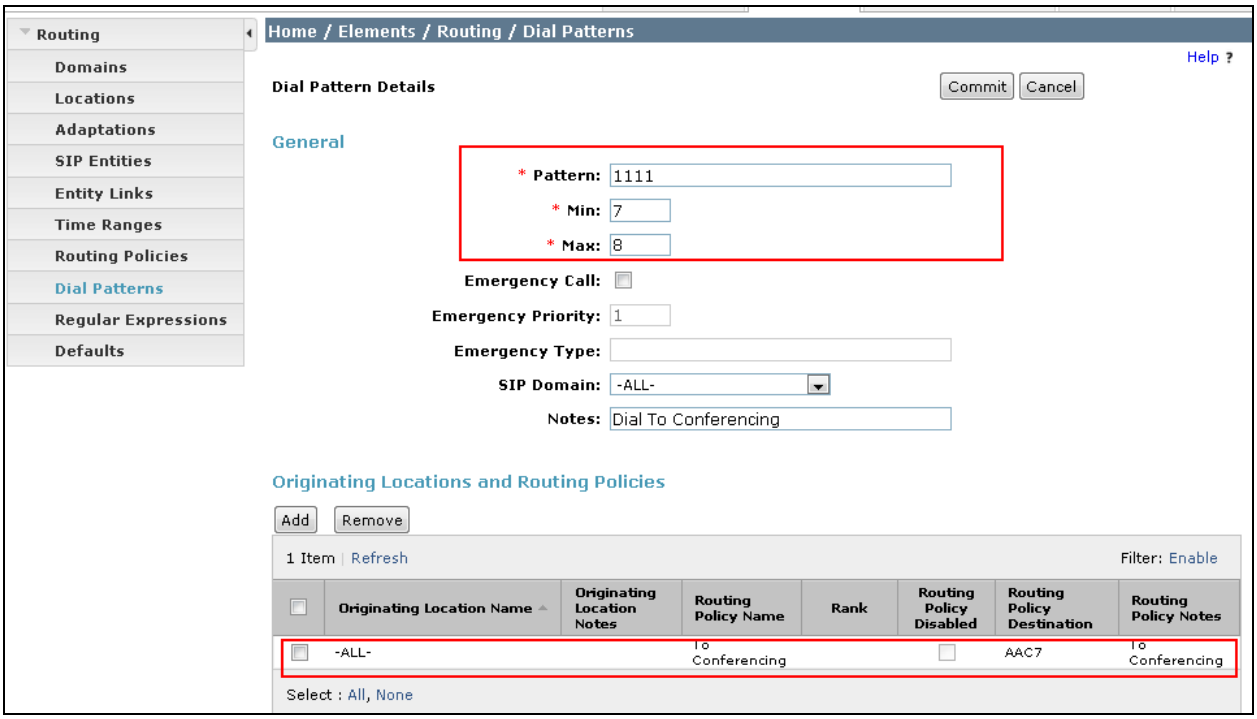
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown). Fill in the following, as shown in the screens below:

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.



©2014 Avaya Inc. All Rights Reserved

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

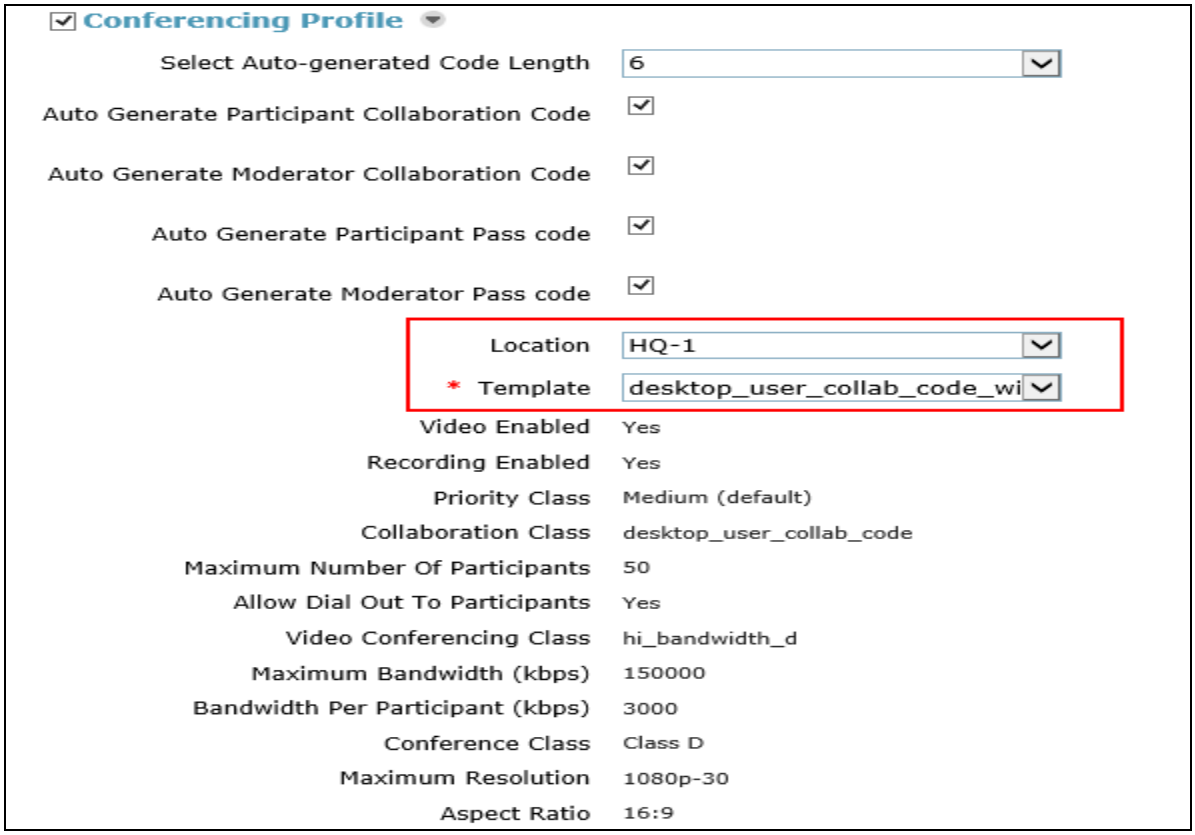
To add Conferencing profile to an existing extension log in to System Manager webpage with administrator credentials as described in **Section 7**.

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.



©2014 Avaya Inc. All Rights Reserved

11. Verification Steps

11.1. Verify Avaya Aura® Session Manager Configuration

Step 1: Verify Session Manager is operational.

Go to **Elements → Session Manager → Dashboard** to verify the overall system status for both Session Manager servers.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass** ✔
- **Security Module** Up
- **Service State** Accept New Service

4 Items | Refresh | Show ALL Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
	SM-1	Core	✔	0/0/0	Up	Accept New Service	12/21	0	10/10	✔	6.3.2.0.632023
	SM-2	Core	✔	0/0/0	Up	Accept New Service	10/15	0	9/9	✔	6.3.2.0.84005

11.2. Verify SIP Entity Link Status

Go to **Elements → Session Manager → System Status → SIP Entity Monitoring** to view more detailed status information one of the SIP Entity Links.

Select the SIP Entity for Avaya Aura® Communication Manager from the **All Monitored SIP Entities (**not shown) table to open the **SIP Entity Entity Link Connection Status** page. Verify the **Conn. Status** for both links is **UP** as shown below.

All Entity Links to SIP Entity: CM Duplex Main

Summary View

Status Details for the selected Session Manager:

2 Items | Refresh Filter: Disable, Apply, Clear

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM-1	[redacted]	5061	TLS	FALSE	UP	200 OK	UP
SM-2	[redacted]	5061	TLS	FALSE	UP	200 OK	UP

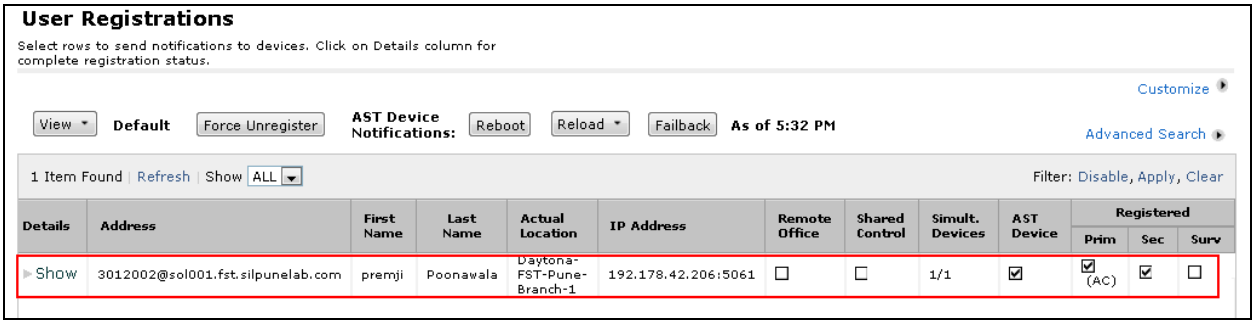
Repeat the steps to verify the Entity Link status for other SIP Entities like IP Office, Messaging, and Conferencing.

©2014 Avaya Inc. All Rights Reserved

11.3. Verify Registrations of SIP Endpoints

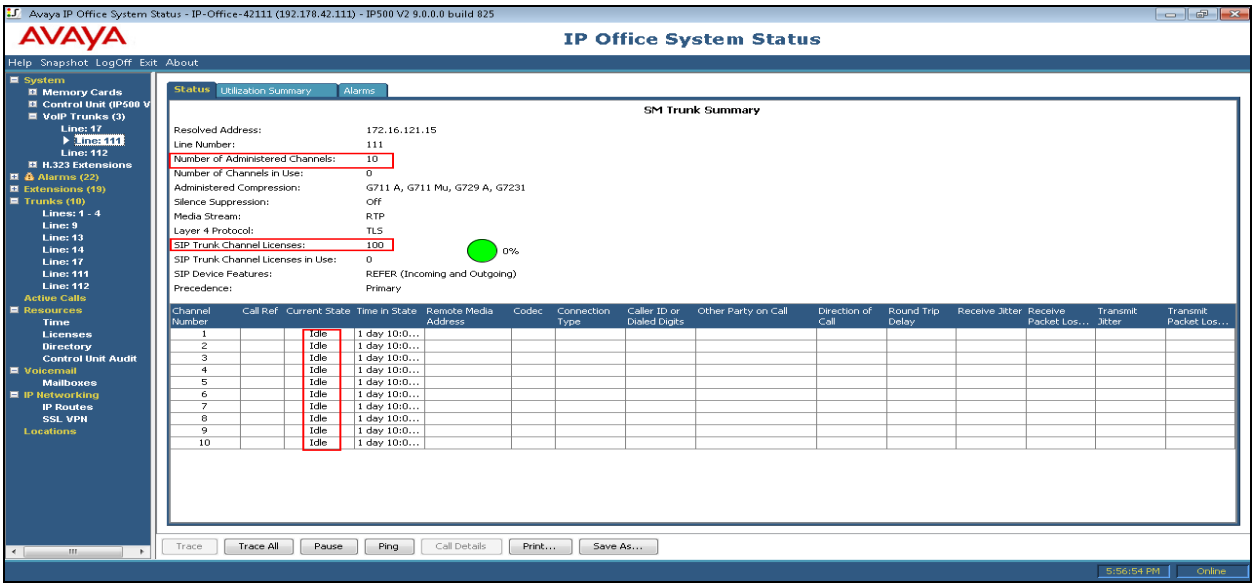
Go to **Elements → Session Manager →System Status → User Registrations** to verify the SIP endpoints have successfully registered with at least one Session Manager.

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



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**.

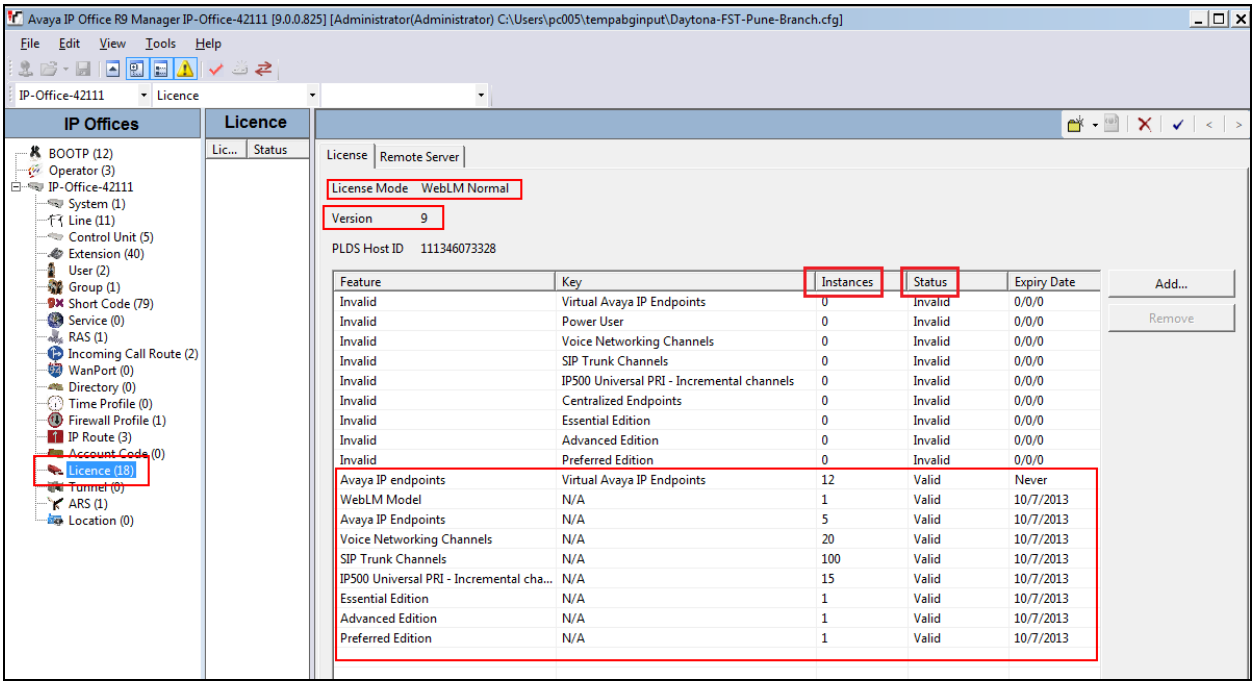


©2014 Avaya Inc. All Rights Reserved

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.

©2014 Avaya Inc. All Rights Reserved

- 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.

©2014 Avaya Inc. All Rights Reserved

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:

©2014 Avaya Inc. All Rights Reserved

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

©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 interoplabnotes@list.avaya.com.