Avaya Solution & Interoperability Test Lab

Application Notes for Convera Integra Suite with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

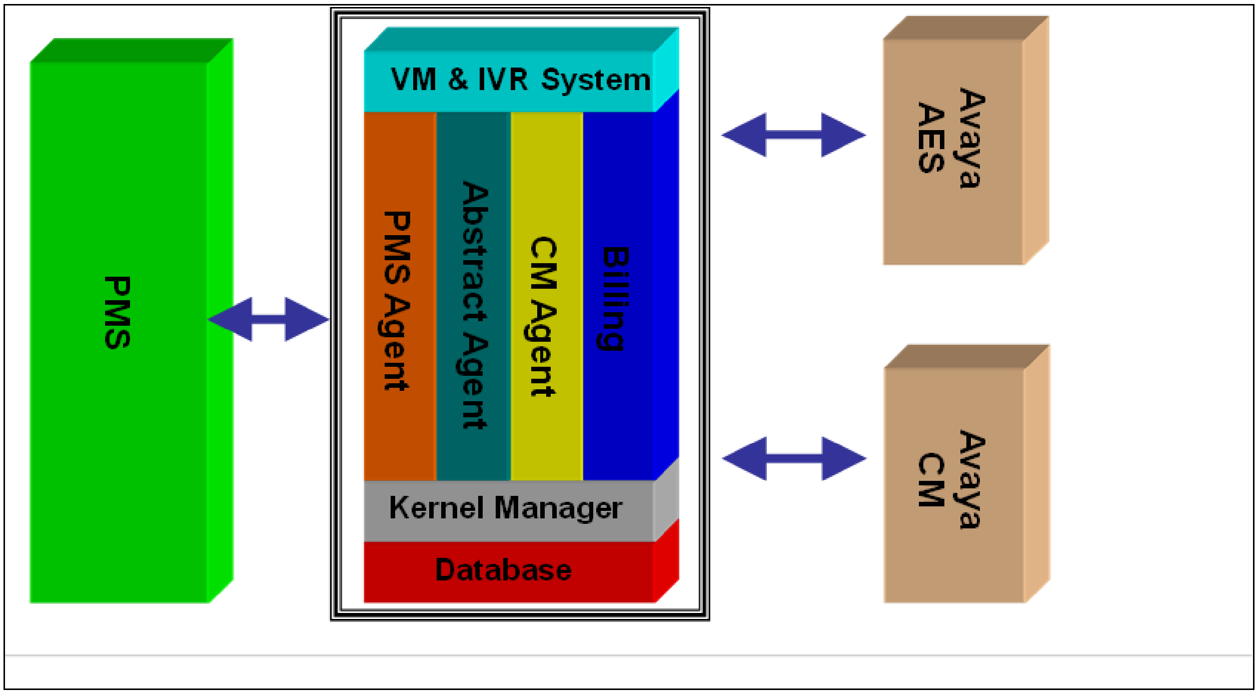
These Application Notes describe the procedures for configuring the Convera Integra Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Convera Integra Suite interface between Avaya Aura® Communication Manager and a hotel's 3rd party Property Management Systems (PMS). This product family is based on a modular approach, allowing hotels to add functionality over time to support environmental controls, video on demand and other services.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Integra Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Integra Suite interface between Avaya Aura® Communication Manager and a hotel's 3rd party Property Management System (PMS). This product family is based on a modular approach, allowing hotels to add functionality to support environmental controls, video on demand and other services.

In addition to billing and posting that manages the costs of telephony and service usage, Integra Suite also supports standard Hospitality feature requests to/from a PMS (guest room check-in/check-out/moves, Do Not Disturb (DND), Automatic Wake-Up (AWU), Message Waiting Lamp (MWL) control and Housekeeping/Room Status changes and Minibar usage. The account posting functionality is facilitated by a Call Detail Recording (CDR) interface to Avaya Aura® Communication Manager, while the Hospitality features are enabled by a PMS data link to Avaya Aura® Communication Manager and System Management Services to Avaya Aura® Application Enablement Services Server. Voice Mail services including Interactive Voice Response (IVR) system for the purpose of Minibar posting and Housekeeping/Room Status is also provided as part of the Suite. Access to these services is via SIP Trunk link direct to Avaya Aura® Communication Manager. The diagram below shows an overall view of the solution.



When notified of a guest room check-in, Integra Suite removes outbound call restrictions on the guest room extension and changes that extension's Hospitality Room Status to "occupied." Conversely, when notified of a guest room check-out, Integra Suite restricts outbound calls on the guest room extension and sets its Hospitality Room Status to "vacant."

2. General Test Approach and Test Results

Feature functionality testing was performed manually. Inbound calls were made to the Avaya IP Telephones (i.e. the guest telephones) over BRI trunks, as well as from other local extensions (analog, digital, and IP Telephone). A simulated PMS application was used to launch changes to telephone message waiting lamps and phone privileges during room check in / check out / move requests, receive room status updates, and activate/deactivate DND.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

Interoperability compliance testing focused on the ability of Integra Suite to work with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Integra Suite features and capabilities that were verified included the following: receipt and processing of Call Detail Records, check-in/check-out/room change for guest extensions, posting of Housekeeping/Room Status changes initiated at guest telephones and forwarding to a simulated Property Management System, MWL activation for incoming voicemail, and DND activation/deactivation.

2.2. Test Results

All executed test cases were completed successfully. However, where check-in, check-out or DND features are executed, the phones will be busied and released to clear the call history.

2.3. Support

For technical support on Integra Suite, contact Convera Systems FZ-LLC at the following:

Email: support@converasys.com
Phone: +90-21-22867576

3. Reference Configuration

The configuration used in performing compliance testing of Integra Suite is shown in **Figure 1**. It shows a network consisting primarily of a pair of Avaya S8800 Server running Avaya Aura® Communication Manager in duplex mode with an Avaya G650 Media Gateway, Avaya Aura® System Manager and Avaya Aura® Session Manager, a Convera server with Integra Suite installed and a pair of phones for each guest room, which are either analog or digital with an Avaya IP Telephone. The Voice Mail and Billing server can be installed on another server but in this compliance testing, it is the same server. Additional utility phones are setup to function as Operator and Front Desk. The CDR and PMS data links from Integra Suite are carried over the IP network and terminated in Avaya Aura® Communication Manager as IP services. Avaya Aura® Enablement Services (AES) Server provides the System Management Services (SMS) to Integra Suite allowing the application to use Web service access to manage objects on Communication Manager. Voice Mail/IVR services are provided on the same Convera server in this compliance testing. The SIP trunk link from Integra Suite is connected via the Session Manager which acts as proxy to Communication Manager.

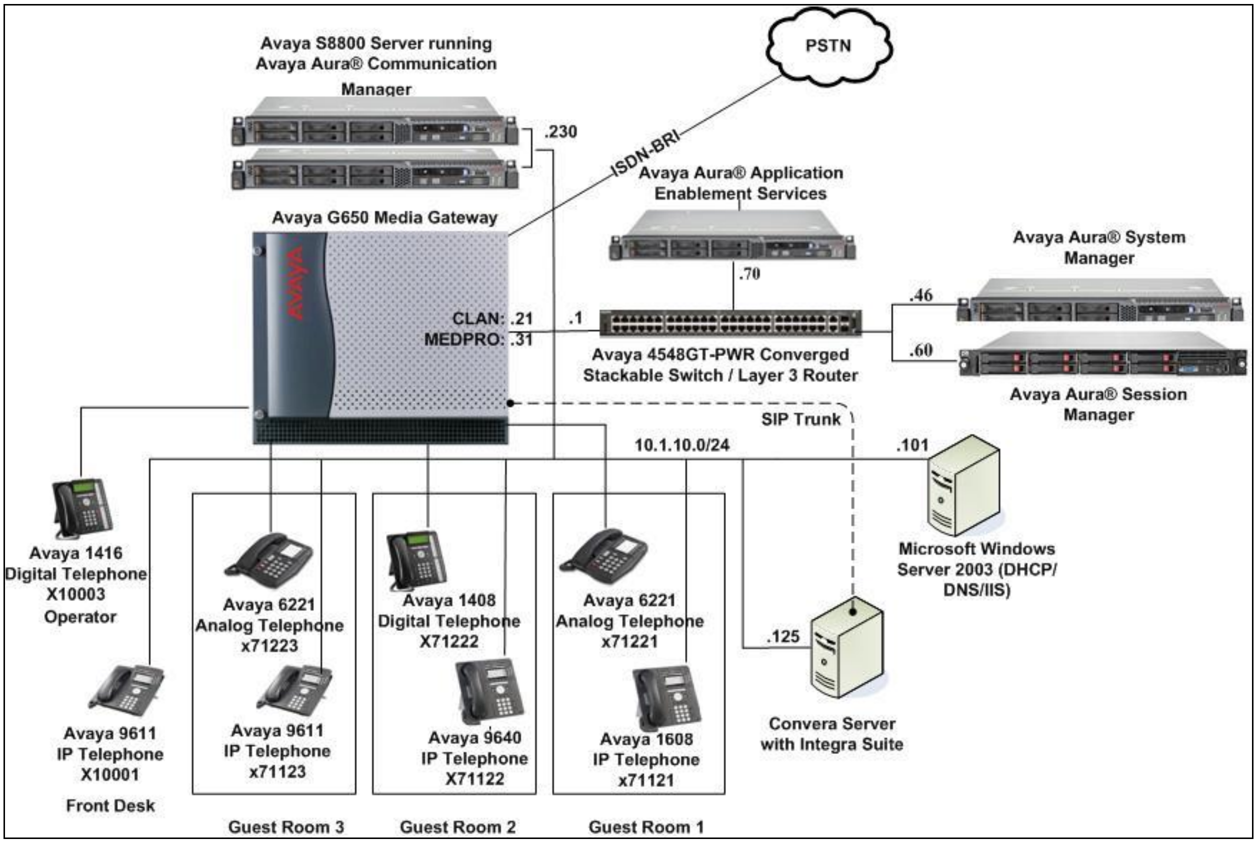


Figure 1: Sample Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release Version
Avaya Aura® Communication Manager	R6.2 SP 2.01
Avaya G650 Media Gateway • TN2312BP IP Server Interface • TN799DP C-LAN Interface • TN2602AP IP Media Processor	- HW07, FW054 HW01, FW040 HW02, FW059
Avaya Aura® Application Enablement Services Server	R6.2.0.18.0
Avaya Aura® System Manager	R6.2 SP3
Avaya Aura® Session Manager	R6.2 SP3
Avaya 4548GT-PWR Converged Stackable Switch	V6.2.4.010
Avaya 9621 IP Telephone	6.2 SP2
Avaya 9611 IP Telephone	6.0 SP5
Avaya 9640 IP Telephone	3.1 SP3
Avaya 1608 IP Telephone	1.32
Avaya 6221 Analog Telephone	-
Avaya 1416 Digital Telephone	-
Avaya 1408 Digital Telephone	-
Integra Suite Server on Windows Server 2008 R2 SP1	7.5

5. Configure Avaya Aura® Communication Manager

This section details the steps required to configure Avaya Communication Manager to interoperate with Integra Suite. These Application Notes assume the Avaya Media Gateway (including circuit packs) has already been administered. Please refer to [1]-[2] for additional details.

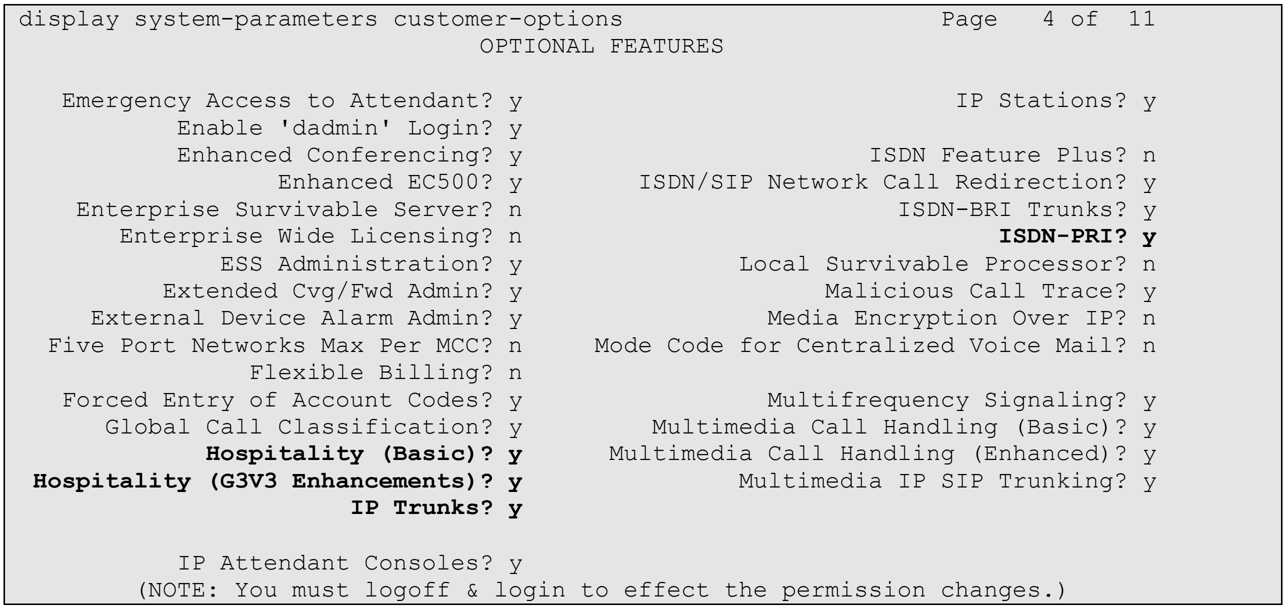
The commands listed in this section were issued at the System Access Terminal (SAT) screen except for the creation of login for SMS using Communication Manager Web interface. For all steps where data are modified, submit the completed administration form for the changes to take effect.

5.1. License

Ensure that license is provided for the SIP Trunking to Voice Mail/IVR other than the hospitality features are turned on as below:

- **Maximum Administered SIP Trunks** : Ensure sufficient number of SIP Trunks allocated
- **IP Trunks?** Must be enabled for IP Trunks
- **ISDN-PRI?** Must be enabled for IP Trunks
- **Hospitality (Basic)?** Enter **y**
- **Hospitality (G3V3 Enhancements)?** Enter **y**

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 90
           Maximum Concurrently Registered IP Stations: 18000 8
             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: 41000 1
                   Maximum Video Capable IP Softphones: 18000 6
                       Maximum Administered SIP Trunks: 24000 58
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   2
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

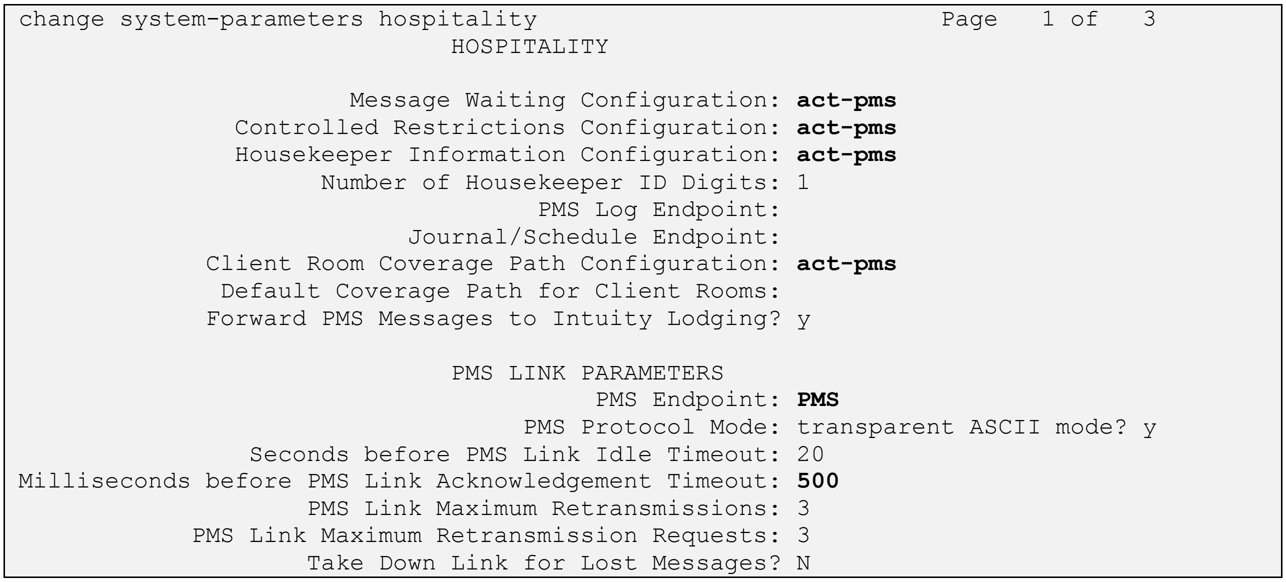


```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Set Hospitality Parameters

Enter **change system-parameters hospitality**. On **Page 1**, set the following values:

- **Message Waiting Configuration:** Enter **act-pms.**
- **Controlled Restrictions Configuration:** Enter **act-pms.**
- **Housekeeper Information Configuration:** Enter **act-pms.**
- **Client Room Coverage Path Configuration:** Enter **act-pms.**
- **Default Coverage Path for Client Rooms:** This is left blank as coverage path is set by PMS.
- **PMS Endpoint:** Enter **PMS.**
- **Milliseconds before PMS Link Acknowledgement Timeout:** Enter **500**
- **Number of Digits from PMS:** Set the digit length of rooms
- **Number of Digits in PMS Coverage Path:** Set the digit length for coverage path



```
change system-parameters hospitality                            Page   1 of   3
                              HOSPITALITY

                       Message Waiting Configuration: act-pms
               Controlled Restrictions Configuration: act-pms
               Housekeeper Information Configuration: act-pms
                     Number of Housekeeper ID Digits: 1
                                    PMS Log Endpoint:
                           Journal/Schedule Endpoint:
             Client Room Coverage Path Configuration: act-pms
              Default Coverage Path for Client Rooms:
             Forward PMS Messages to Intuity Lodging? y

                              PMS LINK PARAMETERS
                                        PMS Endpoint: PMS
                                   PMS Protocol Mode: transparent ASCII mode? y
                Seconds before PMS Link Idle Timeout: 20
Milliseconds before PMS Link Acknowledgement Timeout: 500
                    PMS Link Maximum Retransmissions: 3
            PMS Link Maximum Retransmission Requests: 3
                    Take Down Link for Lost Messages? N
```

```
change system-parameters hospitality                            Page   2 of   3
                              HOSPITALITY

            Dual Wakeups? y    Daily Wakeup? y    VIP Wakeup? y
                                   VIP Wakeups Per 5 Minutes: 5
                            Room Activated Wakeup With Tones? y
                    Time of Scheduled Wakeup Activity Report:
                     Time of Scheduled Wakeup Summary Report:
           Time of Scheduled Emergency Access Summary Report:
                                           Announcement Type: silence


          Length of Time to Remain Connected to Announcement: 30
             Extension to Receive Failed Wakeup LWC Messages:
            Routing Extension on Unavailable Voice Synthesis:
                    Display Room Information in Call Display? y
                          Automatic Selection of DID Numbers? y
                         Custom Selection of VIP DID Numbers? y
                                  Number of Digits from PMS: 5
                                           PMS Sends Prefix? n
                      Number of Digits in PMS Coverage Path: 4
                                     Digit to Insert/Delete:
```

5.3. Define the Integra Suite Server as an IP Node Name

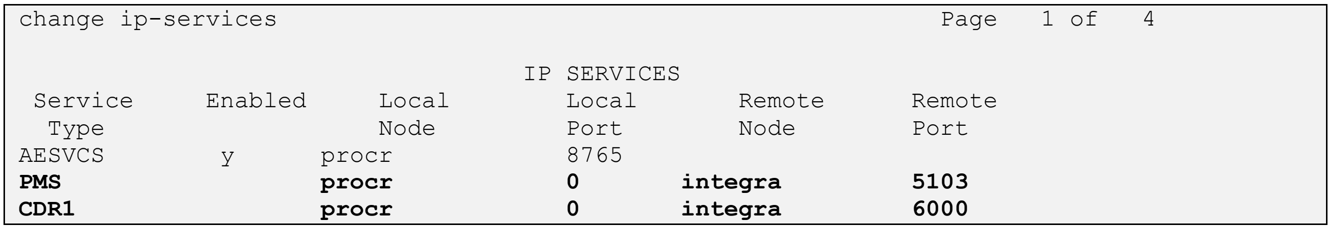
Enter **change node-names ip** and add an entry for the Integra Suite server using an appropriately descriptive value for the **Name** (in this case, **integra**) and the corresponding **IP Address** (in this example, **10.1.10.125**). Add also an entry for the Session Manager using an appropriately descriptive value for the **Name** (in this case, SM1) and the corresponding **IP Address** (in this example, **10.1.10.60**)

```
change node-names ip i                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
integra             10.1.10.125
lsp-g430            10.1.40.10
msgserver           10.1.10.10
n                   10.3.10.253
procr               10.1.10.230
procr6              ::
s8300-siteB         10.1.20.10
s8500-clan1         10.1.10.21
s8500-clan2         10.1.10.22
s8500-medpro1       10.1.10.31
s8500-medpro2       10.1.10.32
s8500-val1          10.1.10.36
site6               10.1.60.10
sm1                 10.1.10.60
 ( 16 of 25   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.4. Define IP-Services in Support of the PMS and CDR Data Links:

Enter **change ip-services** and add entries with a Service Type of **PMS** and **CDR1** (or, if a CDR1 service is already defined, **CDR2**), respectively. In each case, enter the following values in the remaining fields:

- **Local Node**: The IP Node Name of a C-LAN board or PROCR (in this example, **procr** is used for IP service definition).
- **Remote Node**: The IP Node Name of the Integra Suite server, as defined in **Figure 1.**
- **Remote Port**: A valid unused port (in this example, the value needs to tally with the integra setup where **5103** fixed port is used for **PMS**, while **6000** is configured for **CDR1**).



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
PMS                  procr            0       integra         5103
CDR1                 procr            0       integra         6000
```

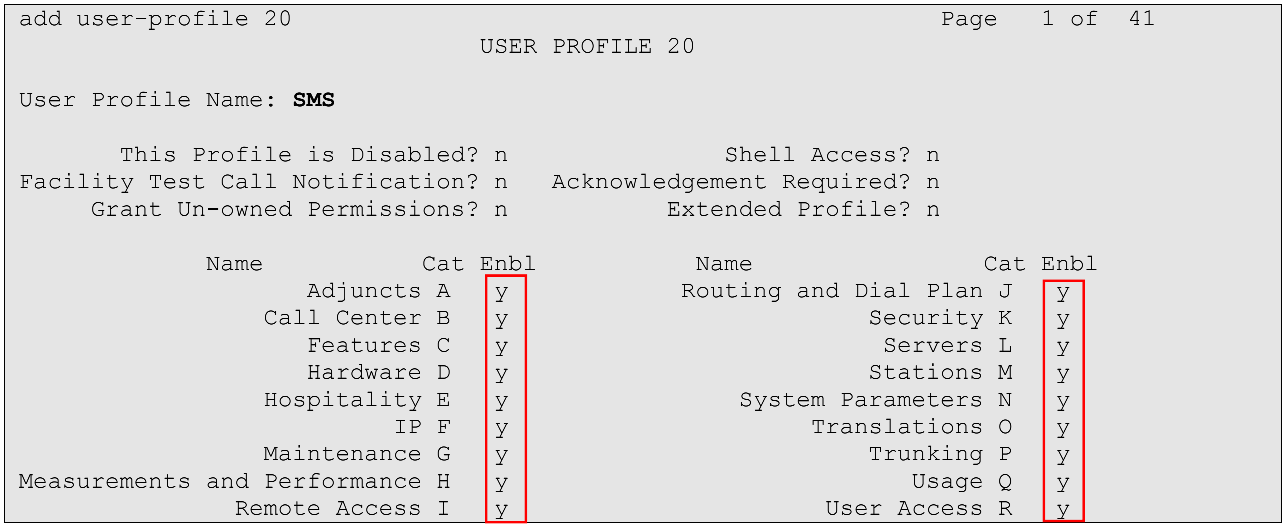
5.5. Administer Login for SMS

This section details the creation of SAT login for SMS. The steps include:

- Add user-profile for SMS
- Configure Login Group
- Configure Login

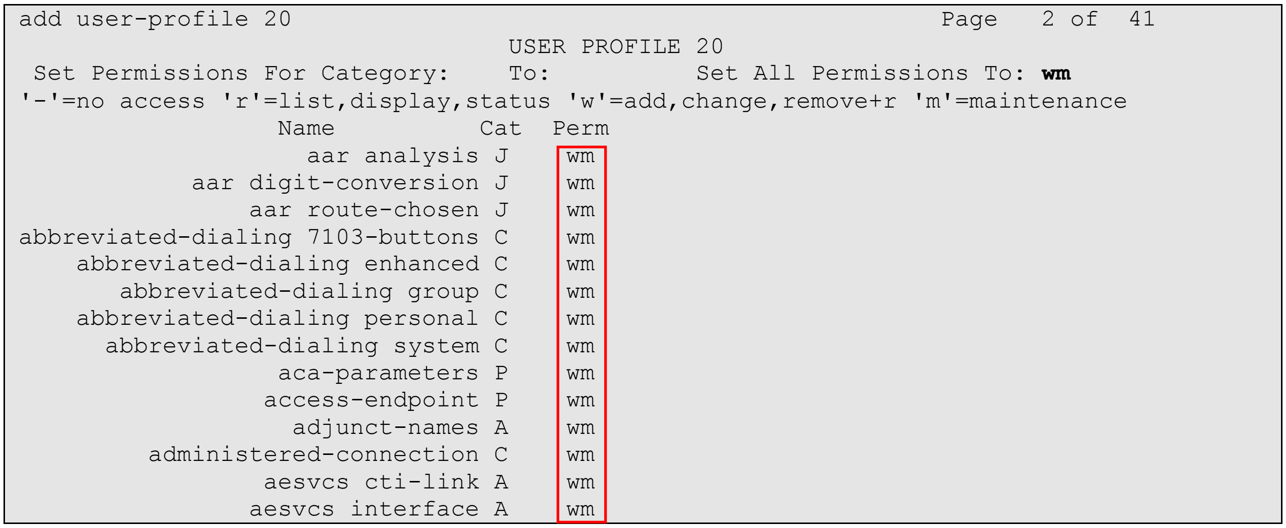
5.5.1. Add User-Profile for SMS

Enter the **add user-profile *n*** command, where ***n*** is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**. In this test configuration, the user profile 20 is created.



```
add user-profile 20                                             Page   1 of   41
                                USER PROFILE 20

User Profile Name: SMS

       This Profile is Disabled? n               Shell Access? n
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl           Name                Cat Enbl
                    Adjuncts A   y            Routing and Dial Plan J   y
                 Call Center B   y                         Security K   y
                    Features C   y                          Servers L   y
                    Hardware D   y                         Stations M   y
                 Hospitality E   y                System Parameters N   y
                          IP F   y                     Translations O   y
                 Maintenance G   y                         Trunking P   y
Measurements and Performance H   y                            Usage Q   y
               Remote Access I   y                      User Access R   y
```

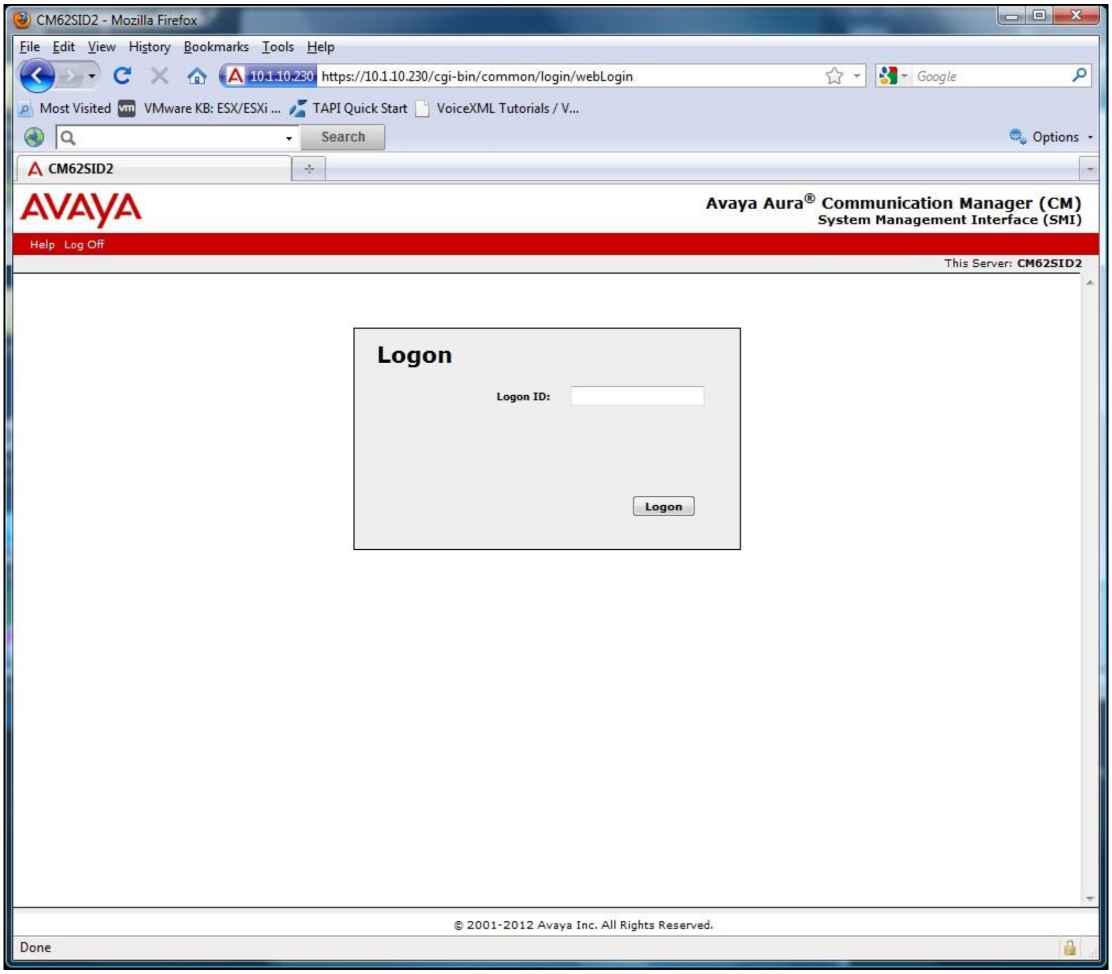
Enter **wm** in **Set All Permissions To** field for setting write and maintenance permission to all categories.



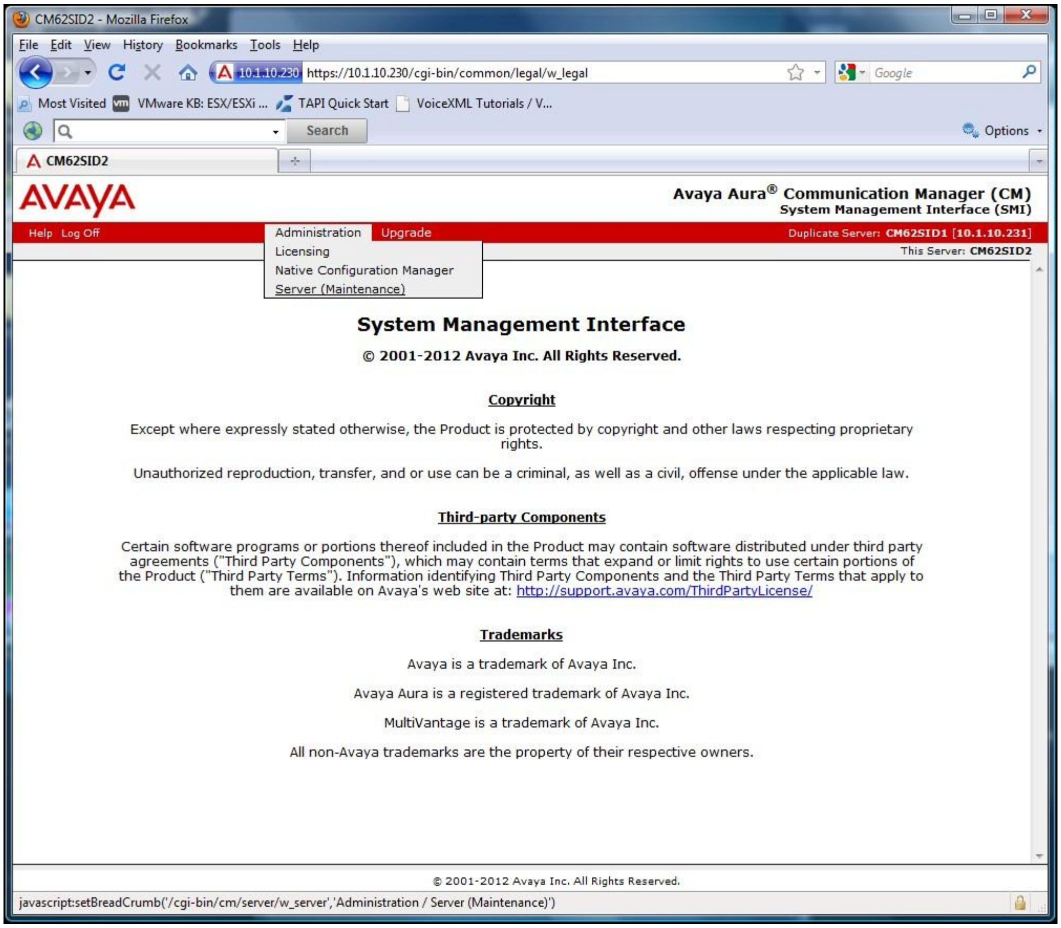
```
add user-profile 20                                             Page   2 of   41
                                  USER PROFILE 20
 Set Permissions For Category:    To:          Set All Permissions To: wm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                    aar analysis J    wm
            aar digit-conversion J    wm
                aar route-chosen J    wm
abbreviated-dialing 7103-buttons C    wm
    abbreviated-dialing enhanced C    wm
       abbreviated-dialing group C    wm
    abbreviated-dialing personal C    wm
      abbreviated-dialing system C    wm
                  aca-parameters P    wm
                 access-endpoint P    wm
                   adjunct-names A    wm
         administered-connection C    wm
                 aesvcs cti-link A    wm
                aesvcs interface A    wm
```

5.5.2. Configure Login Group

Using a web browser, enter https://<IP address of Communication Manager> to connect to the Avaya Server being configured and log in using appropriate credentials.


CM62SID2 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.1.10.230/cgi-bin/common/login/webLogin
Most Visited
VMware KB: ESX/ESXi ...
TAPI Quick Start
VoiceXML Tutorials / V...
Search
Options
CM62SID2
AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: CM62SID2
Logon
Logon ID:
Logon
© 2001-2012 Avaya Inc. All Rights Reserved.
Done

Click **Administration → Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.


CM62SID2 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.1.10.230/cgi-bin/common/legal/w_legal
Most Visited
VMware KB: ESX/ESXi ...
TAPI Quick Start
VoiceXML Tutorials / V...
Search
Options
CM62SID2
AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Administration
Upgrade
Licensing
Native Configuration Manager
Server (Maintenance)
Duplicate Server: CM62SID1 [10.1.10.231]
This Server: CM62SID2

System Management Interface

© 2001-2012 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

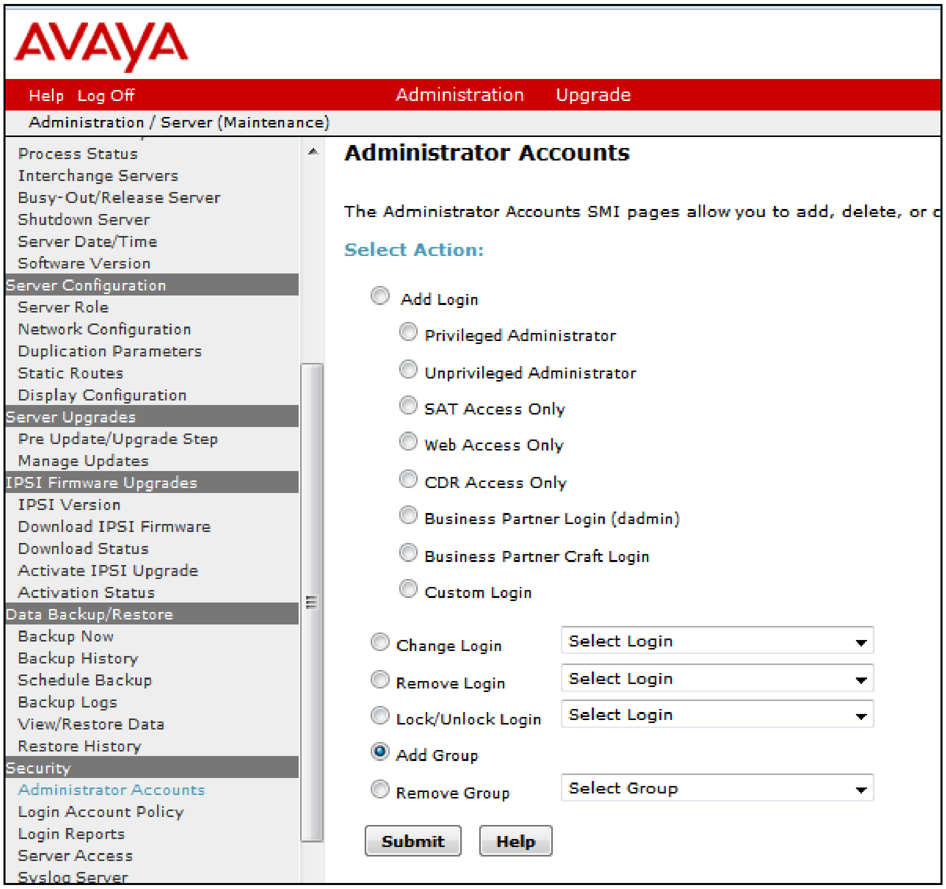
MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

© 2001-2012 Avaya Inc. All Rights Reserved.

javascript:setBreadCrumb('/cgi-bin/cm/server/w_server','Administration / Server (Maintenance)')

From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Group** and click **Submit**.



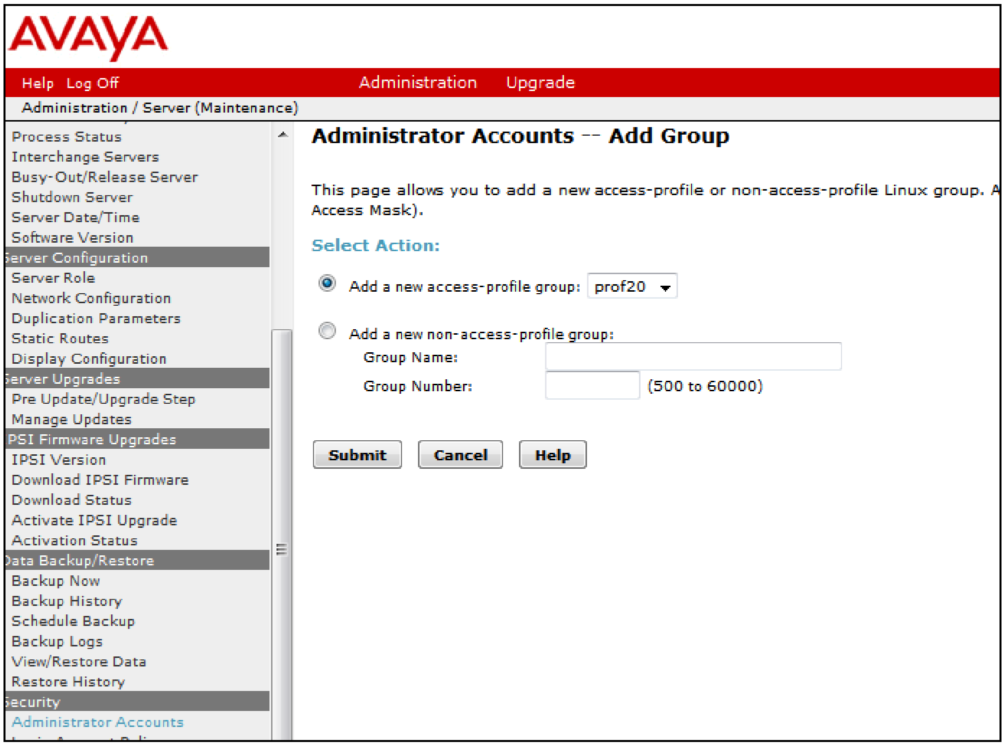
Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or c

Select Action:

○ Add Login
○ Privileged Administrator
○ Unprivileged Administrator
○ SAT Access Only
○ Web Access Only
○ CDR Access Only
○ Business Partner Login (dadmin)
○ Business Partner Craft Login
○ Custom Login
○ Change Login Select Login
○ Remove Login Select Login
○ Lock/Unlock Login Select Login
● Add Group
○ Remove Group Select Group

Select **Add a new access-profile group** and select **prof20** from the drop-down box to correspond to the user-profile created in **Section 5.5.1**. Click **Submit**. This completes the creation of the login group.



Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. A
Access Mask).

Select Action:

● Add a new access-profile group: prof20

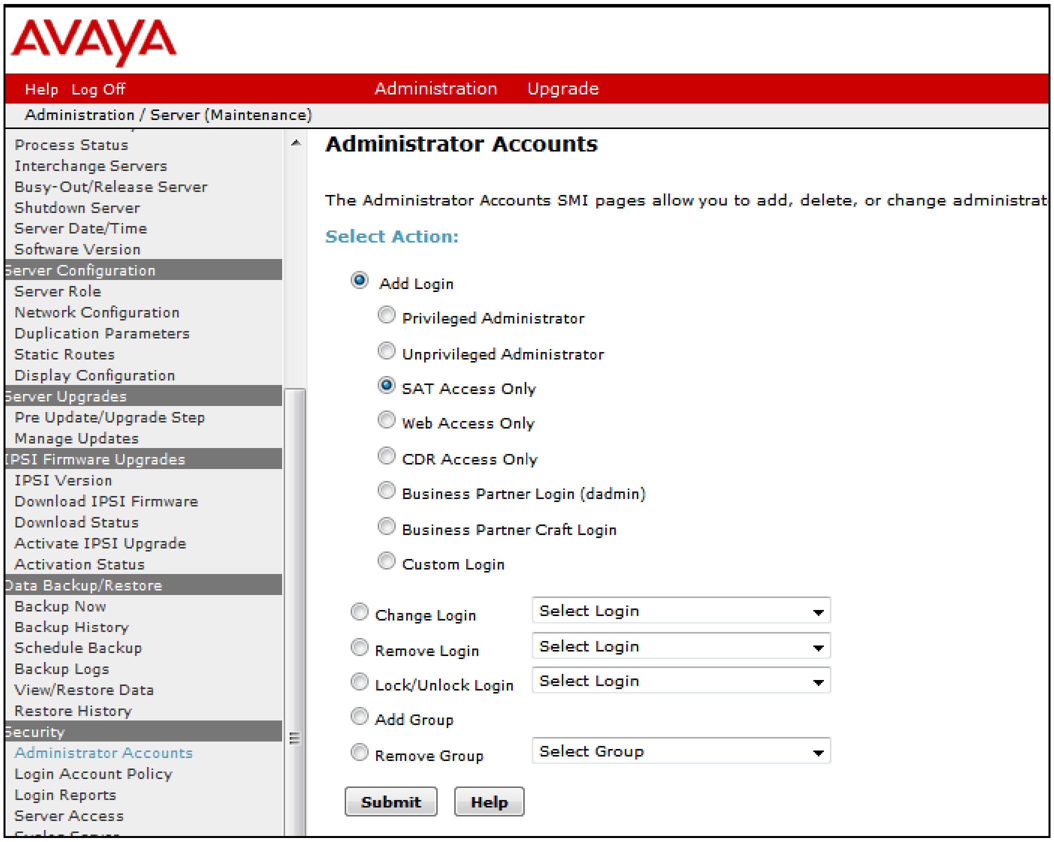
○ Add a new non-access-profile group:

Group Name:

Group Number: (500 to 60000)

5.5.3. Configure Login

From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrat

Select Action:

● Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ● SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login: Select Login

○ Remove Login: Select Login

○ Lock/Unlock Login: Select Login

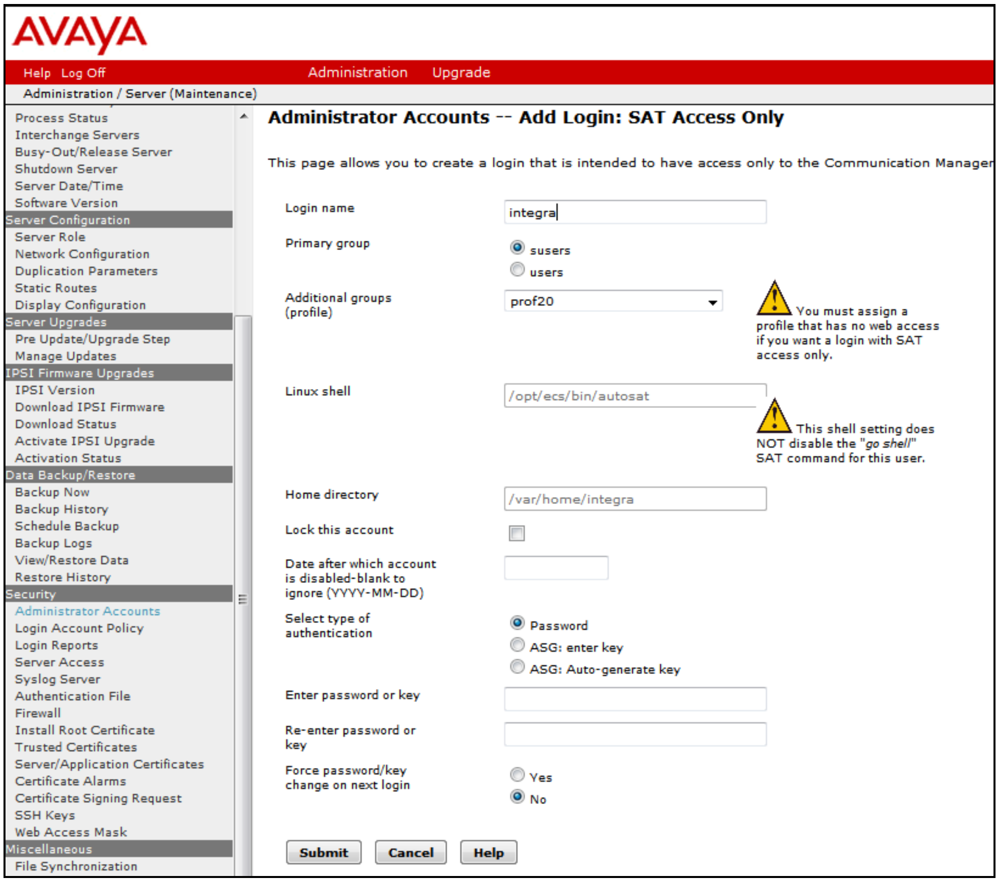
○ Add Group

○ Remove Group: Select Group

For the field **Login name**, enter the login. In this configuration, the login **integra** is created. Configure the other parameters for the login as follows:

- Primary group: **susers**
- Additional groups (profile): **prof20** [Select the login group created in **Section 5.5.2**]
- Select type of authentication: **Password** [Uses a password for authentication.]
- Enter password or key / Re-enter password or key [Define the password.]

Click **Submit** to continue. This completes the configuration of the login.



Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manager

Login name: integra

Primary group: ● susers ○ users

Additional groups (profile): prof20

You must assign a profile that has no web access if you want a login with SAT access only.

Linux shell: /opt/ecs/bin/autosat

This shell setting does NOT disable the "*go shell*" SAT command for this user.

Home directory: /var/home/integra

Lock this account: □

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Select type of authentication: ● Password ○ ASG: enter key ○ ASG: Auto-generate key

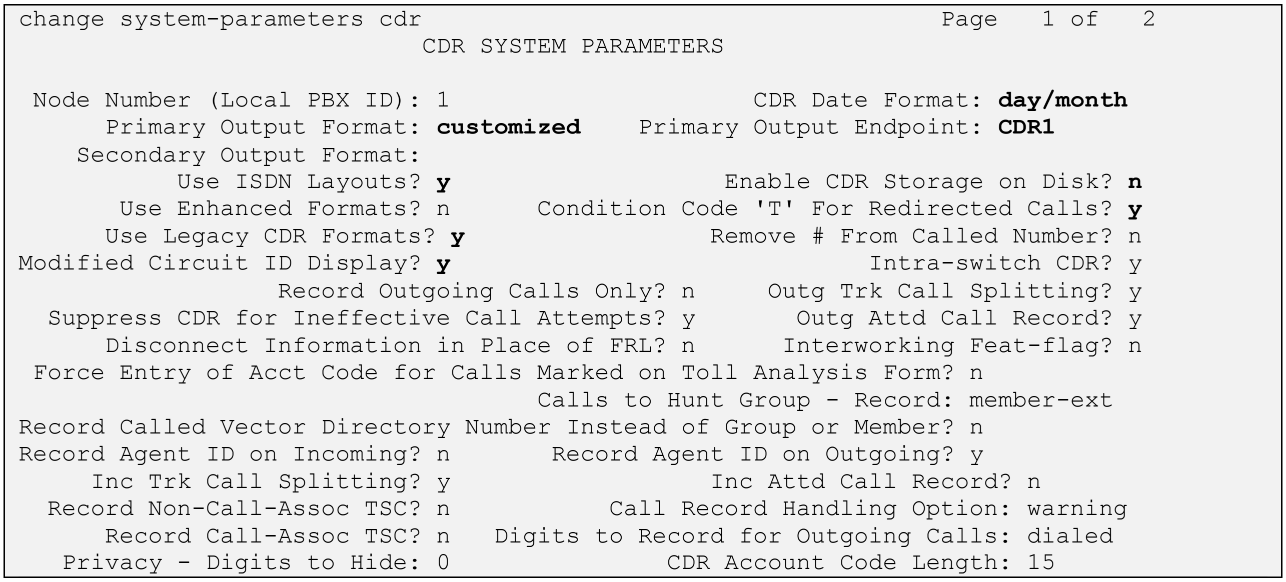
Enter password or key:

Re-enter password or key:

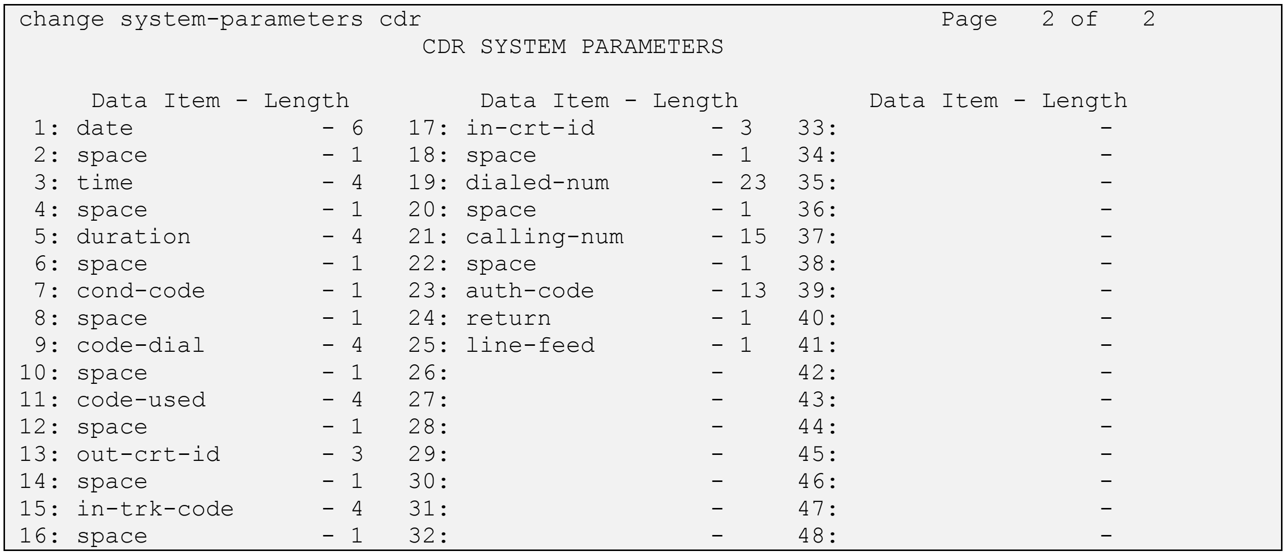
Force password/key change on next login: ○ Yes ● No

5.6. Administer CDR Output Format

Enter **change system-parameters cdr** and choose one of the standard output formats for the **Primary Output Format** field (in this example, **customized** was entered). This selection will determine the expected call detail record format that will be administered in Integra Suite. For more information on CDR output formats in Communication Manager, please refer to [2].



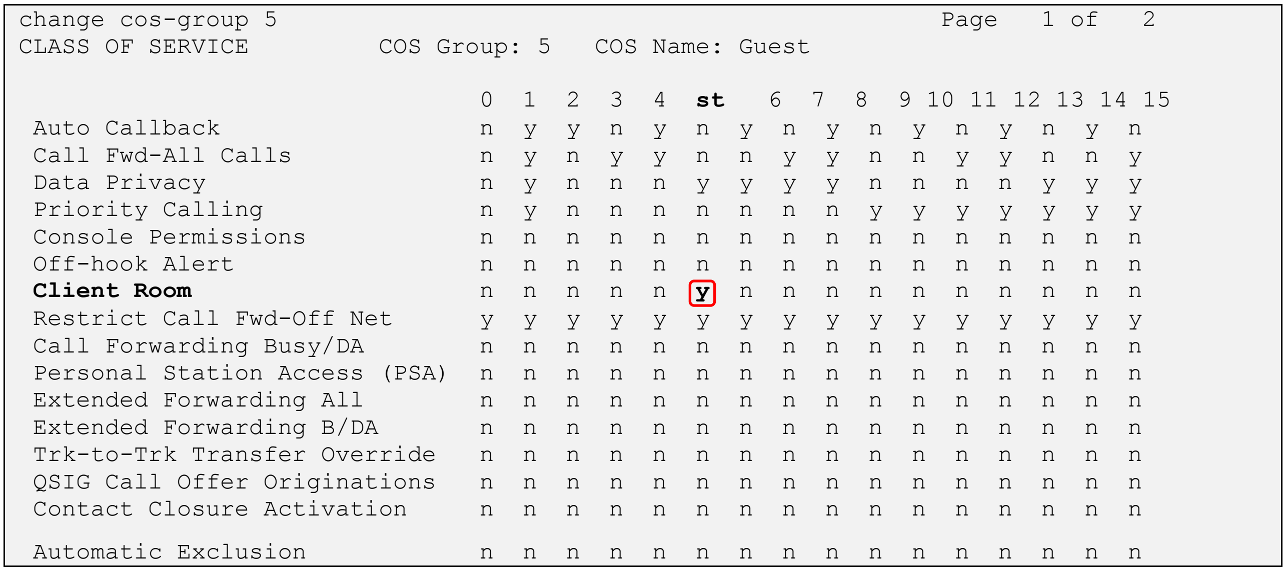
```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                     CDR Date Format: day/month
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? y                   Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? y
      Use Legacy CDR Formats? y                 Remove # From Called Number? n
Modified Circuit ID Display? y                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
```



```
change system-parameters cdr                                    Page   2 of   2
                            CDR SYSTEM PARAMETERS

     Data Item - Length         Data Item - Length         Data Item - Length
 1: date             - 6   17: in-crt-id        - 3   33:                  -
 2: space            - 1   18: space            - 1   34:                  -
 3: time             - 4   19: dialed-num       - 23  35:                  -
 4: space            - 1   20: space            - 1   36:                  -
 5: duration         - 4   21: calling-num      - 15  37:                  -
 6: space            - 1   22: space            - 1   38:                  -
 7: cond-code        - 1   23: auth-code        - 13  39:                  -
 8: space            - 1   24: return           - 1   40:                  -
 9: code-dial        - 4   25: line-feed        - 1   41:                  -
10: space            - 1   26:                  -     42:                  -
11: code-used        - 4   27:                  -     43:                  -
12: space            - 1   28:                  -     44:                  -
13: out-crt-id       - 3   29:                  -     45:                  -
14: space            - 1   30:                  -     46:                  -
15: in-trk-code      - 4   31:                  -     47:                  -
16: space            - 1   32:                  -     48:                  -
```

5.7. Add Client Room Properties to a Class of Service

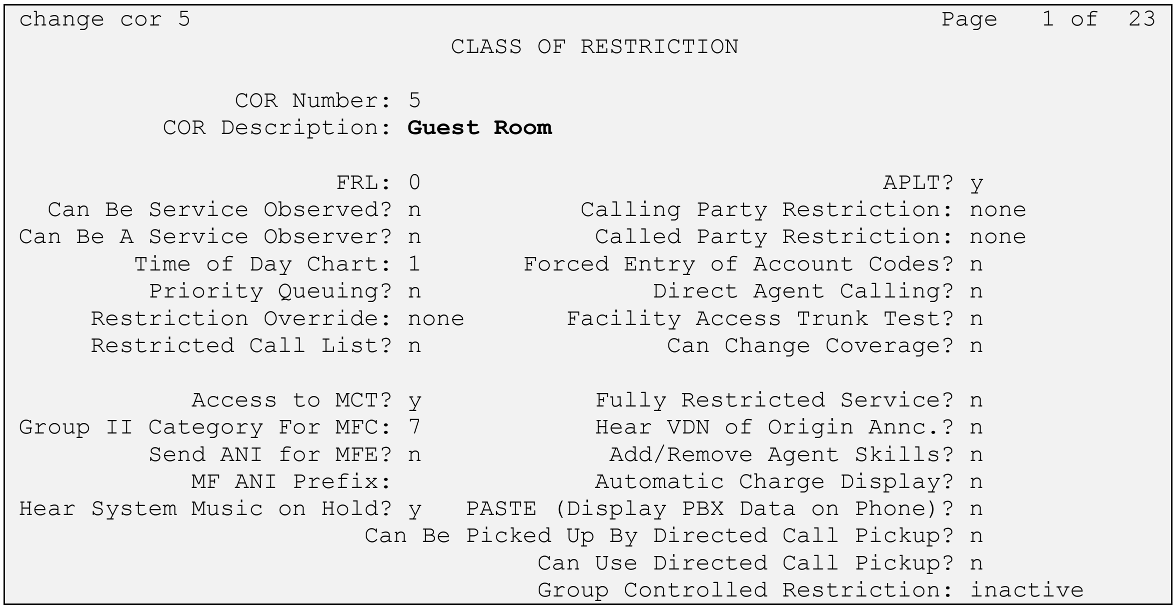
Enter **change cos**, and for the Class of Service to be assigned to guest telephones, set the **Client Room** field to **y** (as shown below for Class of Service **5**).



```
change cos-group 5                                              Page    1 of    2
CLASS OF SERVICE         COS Group: 5   COS Name: Guest

                                0  1  2  3  4  st   6  7  8  9 10 11 12 13 14 15
 Auto Callback                  n  y  y  n  y  n  y  n  y  n  y  n  y  n  y  n
 Call Fwd-All Calls             n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  y
 Data Privacy                   n  y  n  n  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling               n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  y
 Console Permissions            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  y  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Call Forwarding Busy/DA        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Personal Station Access (PSA)  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All        n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA       n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 QSIG Call Offer Originations   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Contact Closure Activation     n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n

 Automatic Exclusion            n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

5.8. Set Guest Room Calling Party Restrictions in a Class of Restriction (COR)

Enter **change cor *n***, where ***n*** is the number of the Class of Restriction to be assigned to guest telephones (in this example, COR **5** is used).



```
change cor 5                                                    Page    1 of   23
                              CLASS OF RESTRICTION

               COR Number: 5
          COR Description: Guest Room

                      FRL: 0                                APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

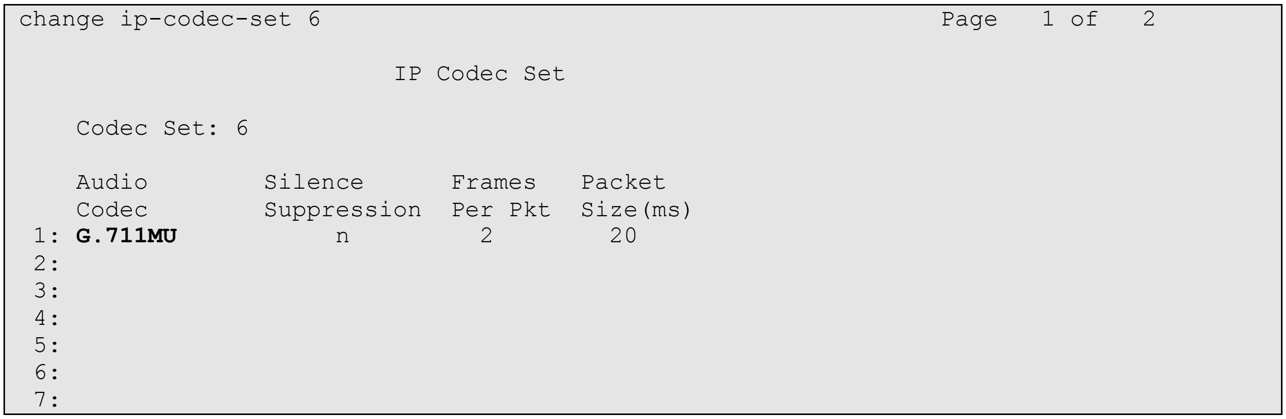
5.9. SIP Trunk to Integra Voice Mail/IVR

This section details the setup of the SIP trunk for calls to Voice Mail/IVR. It includes the following:

- Create IP Network Region and Codec
- Create Signalling-Group
- Add Sip Trunk-Group
- Create Uniform Dialplan
- Routing of IVR and Voice Mail calls

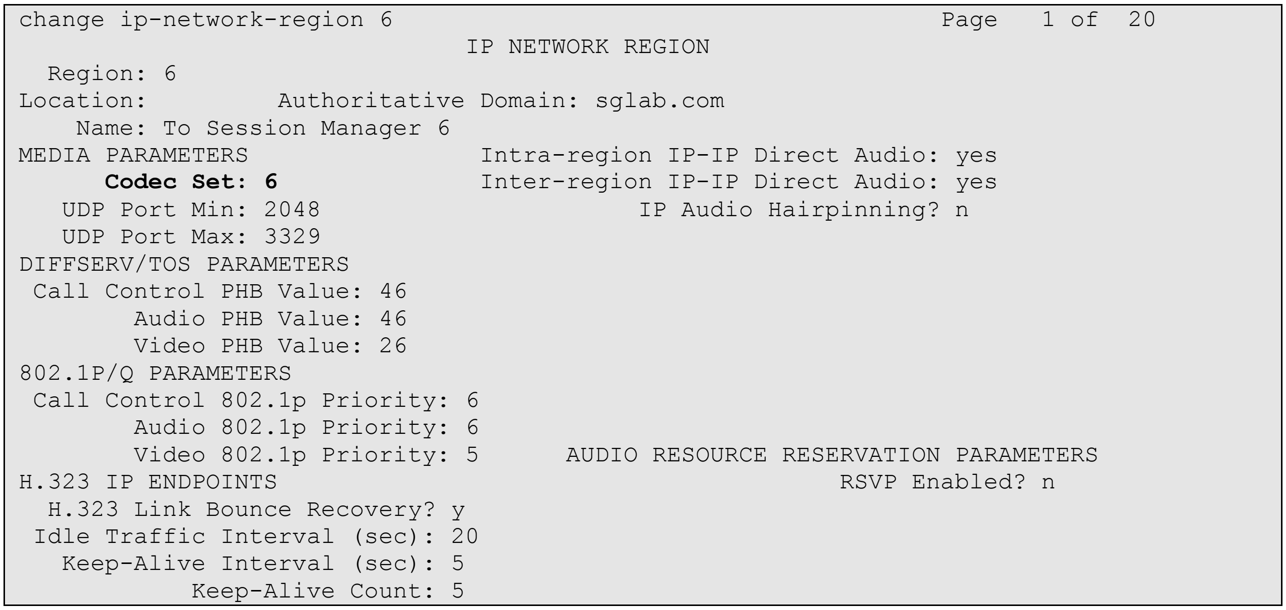
5.9.1. Create IP Network Region and Codec

Enter **change ip-codec-set 6** and check that the supported **G711Mu** audio codec is administered for IP Network Region 6 assigned in this compliance test for Integra Server.



```
change ip-codec-set 6                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 6

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

Enter **change ip-network-region 6** to check that the **Codec Set** is set to **6** above.

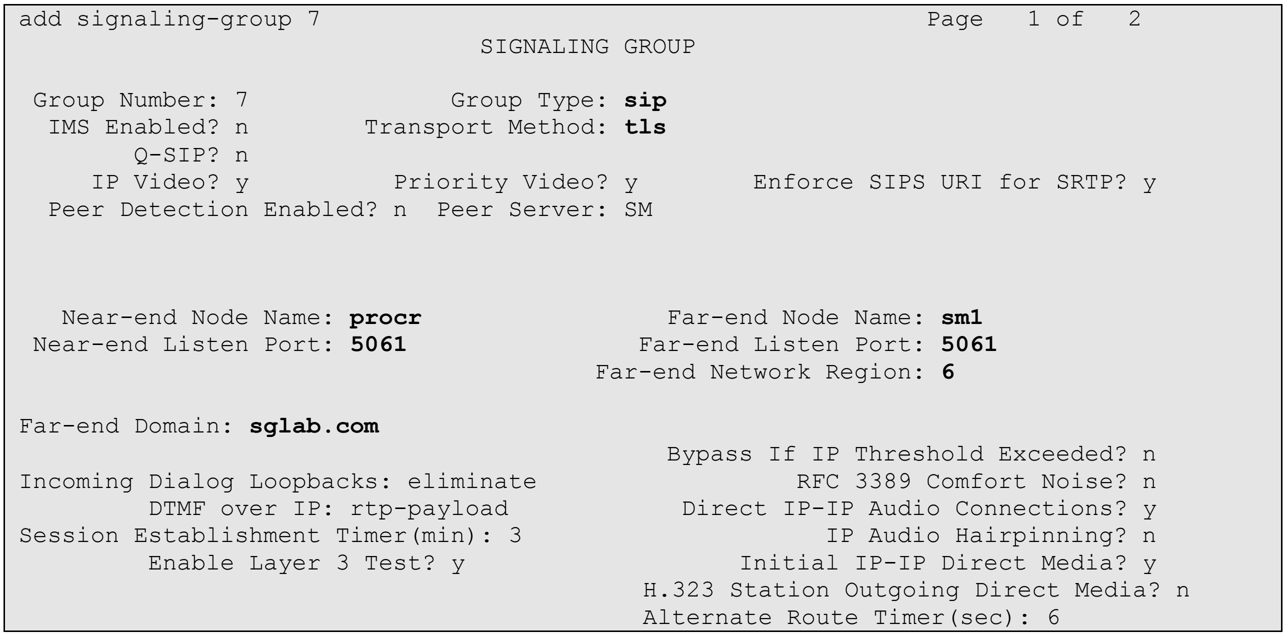


```
change ip-network-region 6                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 6
Location:          Authoritative Domain: sglab.com
    Name: To Session Manager 6
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 6              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   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
```

5.9.2. Create Signaling-Group

Enter **add sig n,** where **n** is the number of the signaling group created (in this example, signaling-group **7**). Enter the following parameter:

- **Group Type :** Enter **sip**
- **Transport Method :** Enter **tls**
- **Near-end Node Name:** Enter **procr**
- **Near-end Listen Port:** Enter **5061**
- **Far-end Node Name:** Enter **sm1**
- **Far-end Listen Port:** Enter **5061**
- **Far-end Network Region:** Enter **6**
- **Far-end Domain:** In this case **sglab.com**



```
add signaling-group 7                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 7              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? n  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: sm1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 6

Far-end Domain: sglab.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? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
                                            H.323 Station Outgoing Direct Media? n
                                            Alternate Route Timer(sec): 6
```

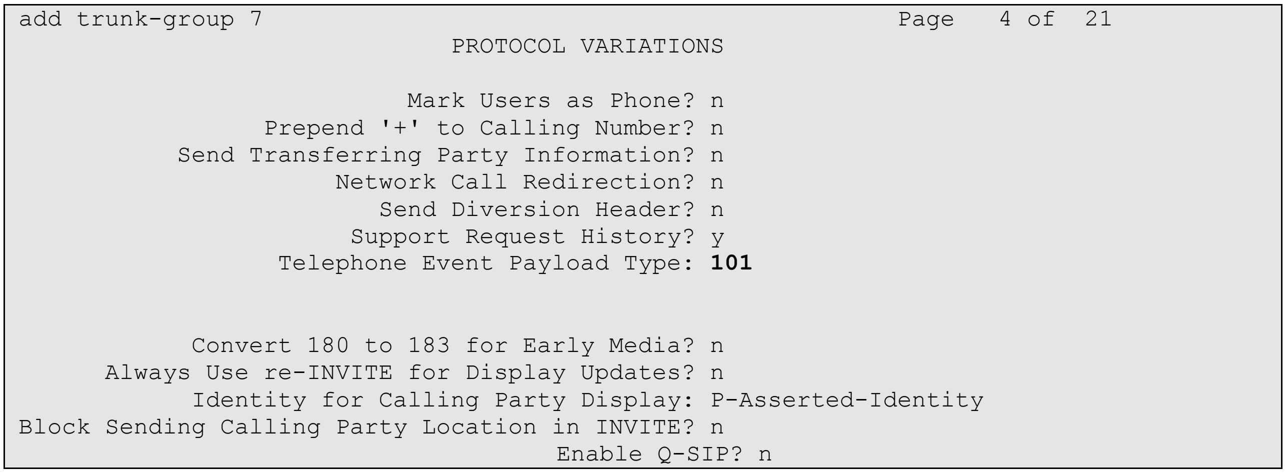
5.9.3. Add SIP Trunk-Group

Enter **add trunk n,** where **n** is the number of the trunk group created (in this example, trunk-group **7**). Enter the following parameter:

- **Group Name :** Enter appropriate name
- **Group Type :** Enter **sip**
- **Service Type :** Enter **tie**
- **Signaling Group:** Enter **7**
- **Number of Members:** Enter appropriate value
- **Numbering Format:** Enter **private**
- **Telephone Event Payload Type:** Enter **101**

```
add trunk-group 7                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 7                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SM1            COR: 1        TN: 1        TAC: #07
   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: 7
                                                     Number of Members: 14
```

```
change trunk-group 7                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? Y
```



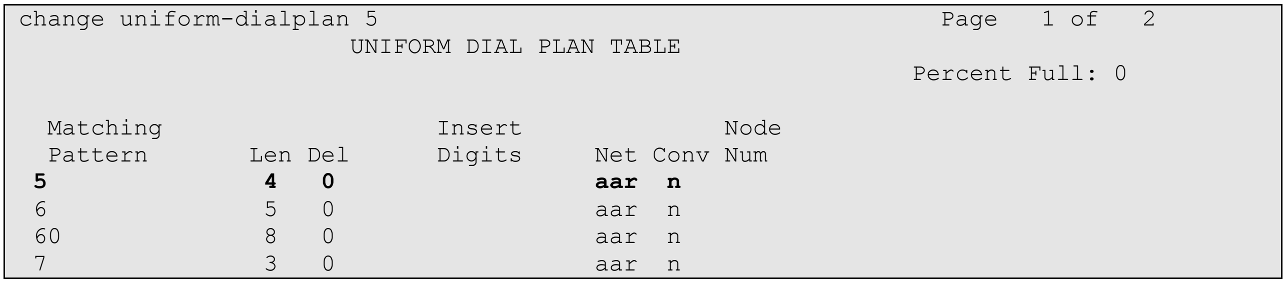
```
add trunk-group 7                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? n
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? n
                      Network Call Redirection? n
                         Send Diversion Header? n
                       Support Request History? y
                  Telephone Event Payload Type: 101


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? n
            Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                     Enable Q-SIP? n
```

5.9.4. Create Uniform Dialplan

Here are the access numbers for Voice Mail and IVR for room status submission:

S/No	Description	Number
1.	Voice Mail Retrieval	5500
2.	Voice Mail Reception	5600
3.	IVR for room status submission	5700

Enter **change uniform-dialplan 5** to create the uniform dialplan for 5XXX to dial the number without aar access code. At the **Matching Pattern** 5, enter the **Len** as 4 and the **Net** as aar.



```
change uniform-dialplan 5                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len  Del      Digits     Net  Conv Num
 5                4    0                  aar   n
 6                5    0                  aar   n
 60               8    0                  aar   n
 7                3    0                  aar   n
```

5.9.5. Private Numbering

Enter **change private-numbering 7** to set guest rooms number as private numbering format since digit 7 is the starting digit of the guest room numbers.

```
change private-numbering 7                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 5  1               6                           5     Total Administered: 4
 5  1               7                           5        Maximum Entries: 540
 5  2               10                          5
 5  7               7                           5
```

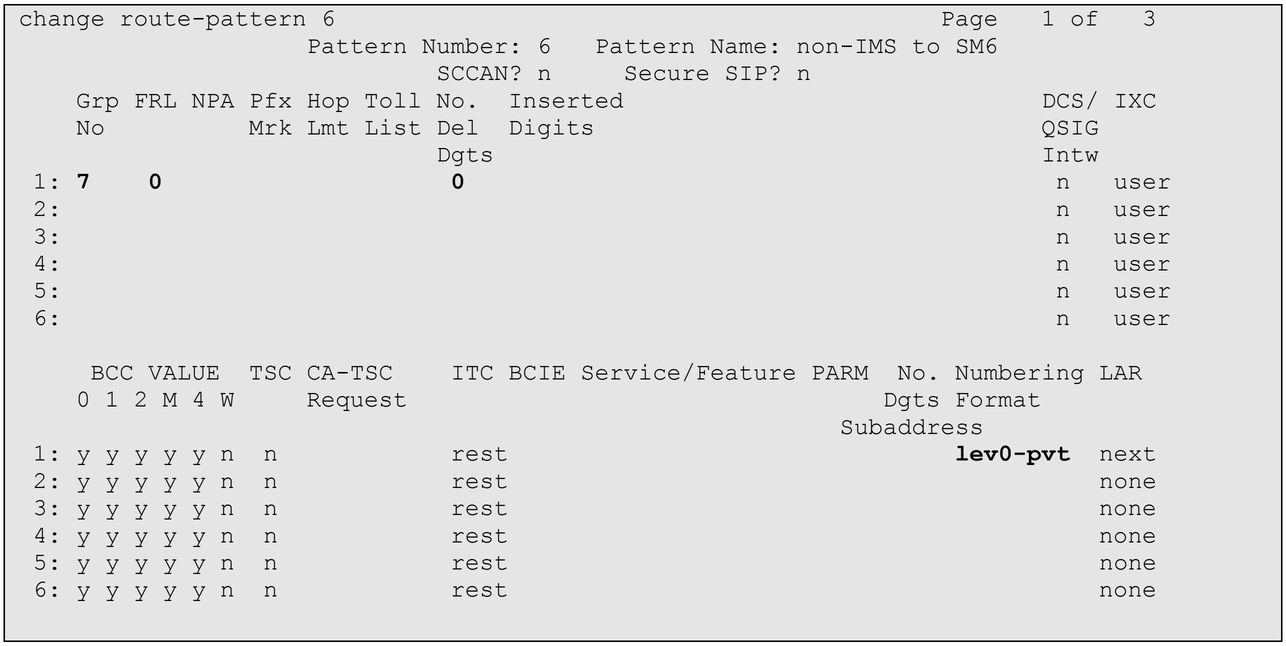
5.9.6. Routing of IVR and Voice Mail calls

Enter **change aar analysis 5** for routing 5XXX calls to Integra Voice Mail/IVR server which in this compliance testing is the same server.

Enter the values for **Dialed String** for 5 as below. **Call Type** is set as **lev0** to indicate private numbering for calling number to Voice Mail.

```
change aar analysis 5                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    5                     4    4     6        lev0         n
    6                     5    5     10       aar          n
    60                    8    8     70       aar          n
    68731233              8    8     30       pubu         n
    7                     3    3     70       aar          n
    702                   8    8     10       aar          n
```

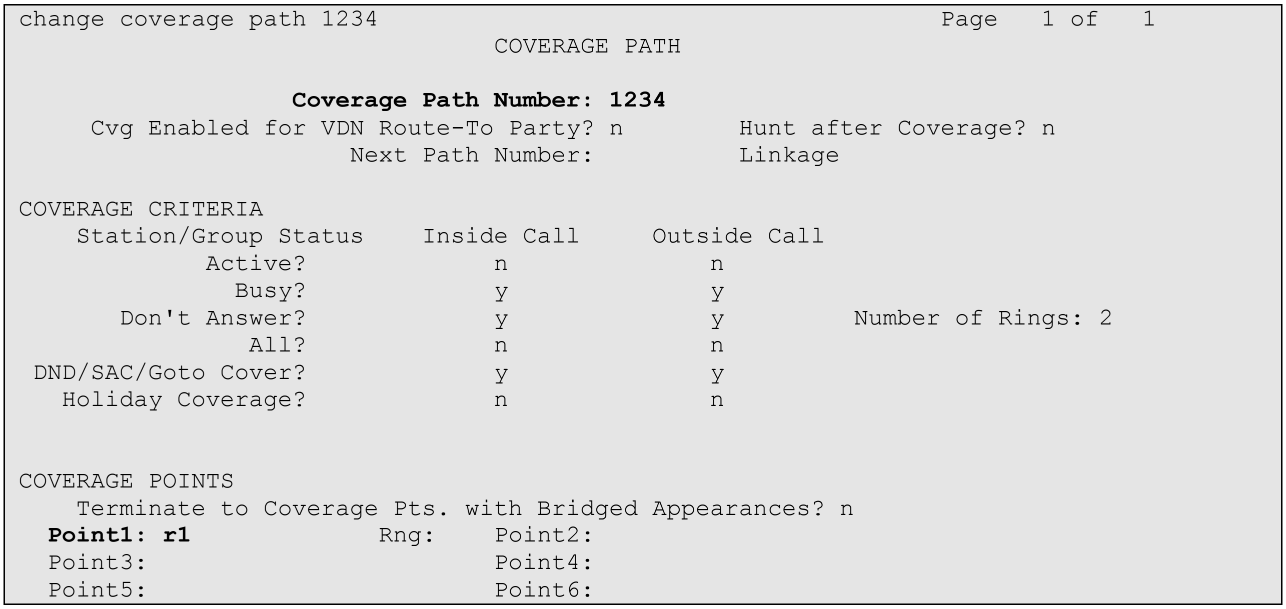
Enter **change route-pattern 6** and enter the trunk group number under the column **Grp No** as 7 created in **Section 5.9.3**. **Numbering Format** is set as **lev0-pvt** to set private numbering for calling number to Voice Mail.



```
change route-pattern 6                                          Page   1 of   3
                    Pattern Number: 6   Pattern Name: non-IMS to SM6
                             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: 7    0                    0                                         n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               lev0-pvt  next
 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
```

5.10. Creating Default Coverage Path

The default coverage path is created here for Voice Mail coverage**.** Enter **change coverage path 1234** and enter the Point1 as **r1** (coverage remote point 1).



```
change coverage path 1234                                       Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 1234
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
       Don't Answer?             y               y       Number of Rings: 2
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: r1            Rng:    Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

Enter **change coverage remote 1** and the point **01** as **85600** where 8 is the aar access code.

```
change coverage remote 1                                              Page   1 of  23

                       REMOTE CALL COVERAGE TABLE
                       ENTRIES FROM 1    TO 1000

01: 85600                 16:                        31:
02:                       17:                        32:
03:                       18:                        33:
04:                       19:                        34:
05:                       20:                        35:
06:                       21:                        36:
07:                       22:                        37:
```

5.11. Assign Class of Service and Class of Restriction Values to Guest Telephones

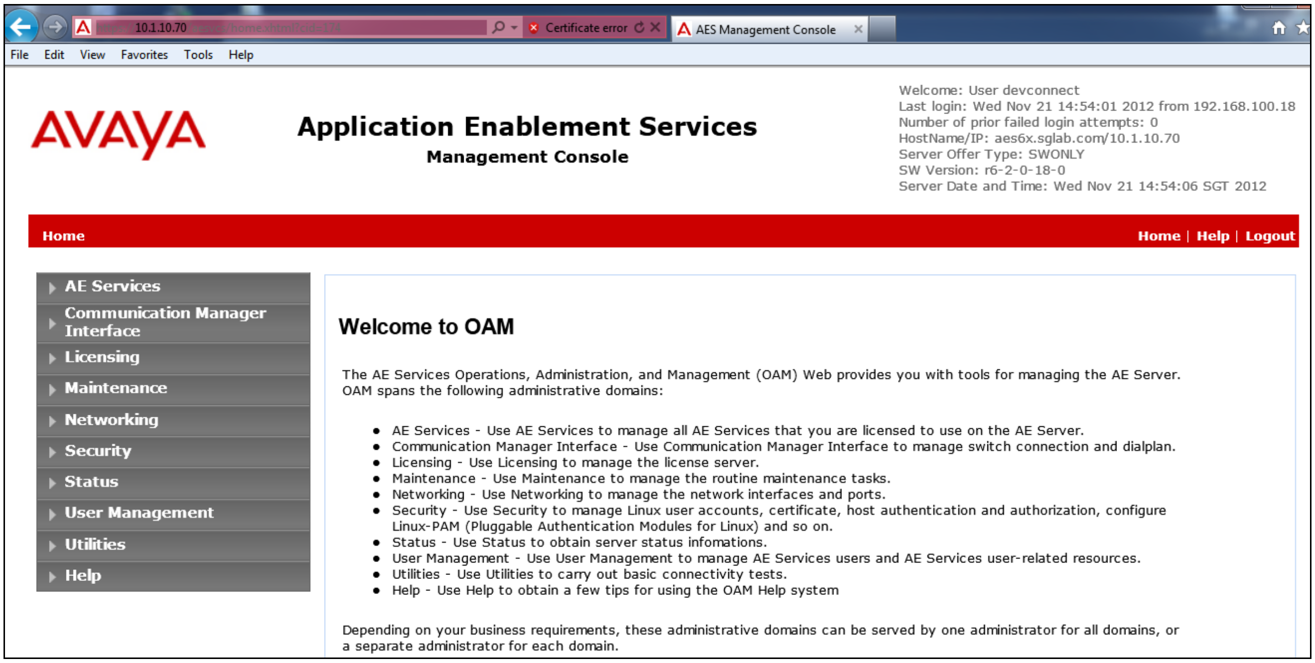
For each guest telephone extension ***x***, enter **change station *x*** and enter in the **COR** and **COS** fields the values corresponding to the Class of Service and Class of Restriction administered in **Section 5.7 and 5.8**, respectively.

```
change station 71121                                          Page   1 of   4
                                     STATION

Extension: 71121                         Lock Messages? n             BCC: 0
     Type: 1608                          Security Code: 111222         TN: 1
     Port: S00191                      Coverage Path 1:               COR: 5
     Name: Mr Meng                     Coverage Path 2:               COS: 5
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 71121
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
                              Short/Prefixed Registration Allowed: default
```

6. Configure Avaya Aura® Application Enablement Services Server

These instructions assume installation of the Avaya AES has already been completed with necessary basic setup administration.

Launch a web browser and enter **https://<IP address of AES server>** to access the Application Enablement Services Management Console. Log in using an administrative login and password (not shown), and the **Welcome To OAM** screen will be displayed.



Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Wed Nov 21 14:54:01 2012 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes6x.sglab.com/10.1.10.70
Server Offer Type: SWONLY
SW Version: r6-2-0-18-0
Server Date and Time: Wed Nov 21 14:54:06 SGT 2012

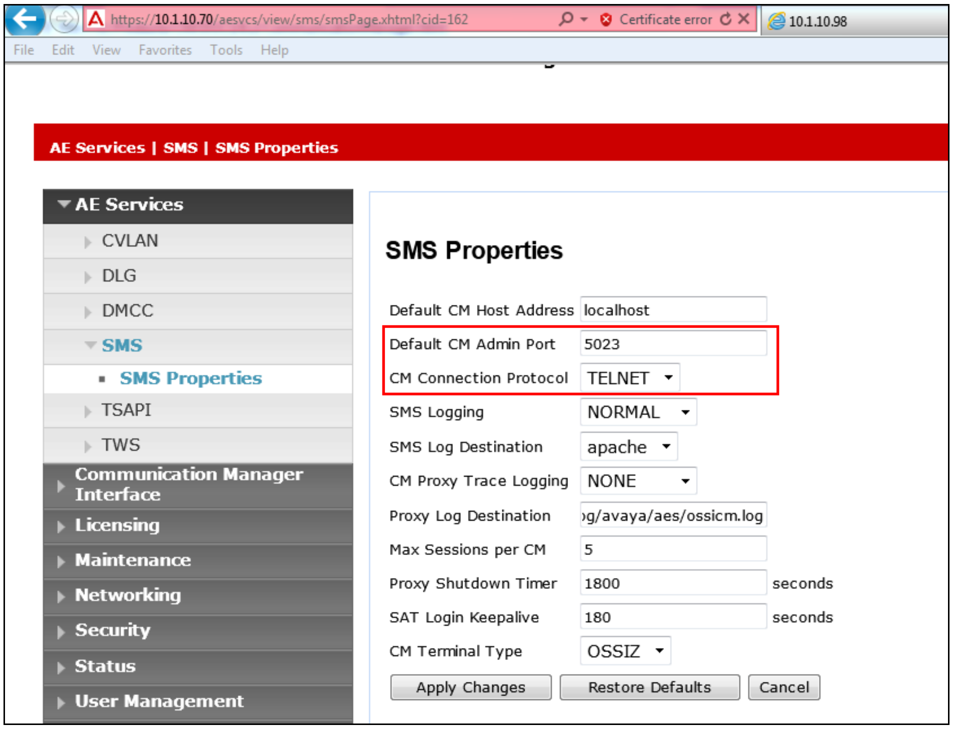
Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status infomations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Click **AE Services**, then **SMS → SMS Properties** in the left pane. Note the **Default CM Admin Port** and **CM Connection Protocol** for the Avaya AES SMS setup which will be used to verify the SMS functionality on the next page.



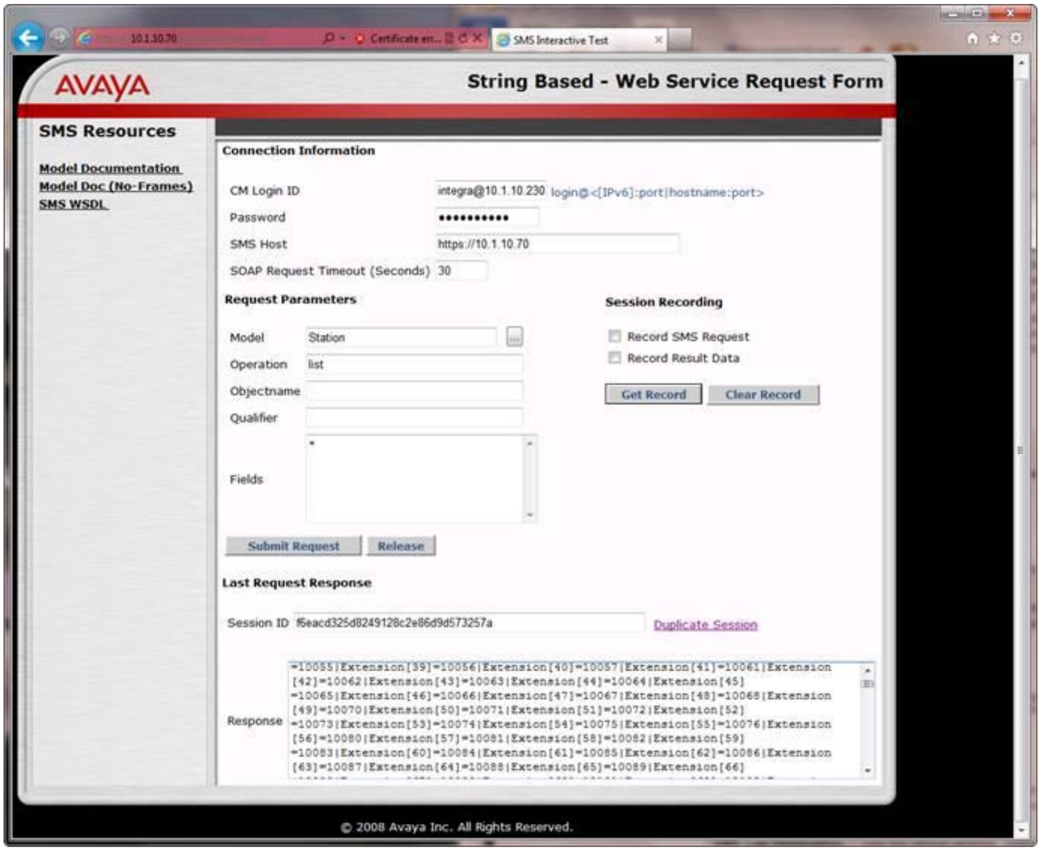
SMS Properties

Default CM Host Address	localhost
Default CM Admin Port	5023
CM Connection Protocol	TELNET
SMS Logging	NORMAL
SMS Log Destination	apache
CM Proxy Trace Logging	NONE
Proxy Log Destination	›g/avaya/aes/ossicm.log
Max Sessions per CM	5
Proxy Shutdown Timer	1800 seconds
SAT Login Keepalive	180 seconds
CM Terminal Type	OSSIZ

To check the SMS functionality, use a web browser, enter **https://<IP address of AES Server>/sms/sms_test.php** with the login/password created in **Section 5.5.3.**

- **CM Login ID :** Define the login in this format “login@<[IPv4/IPv6 of CM]:port”
- **Password :** Define the password
- **SMS Host:** https://<AES Server ip address>
- **Model:** Refer to any valid model from reference [3]
- **Operation:** Refer to any valid operation from reference [3]

Click **Submit Request** and there will be appropriate response if information above is correct.



String Based - Web Service Request Form

Connection Information

CM Login ID: integra@10.1.10.230 login@<[IPv6]:port|hostname:port>

Password: ••••••••••••

SMS Host: https://10.1.10.70

SOAP Request Timeout (Seconds): 30

Request Parameters

Model: Station

Operation: list

Objectname:

Qualifier:

Fields: *

Session Recording

□ Record SMS Request

□ Record Result Data

Last Request Response

Session ID: f6eacd325d8249128c2e86d9d573257a

Response:

```
=10055|Extension[39]=10056|Extension[40]=10057|Extension[41]=10061|Extension
[42]=10062|Extension[43]=10063|Extension[44]=10064|Extension[45]
=10065|Extension[46]=10066|Extension[47]=10067|Extension[48]=10068|Extension
[49]=10070|Extension[50]=10071|Extension[51]=10072|Extension[52]
=10073|Extension[53]=10074|Extension[54]=10075|Extension[55]=10076|Extension
[56]=10080|Extension[57]=10081|Extension[58]=10082|Extension[59]
=10083|Extension[60]=10084|Extension[61]=10085|Extension[62]=10086|Extension
[63]=10087|Extension[64]=10088|Extension[65]=10089|Extension[66]
```

7. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Avaya Aura Session Manager to support the routing of calls to Integra Suite server.

These instructions assume other administration activities have already been completed such as defining SIP entities for Session Manager, defining the network connection between System Manager and Session Manager, and defining Communication Manager as a Managed Element.

The following administration activities will be described:

- Define SIP Domain and Locations
- Define SIP Entity for Integra Server
- Define Entity Links, which describe the SIP trunk parameters used by Integra Server when routing calls between SIP Entities
- Define Routing Policies and Dial Patterns which control routing between SIP Entities

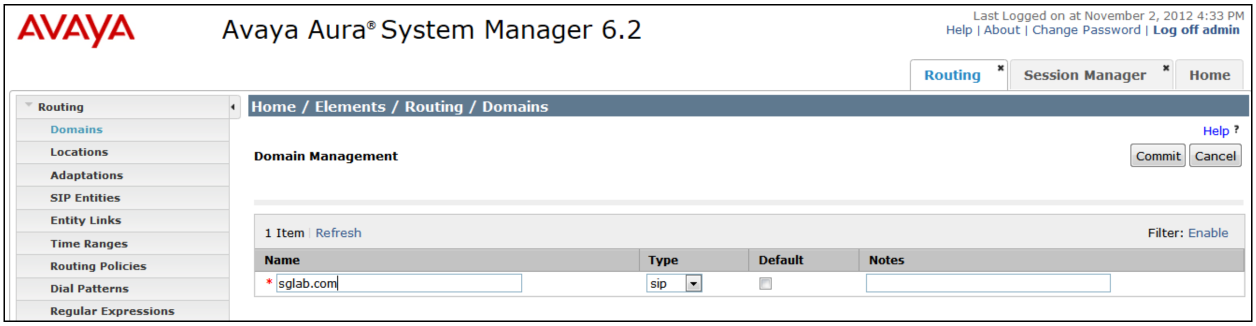
Configuration is accomplished by accessing the browser-based GUI of Avaya System Manager, using the URL "**http://<ip-address>/SMGR**", where "**<ip-address>**" is the IP address of Avaya System Manager. Log in with the appropriate credentials.

7.1. Define SIP Domains

Expand **Elements →Routing** and select **Domains** from the left navigation menu.
Click **New**. Enter the following values and use default values for remaining fields**.**

- **Name** Enter the Authoritative Domain Name
  For the sample configuration, "**sglab.com**" was used.
- **Type** Select "**sip**" from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



Domain Management

1 Item

Name	Type	Default	Notes
* sglab.com	sip	☐	

7.2. Define Locations

Locations are used to identify logical and/or physical locations where SIP Entities or SIP endpoints reside, for purposes of bandwidth management or location-based routing.
Expand **Elements** →**Routing** and select **Locations** from the left navigation menu.

Click **New** (not shown)**.** In the **General** section, enter the following values and use default values for remaining fields.

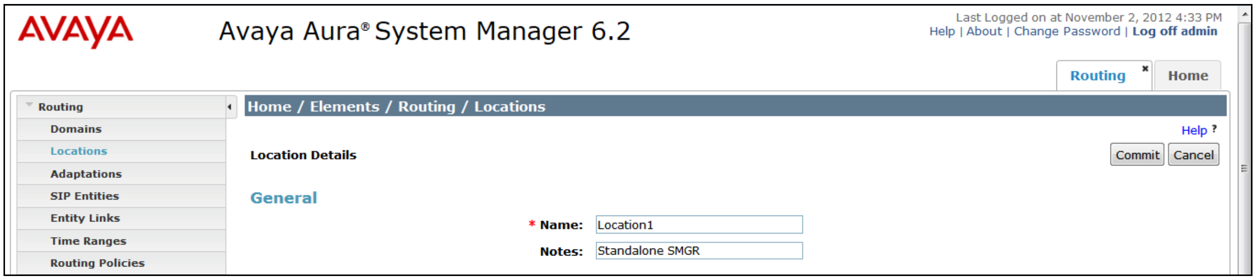
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

Scroll down to the **Location Pattern** section and lick **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- For the sample configuration, "**10.1.***" was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows a Location used for SIP entities in the sample configuration.



Home / Elements / Routing / Locations

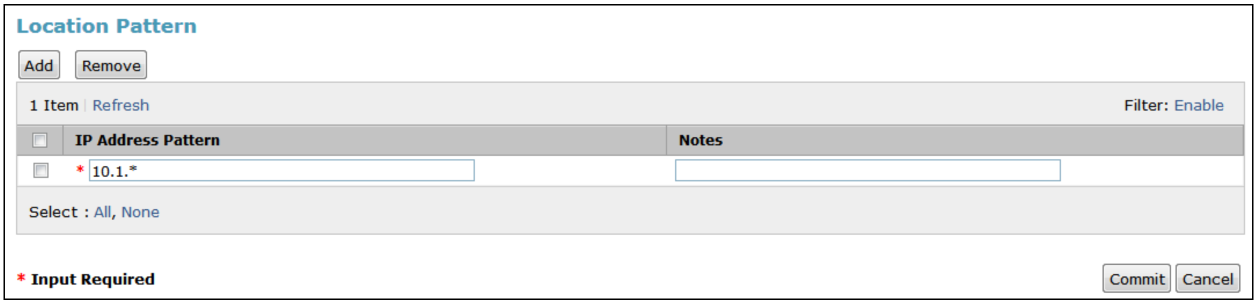
Location Details

General

* Name: Location1

Notes: Standalone SMGR

Note: screen has been abbreviated for clarity.



Location Pattern

1 Item

☐	IP Address Pattern	Notes
☐	* 10.1.*	

* Input Required

7.3. Define SIP Entities

A SIP Entity must be added for Communication Manager Server. To add a SIP Entity, expand **Elements →Routing** and select **SIP Entities** from the left navigation menu.

Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

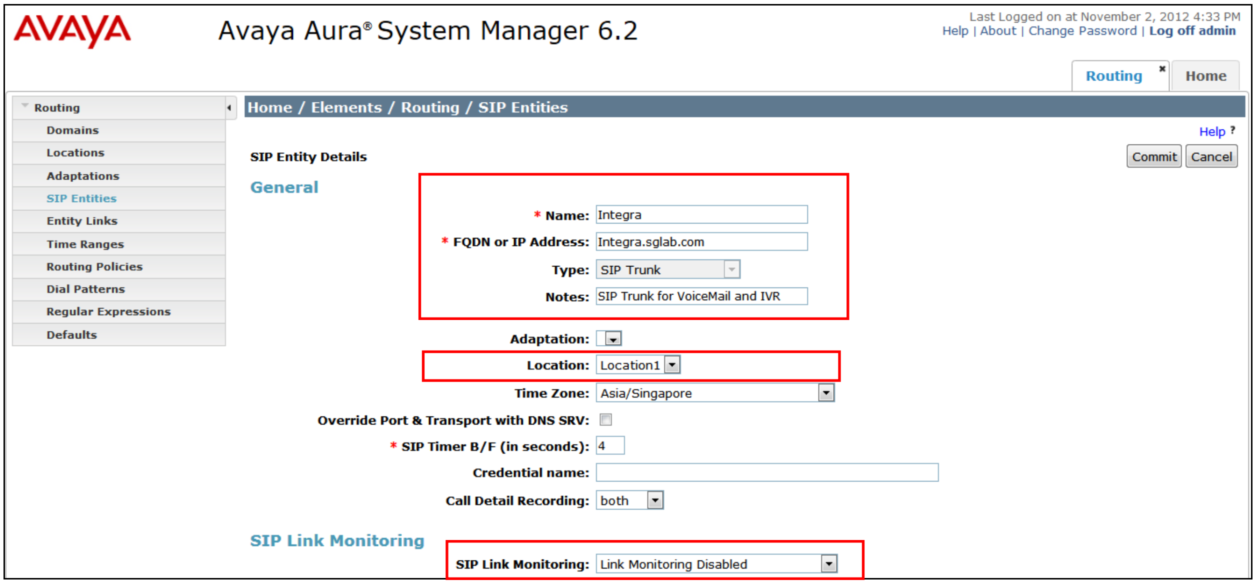
- **Name:** Enter an identifier for new SIP Entity.
  In the sample configuration, "**Integra**" was used.
- **FQDN or IP Address:** Enter FQDN as **Integra.sglab.com** as this has been map to 10.1.10.125
- **Type:** Select "**SIP Trunk**"
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select Location defined for Communication Manager in **Section 7.2**.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select "**Link Monitoring Disabled**". This is because Integra Voice Mail Server does not support OPTION request for status.

Click **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Communication Manager.



SIP Entity Details

General

* Name: Integra

* FQDN or IP Address: Integra.sglab.com

Type: SIP Trunk

Notes: SIP Trunk for VoiceMail and IVR

Adaptation:

Location: Location1

Time Zone: Asia/Singapore

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: both

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

7.4. Define Entity Links

A SIP trunk between Integra Server and Communication Manager is described by an Entity Link. In the sample configuration, SIP Entity Links were added between Communication Manager and Integra Server.

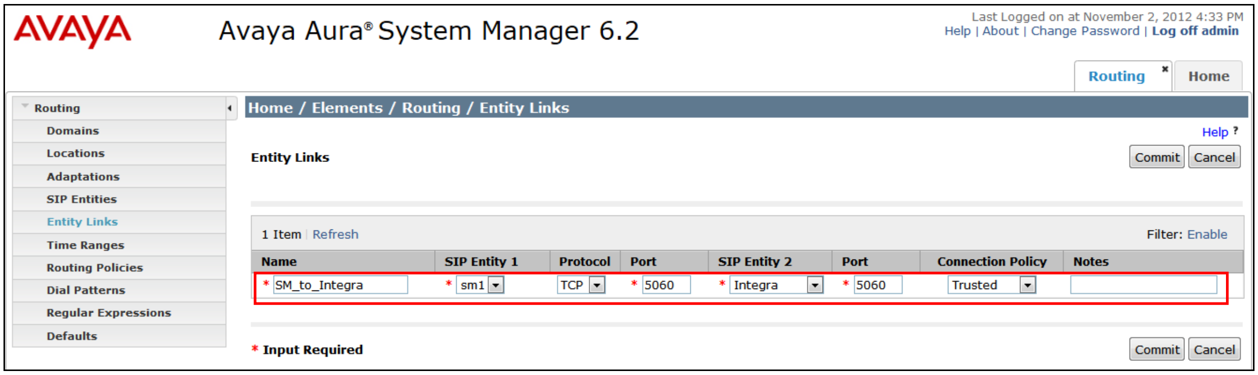
To add an Entity Link, expand **Elements** →**Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to Communication Manager.
- **SIP Entity 1** Select Session Manager already defined.
- **SIP Entity 2** Select the SIP Entity added for Communication Manager defined in **Section 7.3** from drop-down menu.
- **Protocol** After selecting both SIP Entities, verify "**TCP**" is selected as the required Protocol.
- **Port** Verify **Port** for both SIP entities is "**5060**".
- **Trusted** Enter .

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Communication Manager Server and Session Manager.



Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM_to_Integra	* sm1	TCP	* 5060	* Integra	* 5060	Trusted	

* Input Required

7.5. Define Routing Policy

Routing policies describe the conditions under which calls will be routed.

To add a routing policy, expand **Elements →Routing** and select **Routing Policies.**

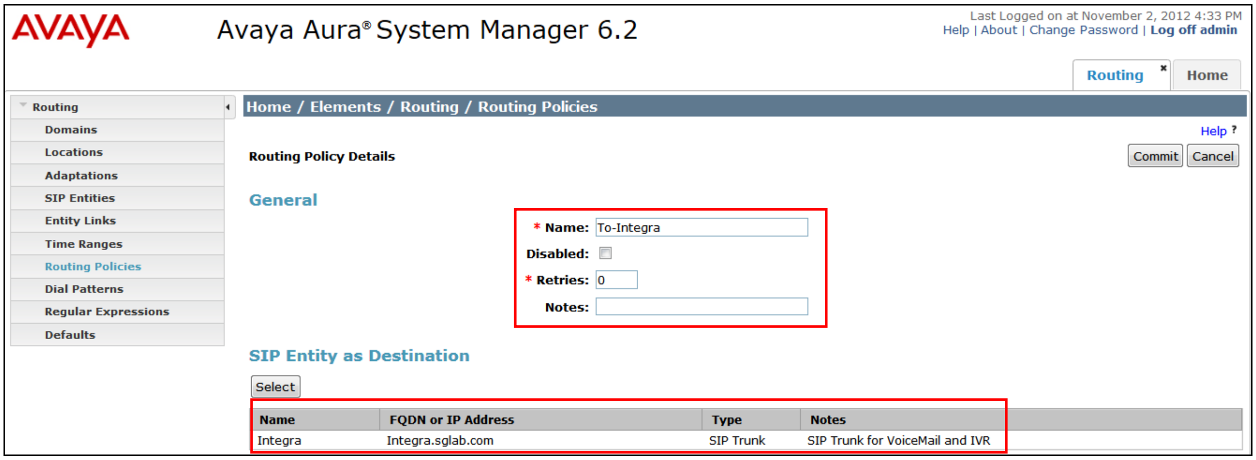
Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier for routing to Integra Server.
- **Disabled:** Leave unchecked.
- **Retries:** Retain default value of "**0**".
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the SIP Entity defined for Integra Server in **Section 7.3** and click **Select.**

The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

The following screen shows the Routing Policy for Communication Manager Server.



Routing Policy Details

General

* Name: To-Integra

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Integra	Integra.sglab.com	SIP Trunk	SIP Trunk for VoiceMail and IVR

7.6. Define Dial Pattern

This section describes the steps to define a dial pattern to route calls to Integra Server. In the sample configuration, 4-digit extensions beginning with “**5XXX**” are assigned to Voice Mail Retrieval/Reception and IVR for room status update.

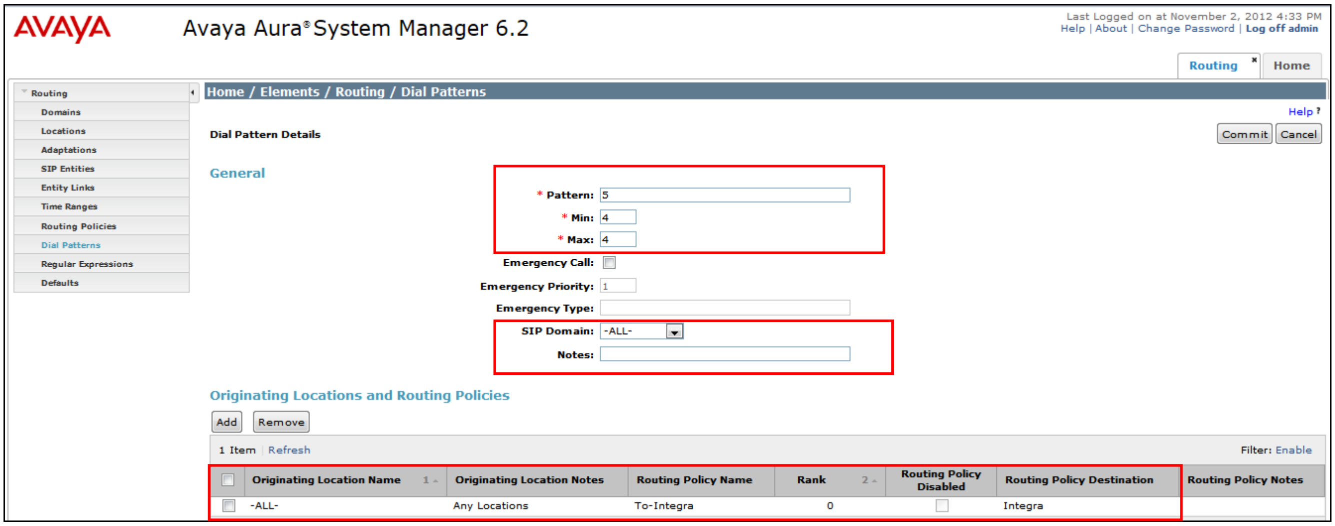
To define a dial pattern, expand **Elements** →**Routing** and select **Dial Patterns.** Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for the Voice Mail/IVR numbers.
- **Min:** Enter the minimum number digits that must be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select “**ALL**” if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add.**
The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select “**ALL**” .
- In **Routing Policies** table, select the appropriate Routing Policy defined for routing to Integra Server in **Section 7.5.**
- Click **Select** to save these changes and return to **Dial Patterns Details** page.

Click **Commit** to save the new definition. The following screen shows the Dial Pattern defined for routing calls to Integra Server.



Dial Pattern Details

General

* Pattern: 5

* Min: 4

* Max: 4

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

1 Item

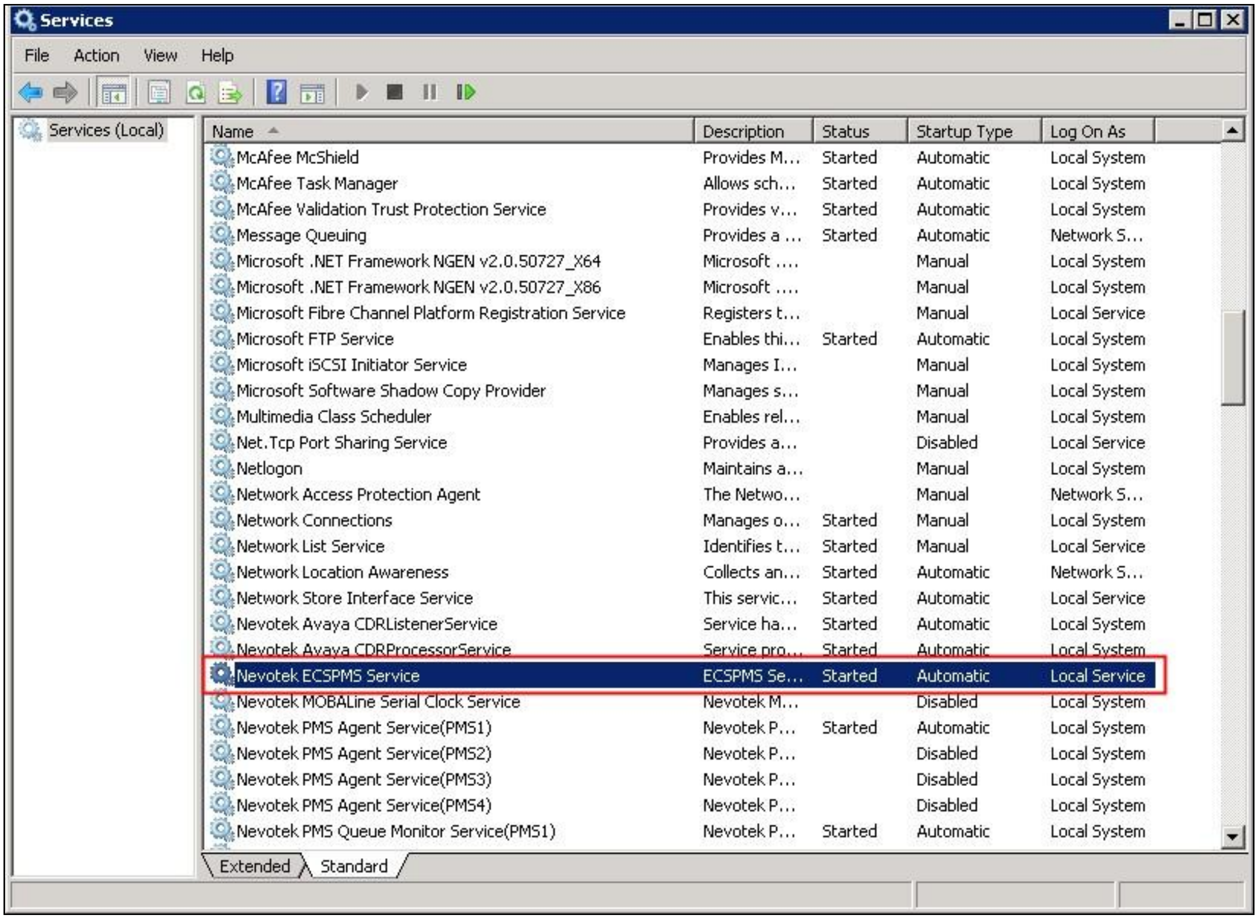
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To-Integra	0	□	Integra	

8. Configure Integra Suite

This section details the essential portion of the Integra Suite configuration to interoperate with Avaya Communication Manager. These Application Notes assume that the Integra Suite application has already been properly installed by Convera services personnel. Further details of the Integra Suite setup can be found in the Integra Installation Guide V1.0 **[6]**.

8.1. PMS interface

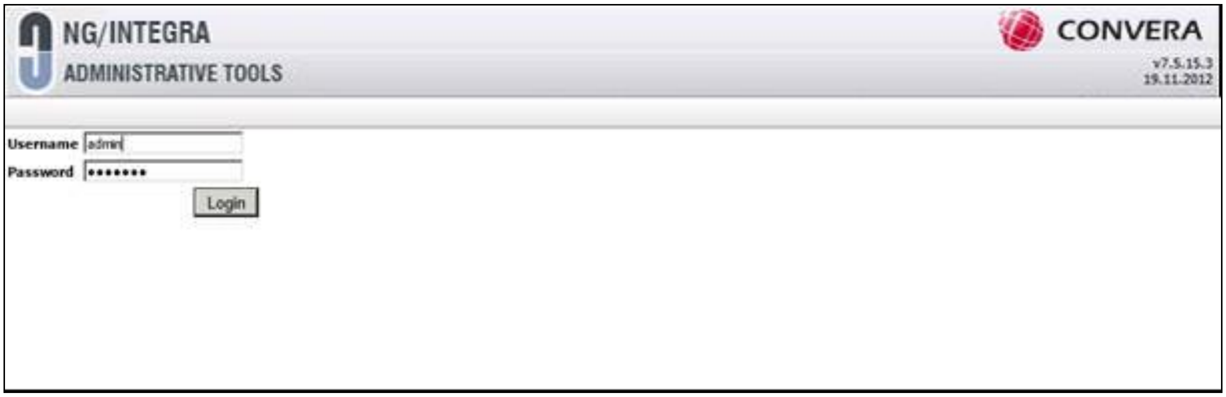
The Integra PMS port is fixed at **5103**. The **Nevotek ECSPMS Service** is to be running to receive guest operations commands like check in/out, light on/off.



Name	Description	Status	Startup Type	Log On As
McAfee McShield	Provides M...	Started	Automatic	Local System
McAfee Task Manager	Allows sch...	Started	Automatic	Local System
McAfee Validation Trust Protection Service	Provides v...	Started	Automatic	Local System
Message Queuing	Provides a ...	Started	Automatic	Network S...
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft		Manual	Local System
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft		Manual	Local System
Microsoft Fibre Channel Platform Registration Service	Registers t...		Manual	Local Service
Microsoft FTP Service	Enables thi...	Started	Automatic	Local System
Microsoft iSCSI Initiator Service	Manages I...		Manual	Local System
Microsoft Software Shadow Copy Provider	Manages s...		Manual	Local System
Multimedia Class Scheduler	Enables rel...		Manual	Local System
Net.Tcp Port Sharing Service	Provides a...		Disabled	Local Service
Netlogon	Maintains a...		Manual	Local System
Network Access Protection Agent	The Netwo...		Manual	Network S...
Network Connections	Manages o...	Started	Manual	Local System
Network List Service	Identifies t...	Started	Manual	Local Service
Network Location Awareness	Collects an...	Started	Automatic	Network S...
Network Store Interface Service	This servic...	Started	Automatic	Local Service
Nevotek Avaya CDRListenerService	Service ha...	Started	Automatic	Local System
Nevotek Avaya CDRProcessorService	Service pro...	Started	Automatic	Local System
Nevotek ECSPMS Service	ECSPMS Se...	Started	Automatic	Local Service
Nevotek MOBALine Serial Clock Service	Nevotek M...		Disabled	Local System
Nevotek PMS Agent Service(PMS1)	Nevotek P...	Started	Automatic	Local System
Nevotek PMS Agent Service(PMS2)	Nevotek P...		Disabled	Local System
Nevotek PMS Agent Service(PMS3)	Nevotek P...		Disabled	Local System
Nevotek PMS Agent Service(PMS4)	Nevotek P...		Disabled	Local System
Nevotek PMS Queue Monitor Service(PMS1)	Nevotek P...	Started	Automatic	Local System

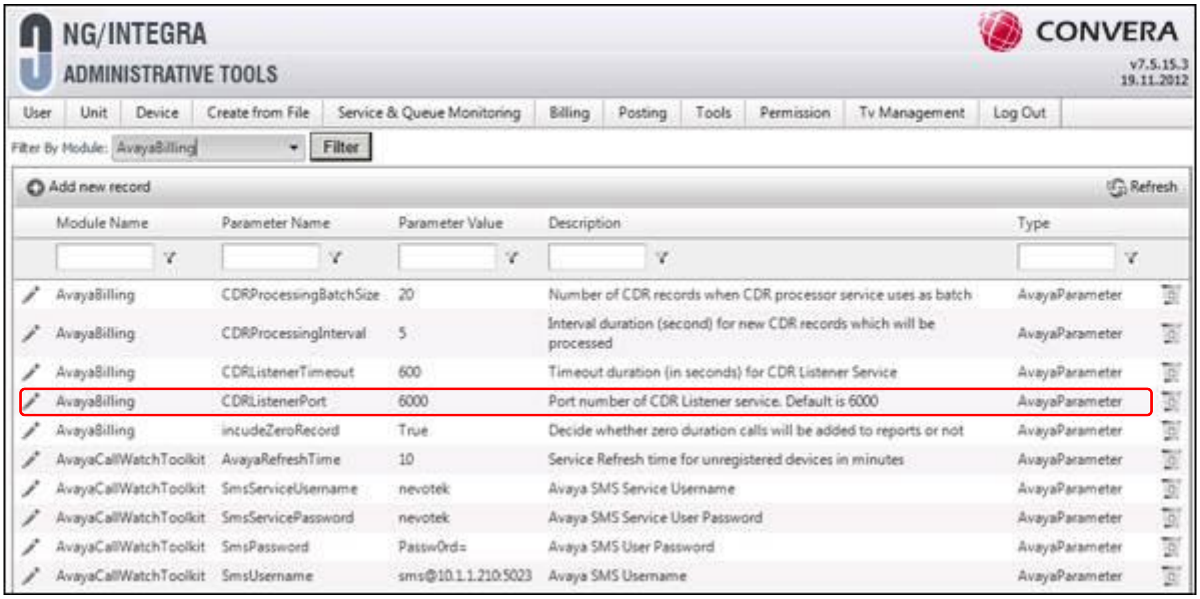
8.2. CDR interface

Integra Suite provides a web interface for administration. Administrator can login with the appropriate login credentials from http://localhost/AdministrativeTools/Default.aspx as shown below.



Username admin
Password •••••••

The Integra CDR listening port is configured as **6000** in **Section 5.4.** The parameter can be verified from the Administrative Tools. Navigate to "**Tools → Parameter Maintenance**" and select from the drop down menu for **AvayaBilling.** The "**CDRListenerPort**" under the **Parameter Name** column is shown as **6000**. .

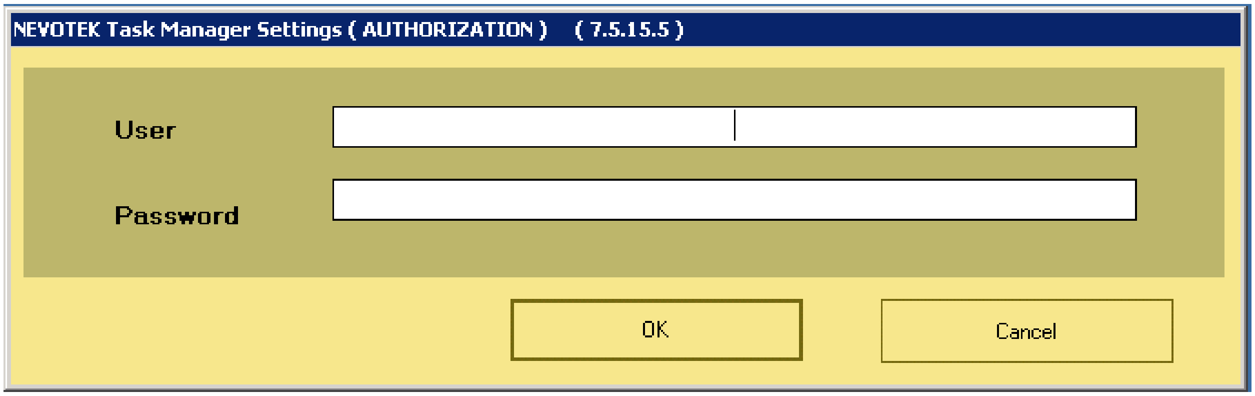


Filter By Module: AvayaBilling

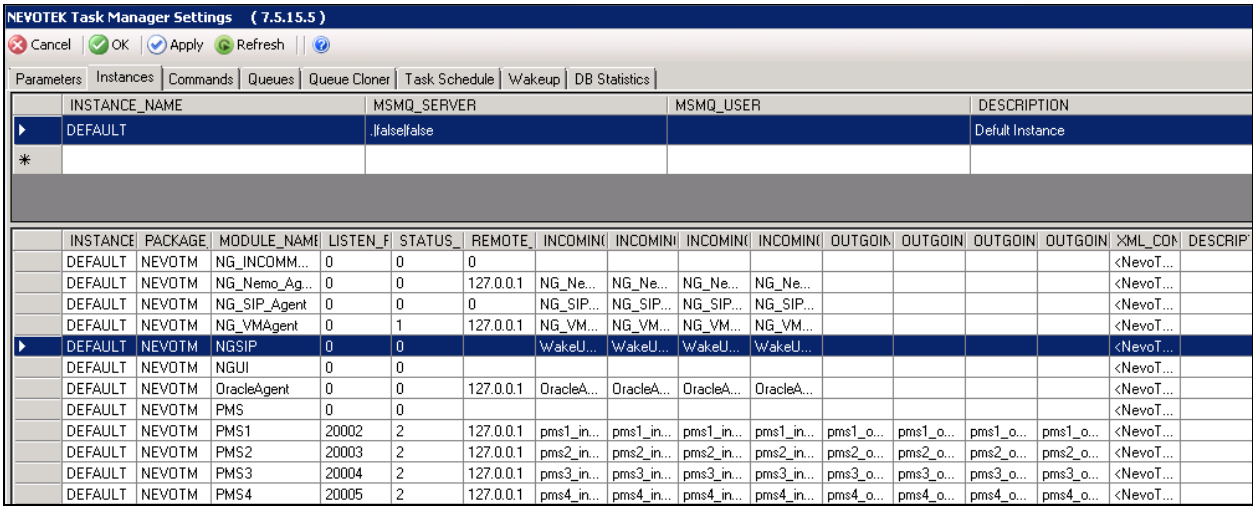
Module Name	Parameter Name	Parameter Value	Description	Type
AvayaBilling	CDRProcessingBatchSize	20	Number of CDR records when CDR processor service uses as batch	AvayaParameter
AvayaBilling	CDRProcessingInterval	5	Interval duration (second) for new CDR records which will be processed	AvayaParameter
AvayaBilling	CDRListenerTimeout	600	Timeout duration (in seconds) for CDR Listener Service	AvayaParameter
AvayaBilling	CDRListenerPort	6000	Port number of CDR Listener service. Default is 6000	AvayaParameter
AvayaBilling	incudeZeroRecord	True	Decide whether zero duration calls will be added to reports or not	AvayaParameter
AvayaCallWatchToolkit	AvayaRefreshTime	10	Service Refresh time for unregistered devices in minutes	AvayaParameter
AvayaCallWatchToolkit	SmsServiceUsername	nevotek	Avaya SMS Service Username	AvayaParameter
AvayaCallWatchToolkit	SmsServicePassword	nevotek	Avaya SMS Service User Password	AvayaParameter
AvayaCallWatchToolkit	SmsPassword	Passw0rd=	Avaya SMS User Password	AvayaParameter
AvayaCallWatchToolkit	SmsUsername	sms@10.1.1.210:5023	Avaya SMS Username	AvayaParameter

8.3. SIP Trunking

The configuration of the SIP Trunk to Communication Manager is done via the NevoTM Setting. On the Integra server, click "Start → All Programs → Nevotek → New Generation → NevoTM_Setting" and the screen below pop up and login with the appropriate credentials.


NEVOTEK Task Manager Settings (AUTHORIZATION) (7.5.15.5)
User
Password
OK
Cancel

The following is the resulting screen after login. Click on the **Instances** tab and navigate to **NGSIP** under the **MODULE_NAME** column and click on the line.

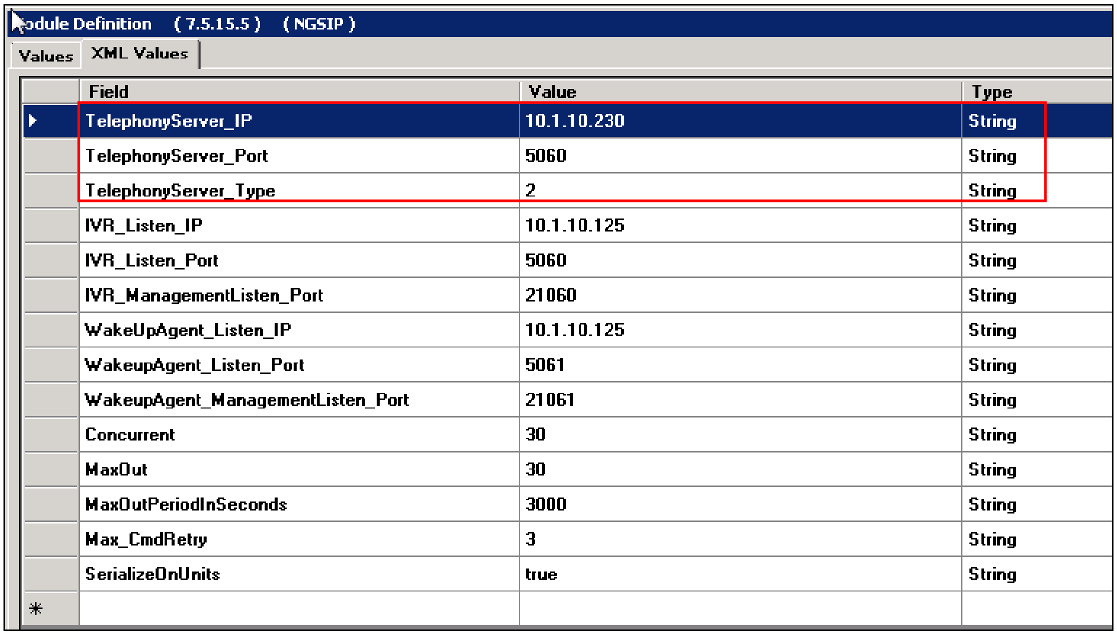


	INSTANCE_NAME	MSMQ_SERVER	MSMQ_USER	DESCRIPTION
▶	DEFAULT	.|false|false		Defult Instance
*				

	INSTANCE	PACKAGE_	MODULE_NAME	LISTEN_F	STATUS_	REMOTE_	INCOMIN(	INCOMIN(	INCOMIN(	INCOMIN(	OUTGOIN	OUTGOIN	OUTGOIN	OUTGOIN	XML_CON	DESCRIP
	DEFAULT	NEVOTM	NG_INCOMM...	0	0	0									<NevoT...	
	DEFAULT	NEVOTM	NG_Nemo_Ag...	0	0	127.0.0.1	NG_Ne...	NG_Ne...	NG_Ne...	NG_Ne...					<NevoT...	
	DEFAULT	NEVOTM	NG_SIP_Agent	0	0	0	NG_SIP...	NG_SIP...	NG_SIP...	NG_SIP...					<NevoT...	
	DEFAULT	NEVOTM	NG_VMAgent	0	1	127.0.0.1	NG_VM...	NG_VM...	NG_VM...	NG_VM...					<NevoT...	
▶	DEFAULT	NEVOTM	NGSIP	0	0		WakeU...	WakeU...	WakeU...	WakeU...					<NevoT...	
	DEFAULT	NEVOTM	NGUI	0	0										<NevoT...	
	DEFAULT	NEVOTM	OracleAgent	0	0	127.0.0.1	OracleA...	OracleA...	OracleA...	OracleA...					<NevoT...	
	DEFAULT	NEVOTM	PMS	0	0										<NevoT...	
	DEFAULT	NEVOTM	PMS1	20002	2	127.0.0.1	pms1_in...	pms1_in...	pms1_in...	pms1_in...	pms1_o...	pms1_o...	pms1_o...	pms1_o...	<NevoT...	
	DEFAULT	NEVOTM	PMS2	20003	2	127.0.0.1	pms2_in...	pms2_in...	pms2_in...	pms2_in...	pms2_o...	pms2_o...	pms2_o...	pms2_o...	<NevoT...	
	DEFAULT	NEVOTM	PMS3	20004	2	127.0.0.1	pms3_in...	pms3_in...	pms3_in...	pms3_in...	pms3_o...	pms3_o...	pms3_o...	pms3_o...	<NevoT...	
	DEFAULT	NEVOTM	PMS4	20005	2	127.0.0.1	pms4_in...	pms4_in...	pms4_in...	pms4_in...	pms4_o...	pms4_o...	pms4_o...	pms4_o...	<NevoT...	

The following screen is displayed. Check that the following parameters are setup appropriately:

TelephonyServer_IP:	<IP address of Communication Manager>
TelephonyServer_Port:	**5060**
TelephonyServer_Type:	**2** = Operations are processed using only SMS service



Field	Value	Type
TelephonyServer_IP	10.1.10.230	String
TelephonyServer_Port	5060	String
TelephonyServer_Type	2	String
IVR_Listen_IP	10.1.10.125	String
IVR_Listen_Port	5060	String
IVR_ManagementListen_Port	21060	String
WakeUpAgent_Listen_IP	10.1.10.125	String
WakeupAgent_Listen_Port	5061	String
WakeupAgent_ManagementListen_Port	21061	String
Concurrent	30	String
MaxOut	30	String
MaxOutPeriodInSeconds	3000	String
Max_CmdRetry	3	String
SerializeOnUnits	true	String

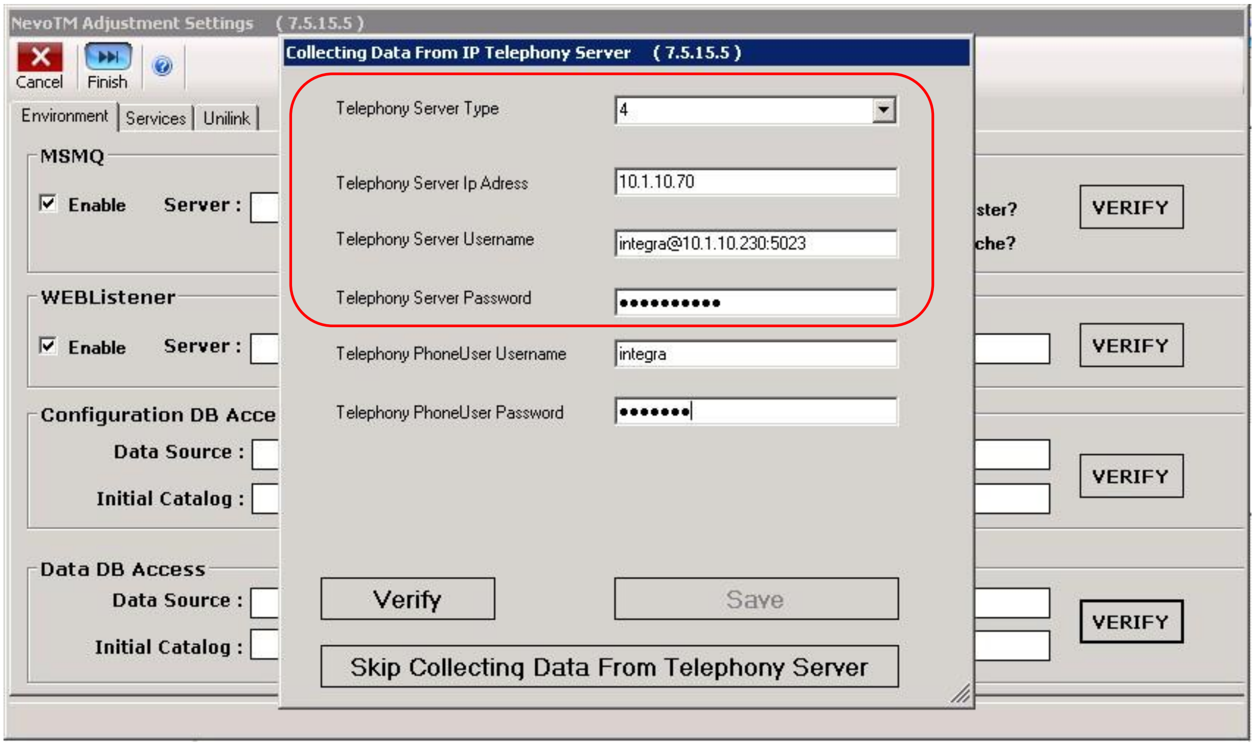
8.4. System Management Services (SMS)

SMS is provided by Avaya AES server for web access to manage objects on Communication Manager. The following shows the screenshot during installation of Integra Suite and the appropriate parameters are administered.

TelephonyServer_Type: **4** = Operations are processed using PMS Link and SMS (for ClearCallHistory and DND)

Telephony Server IP Address: < IP address of AES server>

Telephony Server Username/Password: This is an internal usage format for access to Communication Manager. It includes a combination of the login created in **Section 5.5.3**, Communication Manager ip and port address.



Collecting Data From IP Telephony Server (7.5.15.5)

Telephony Server Type: 4

Telephony Server Ip Adress: 10.1.10.70

Telephony Server Username: integra@10.1.10.230:5023

Telephony Server Password: ●●●●●●●●●●●

Telephony PhoneUser Username: integra

Telephony PhoneUser Password: ●●●●●●●

9. Verification Steps

This section describes steps that may be used to verify the configuration.

To verify that the PMS data link between Communication Manager and Integra Suite is operational, enter **status pms-link** at the SAT and look for a status of **up** in the **Physical Link State** and **Protocol State** fields.

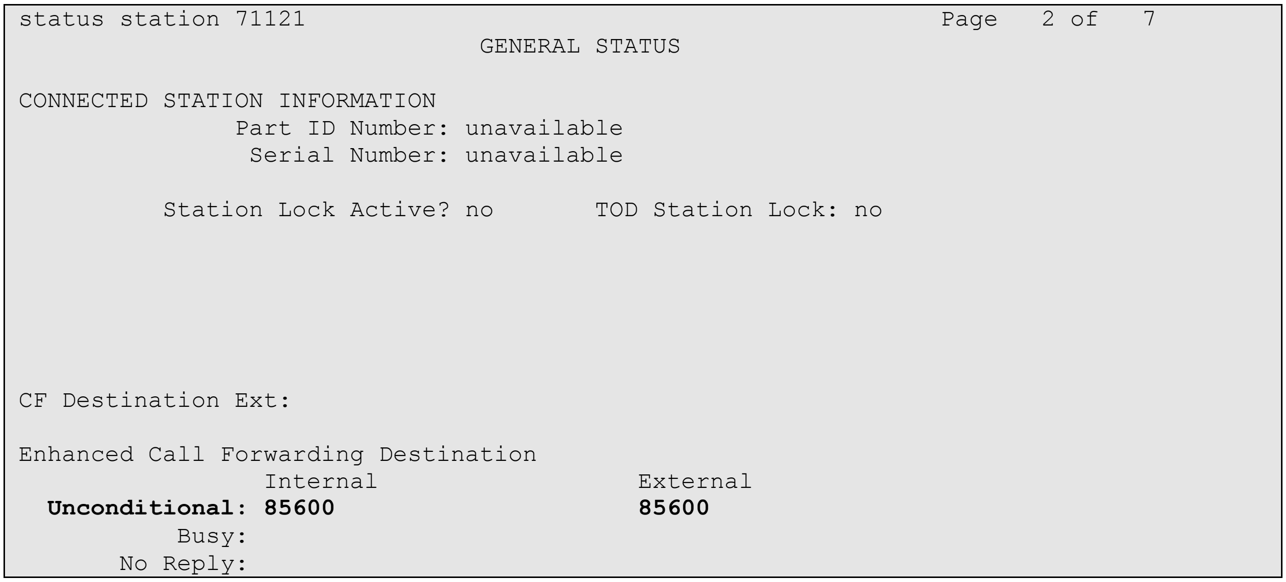
```
status pms-link
                            PMS LINK STATUS

        Physical Link State: up
             Protocol State: up

           Maintenance Busy? no
         Data Base Swapping? yes
```

To verify that the CDR data link between Communication Manager and Integra Suite is operational, enter **status cdr-link** at the SAT and look for a status of **up** in the **Link State** field of the CDR link to Integra Suite (in this example, the **Primary** link).

```
status cdr-link
                                CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2012/11/15 03:19:28            0000/00/00 00:00:00
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK
```

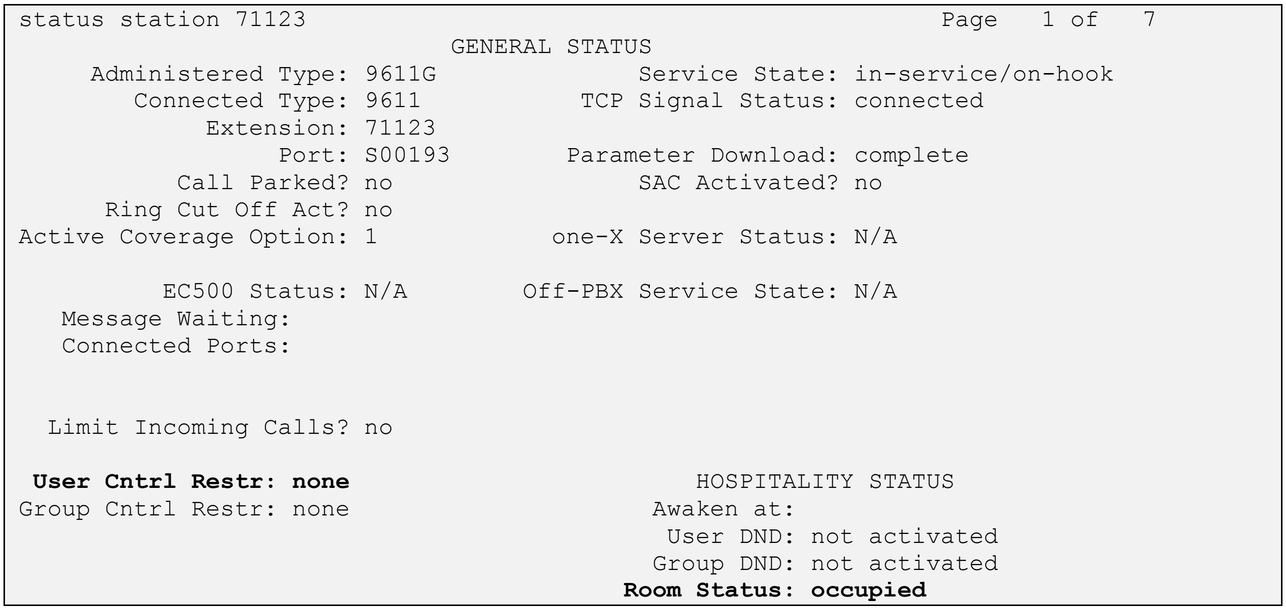
To verify that the Voice Mail functions, call any guest rooms that are Check-In and leave a voice mail message. Check that the message waiting light is turned on. Dial the Voice Mail retrieval number and retrieve the message and check that the message waiting light is off.

To verify SMS, initiate DND from the associated Property Management System. At Communication Manager SAT, enter **status station *x*** and verify that **CF Destination Ext** for **Unconditional** is set to Voice Mail number for both Internal and External Calls. All calls to the guest room will be routed to Voice Mail service for a Check-In guest.



```
status station 71121                                            Page   2 of   7
                                GENERAL STATUS

CONNECTED STATION INFORMATION
               Part ID Number: unavailable
                Serial Number: unavailable

          Station Lock Active? no       TOD Station Lock: no






CF Destination Ext:

Enhanced Call Forwarding Destination
                 Internal                  External
  Unconditional: 85600                     85600
           Busy:
       No Reply:
```

To verify the ability to check in guest extension *x*, initiate such a request from the associated Property Management System. At Communication Manager SAT, enter **status station *x*** and verify that **Room Status** is **occupied** and **User Cntrl Restr** is **none**.



```
status station 71123                                            Page   1 of   7
                              GENERAL STATUS
     Administered Type: 9611G              Service State: in-service/on-hook
        Connected Type: 9611           TCP Signal Status: connected
             Extension: 71123
                  Port: S00193        Parameter Download: complete
           Call Parked? no                 SAC Activated? no
      Ring Cut Off Act? no
Active Coverage Option: 1            one-X Server Status: N/A

          EC500 Status: N/A        Off-PBX Service State: N/A
   Message Waiting:
   Connected Ports:


  Limit Incoming Calls? no

 User Cntrl Restr: none                        HOSPITALITY STATUS
Group Cntrl Restr: none                     Awaken at:
                                             User DND: not activated
                                            Group DND: not activated
                                          Room Status: occupied
```

10. Conclusion

These Application Notes describe the procedures for configuring Integra Suite to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All interoperability compliance test cases executed against such a configuration were completed successfully with observations noted in **Section 2.2**.

11. Additional References

The following documents are available at http://support.avaya.com.

[1] *Administering Network Connectivity on Avaya Aura® Communication Manager*, Feb 2012, Document ID 555-233-504 Issue 16.0

[2] *Administering Avaya Aura® Communication Manager Release 6.2*, Feb 2012, Document ID 03-300509 Issue 7.0

[3] Application Enablement Services Web Services Programmer's Guide Release 6.1, Feb 2011, Document ID 02-300362 Issue 1

[4] *Avaya Aura™ Enablement Services Administration and Maintenance Guide*, Jul 2012, Release 6.2

[5] *Administering Avaya Aura™ Session Manager Release 6.2*, Jul 2012, Document ID 03-603324 Release 6.2

The following documents are provided by Convera Systems FZ-LLC.

[6] *Integra Installation Guide V1.0*, 26 June 2012

[7] *Integra Administration Guide V1.0 draft*, 29 May 2012

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 Developer*Connection* Program at devconnect@avaya.com.