Avaya Solution & Interoperability Test Lab

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

Abstract

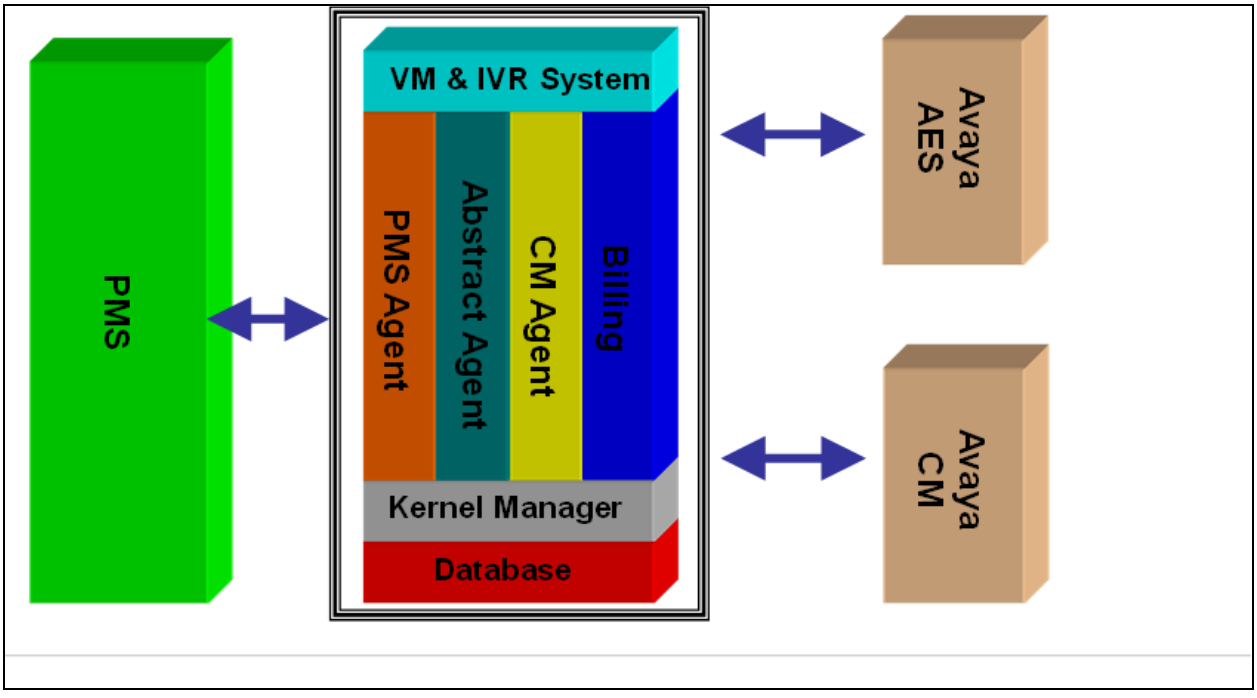
These Application Notes describe the procedures for configuring the Convera Integra Suite to interoperate with Avaya Aura® Communication Manager. Convera Integra Suite interface between Avaya Aura® Communication Manager and a hotel's 3rd party Property Management Systems (PMS). This product family is 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. 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. 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, 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 directly to the Communication Manager via TCP.

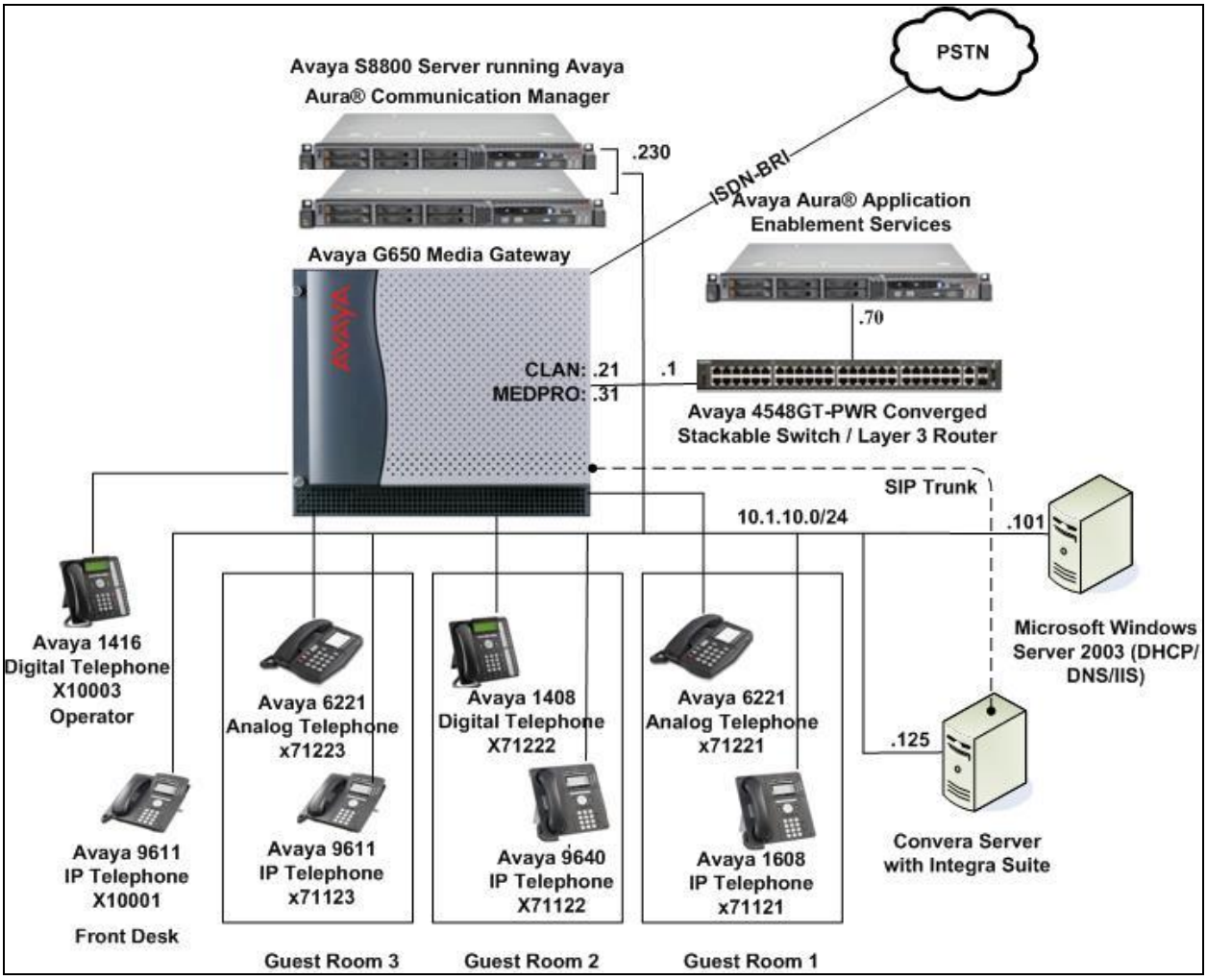


Figure 1: Sample Test Configuration

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 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**).

```
change node-names ip                                            Page   1 of   2
                                 IP NODE NAMES
    Name                 IP Address
ESS                   10.1.10.239
Gateway001            10.1.10.1
IPOffice              10.1.30.10
PC2                   10.1.10.152
aes1                  10.1.10.71
cms1                  10.1.10.85
default               0.0.0.0
integra               10.1.10.125
```

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.

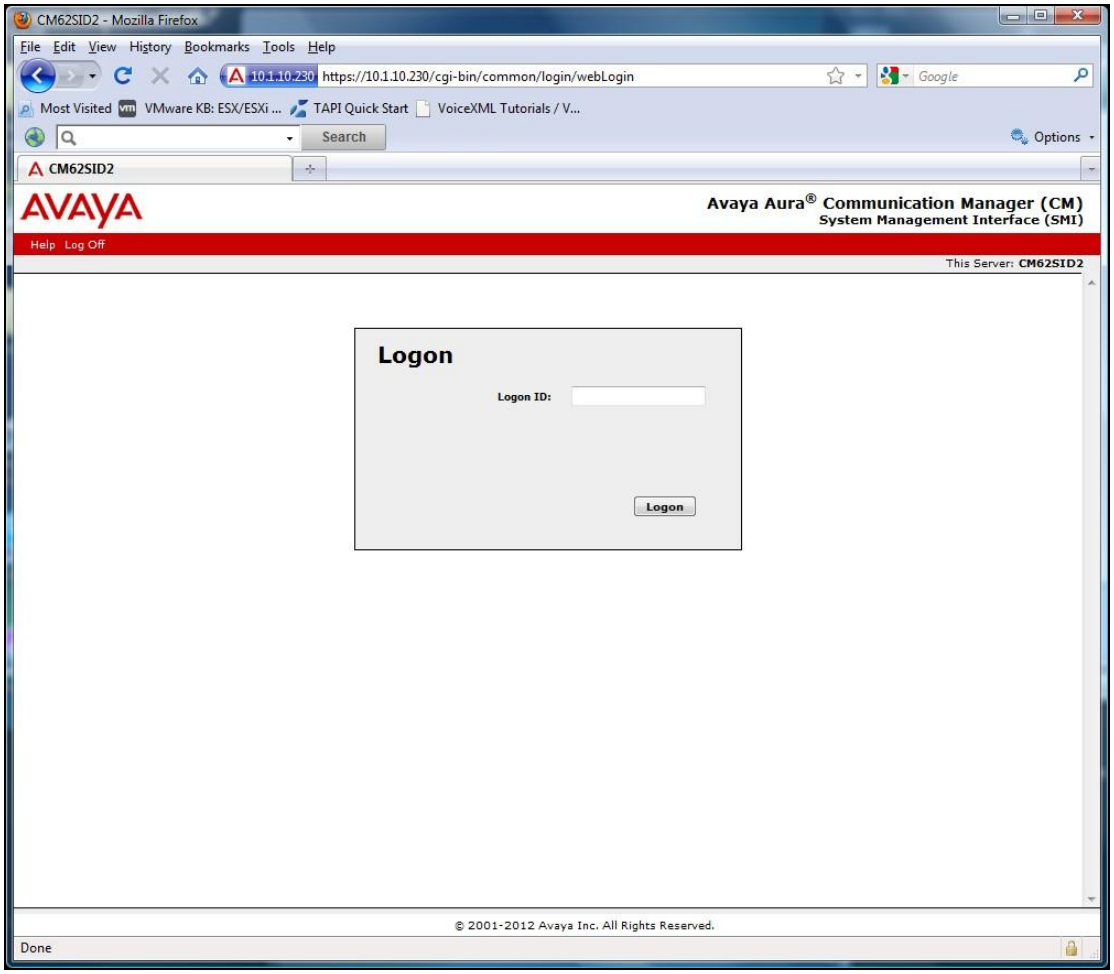
```
add user-profile 20                                          Page   1 of  41
                              USER PROFILE 20

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.

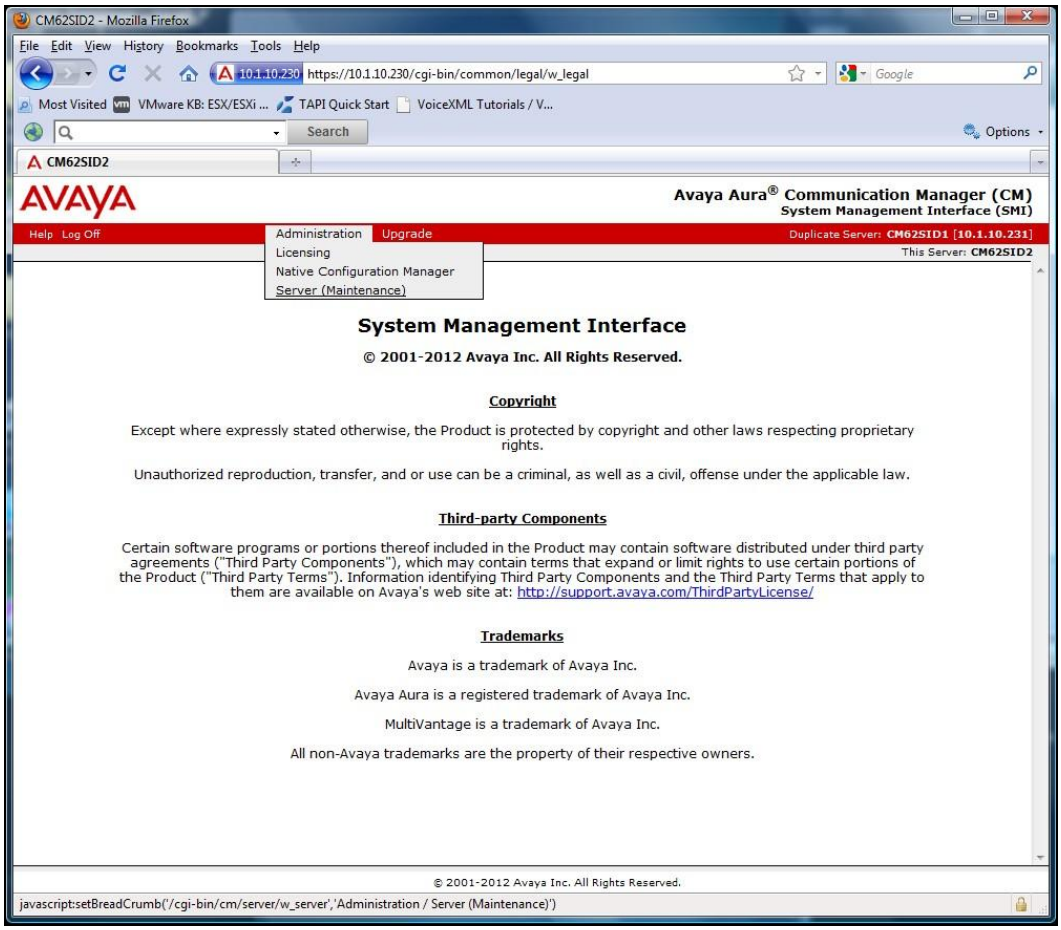
```
add user-profile 20                                          Page   2 of  41
                              USER PROFILE 20
 Set Permissions For Category:    To:          Set All Permissions To: wm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          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

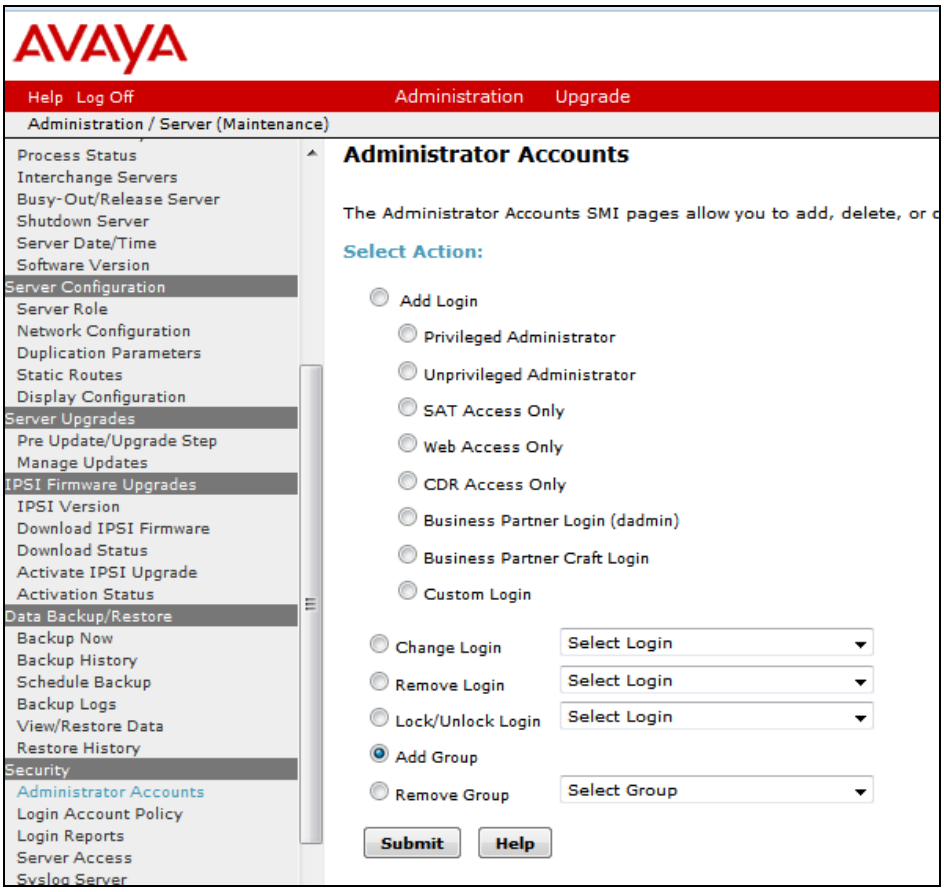
Using a web browser, enter https://<IP address of Communication Manager> to connect to the Avaya Server being configured and log in using appropriate credentials.



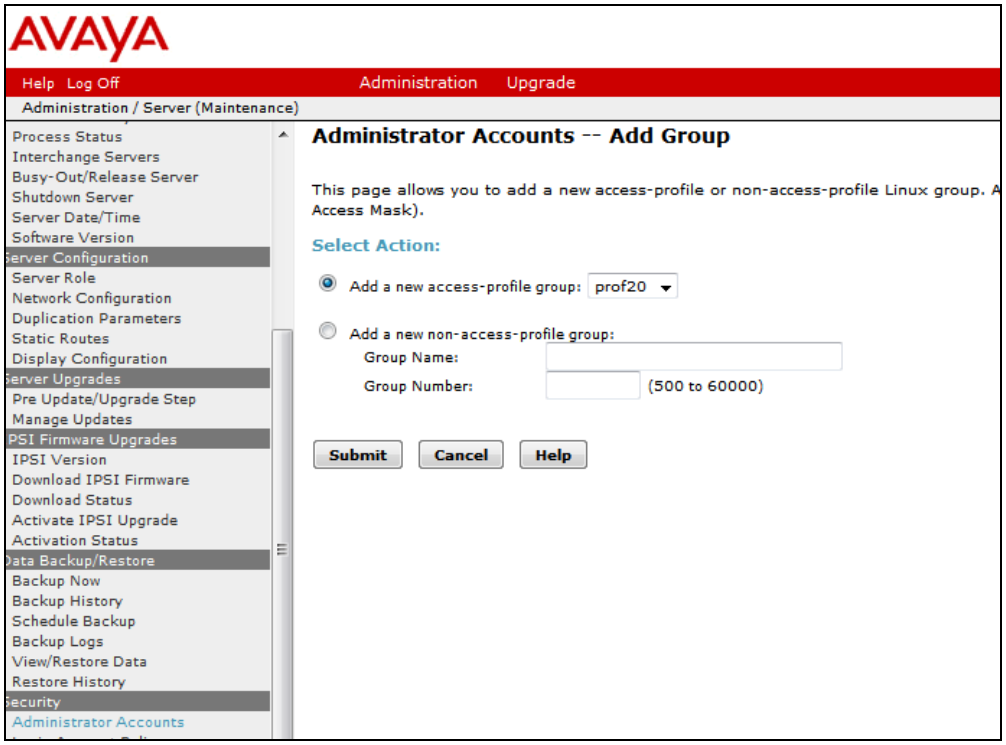
Click **Administration → Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.



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

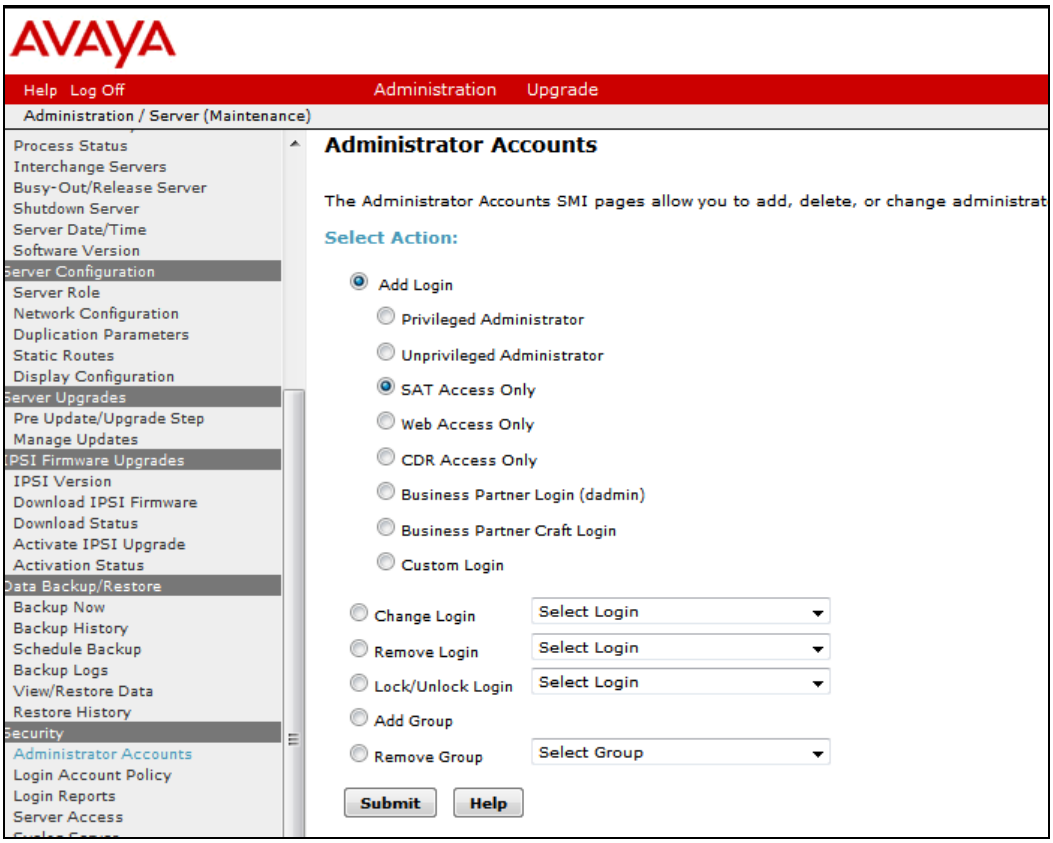


Select **Add a new access-profile group** and select **prof20** from the drop-down box to correspond to the user-profile created in **Section 5.5.1**. Click **Submit**. This completes the creation of the login group.



5.5.3. Configure Login

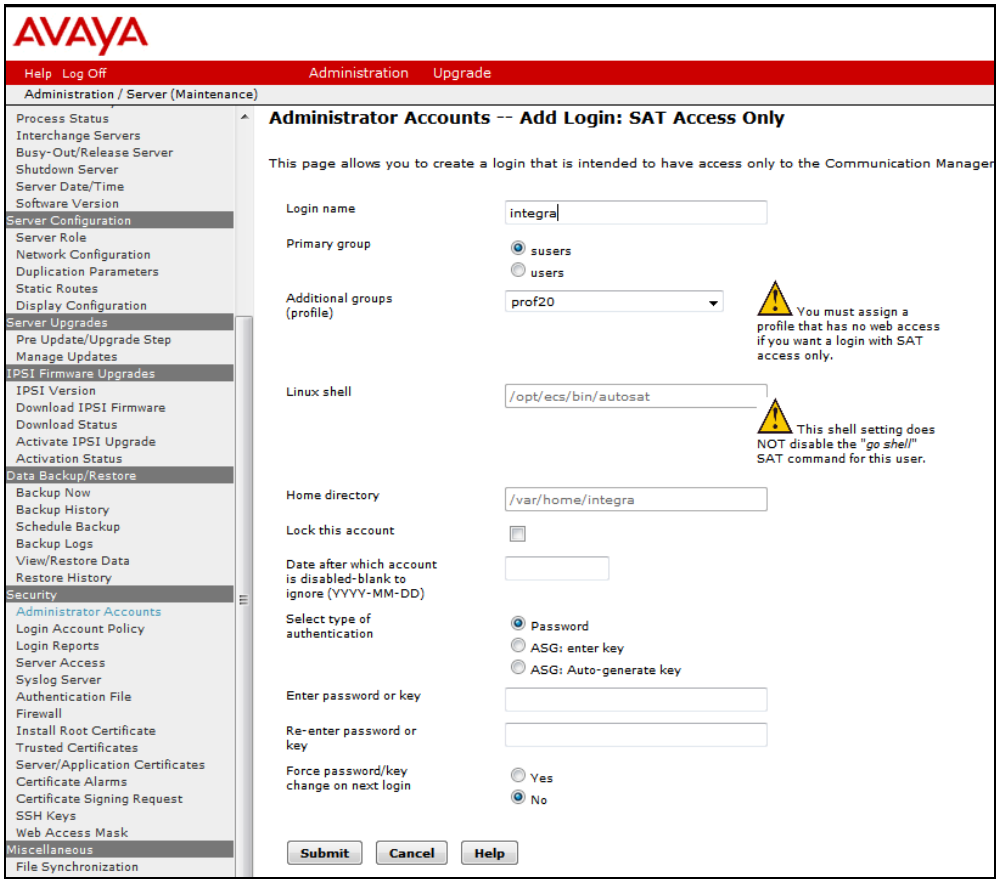
From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.



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.



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 1** and check that the supported **G711Mu** audio codec is administered for the local IP Network Region 1.

```
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.711MU           n         2        20
 2: G.711A            n         2        20
 3: G.729             n         2        20
 4: G.729B            n         2        20
 5:
 6:
 7:
```

Enter **change ip-network-region 1** to check that the **Codec Set** is set to **1** above.

```
change ip-network-region 1                                     Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sglab.com
    Name: Local
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: 3999
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 **55**). Enter the following parameter:

- **Group Type :** Enter **sip**
- **Transport Method :** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Near-end Listen Port:** Enter **5060**
- **Far-end Node Name:** Enter **integra**
- **Far-end Listen Port:** Enter **5060**
- **Far-end Network Region:** Enter **1** (local network)
- **Far-end Domain:** In this case **sglab.com**

```
add signaling-group 55                                          Page   1 of   2
                              SIGNALING GROUP

 Group Number: 55             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                Far-end Node Name: integra
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1

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? n
Session Establishment Timer(min): 3                   IP Audio Hairpinning? y
        Enable Layer 3 Test? 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 **55**). Enter the following parameter:

- **Group Name :** Enter appropriate name
- **Group Type :** Enter **sip**
- **Service Type :** Enter **tie**
- **Signaling Group:** Enter **55**
- **Number of Members:** Enter appropriate value
- **Numbering Format:** Enter **public**
- **Telephone Event Payload Type:** Enter **101**

```
add trunk-group 55                                          Page   1 of  21
                             TRUNK GROUP

Group Number: 55                   Group Type: sip           CDR Reports: y
  Group Name: Voice Mail                  COR: 1        TN: 1        TAC: #55
   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: 55
                                                   Number of Members: 30
```

```
add trunk-group 55                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y



                   Numbering Format: public
                                          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 55                                              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. Public Numbering

Enter **change public-numbering 7** to set guest rooms number as public numbering format since digit 7 is the starting digit of the guest room numbers. Set the values for **Ext Code** 7 as in the row below.

```
change public-unknown-numbering 7                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN            CPN
Len Code          Grp(s)    Prefix         Len
                                                 Total Administered: 12
 5  1             10                       5        Maximum Entries: 9999
 5  1             20        611            8
 5  1             30        310            8     Note: If an entry applies to
 5  1             31                       5     a SIP connection to Avaya
 5  1             55                       5     Aura(R) Session Manager,
 5  1             70                       5     the resulting number must
 5  1             90        190            8     be a complete E.164 number.
 5  1             99                       5
 5  7             7                        5
 5  10012         1         68731233       8
 5  10099         1         68731267       8
 5  10099         30        61010099       8
```

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.

```
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    5         pubu         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 5** and enter the trunk group number under the column **Grp No** as 55 created in **Section 5.9.3.**

```
change route-pattern 5                                          Page   1 of   3
                     Pattern Number: 5   Pattern Name: Voice Mail
                                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: 55   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                                     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
```

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:
08:                        23:                         38:
09:                        24:                         39:
10:                        25:                         40:
11:                        26:                         41:
12:                        27:                         42:
13:                        28:                         43:
14:                        29:                         44:
15:                        30:                         45:
```

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

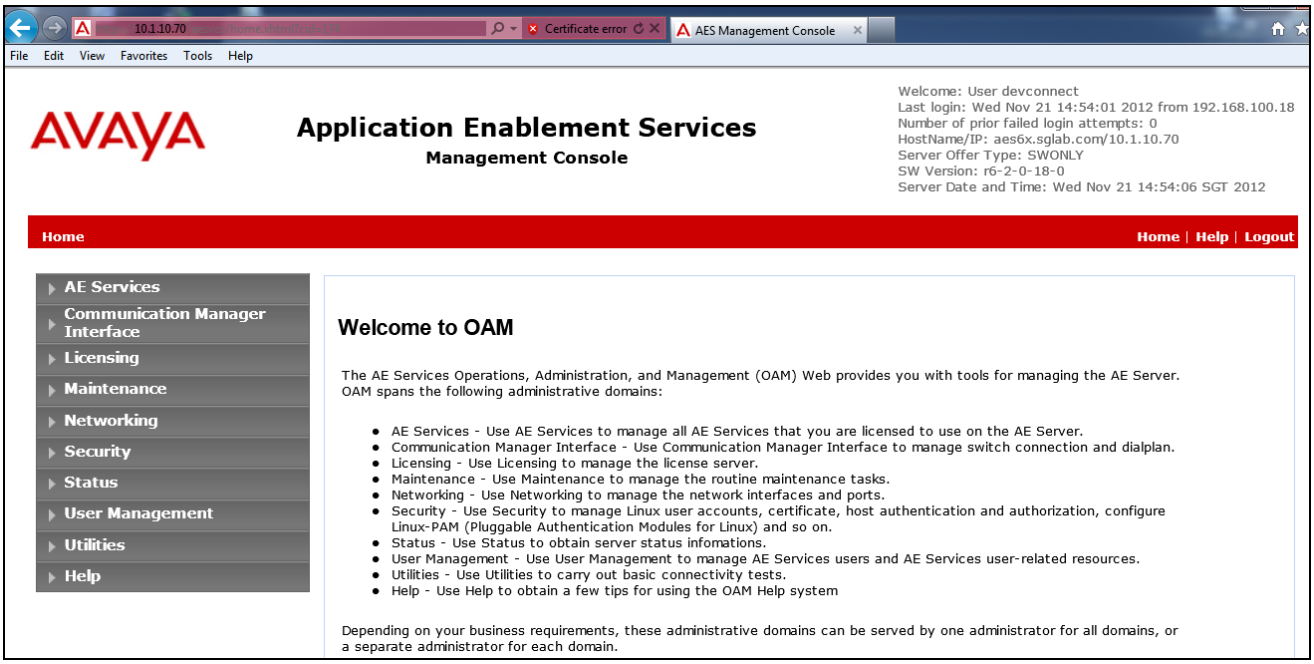
For each guest telephone extension ***x***, enter **change station *x*** and enter in the **COR** and **COS** fields the values corresponding to the Class of Service and Class of Restriction administered in **Section 5.7 and 5.8**, respectively.

```
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
```

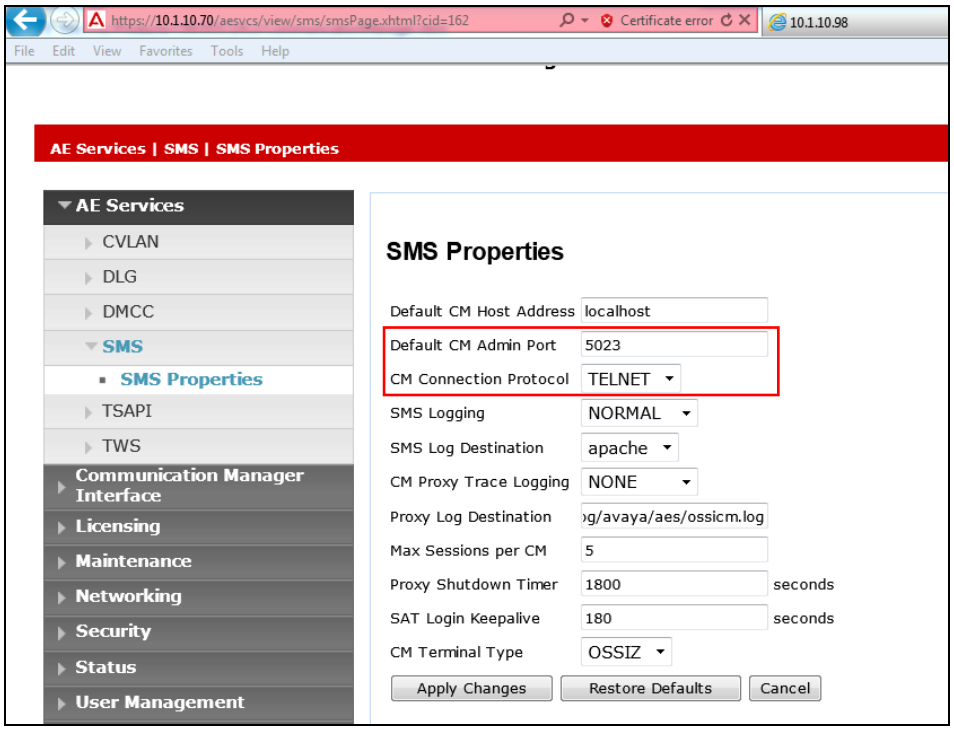
6. Configure Avaya Aura® Application Enablement Services Server

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.



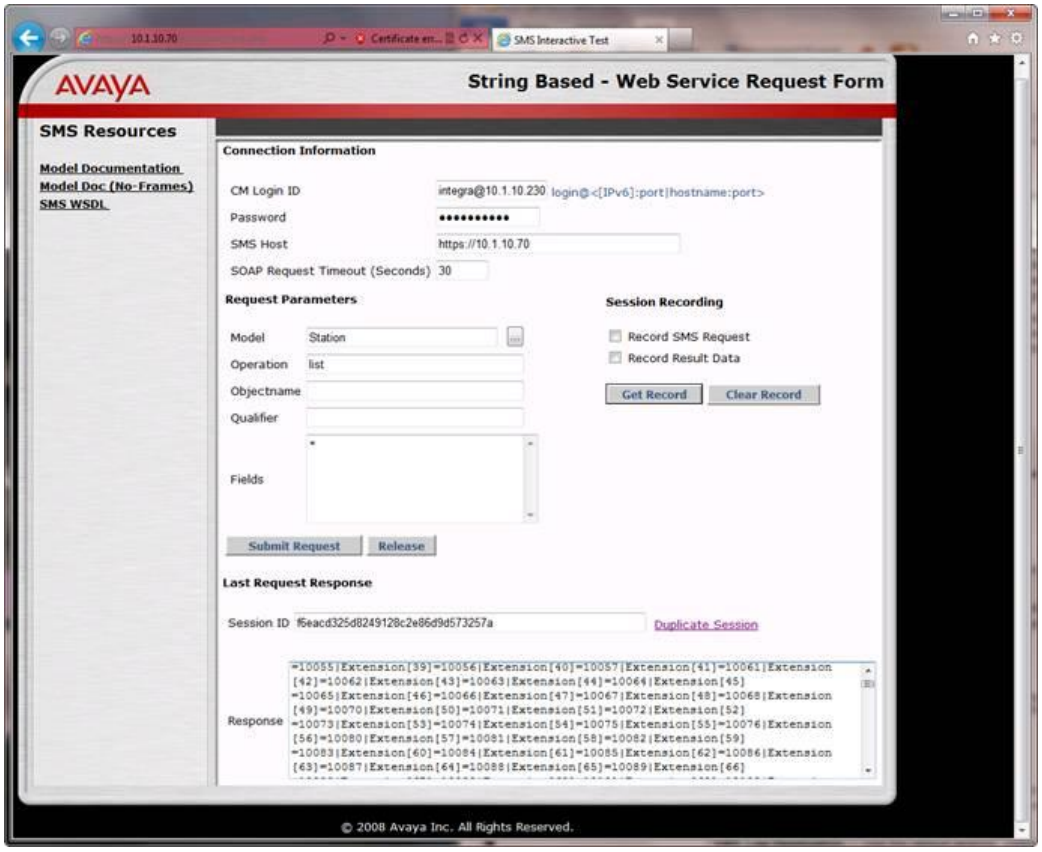
Click **AE Services**, then **SMS → SMS Properties** in the left pane. Note the **Default CM Admin Port** and **CM Connection Protocol** for the Avaya AES SMS setup which will be used to verify the SMS functionality on the next page.



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.

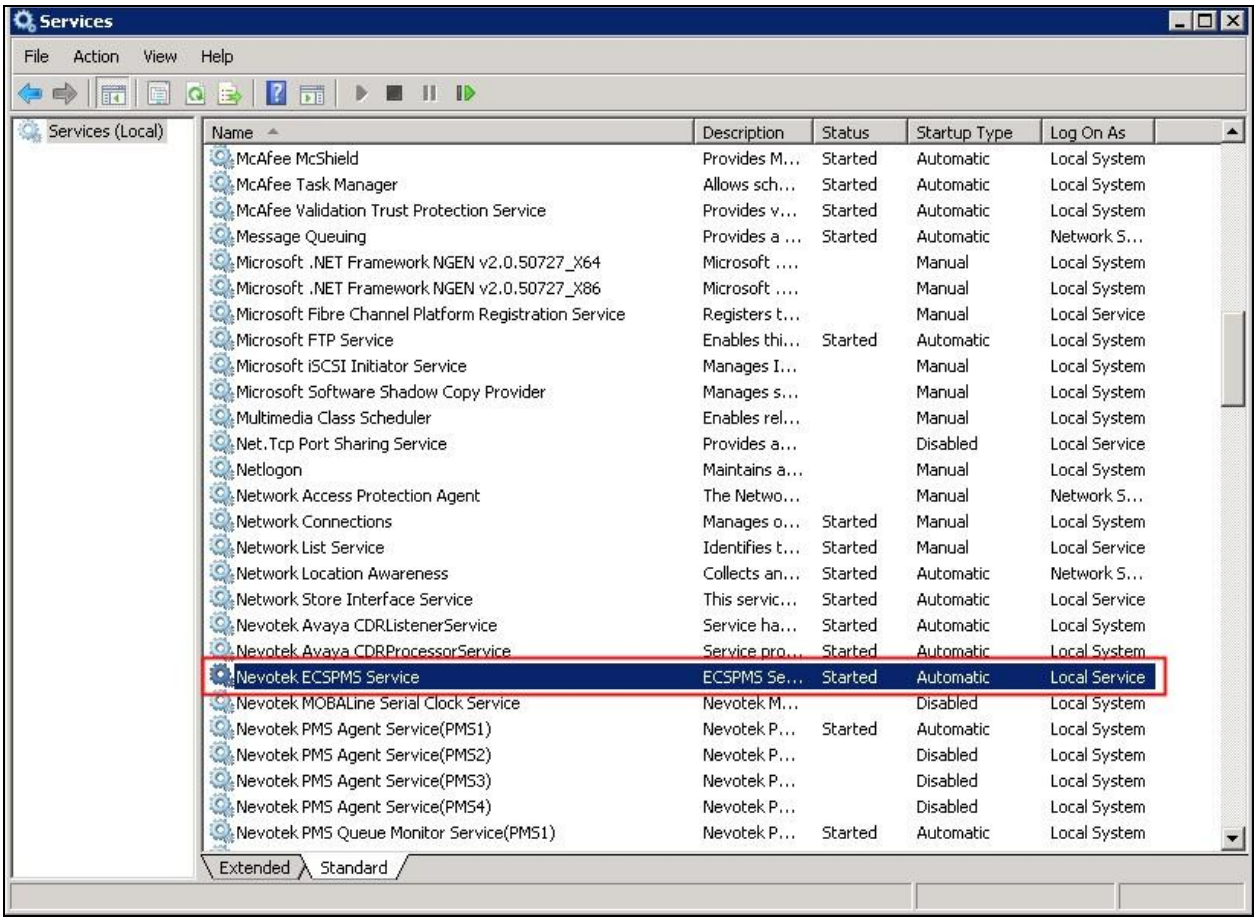


7. Configure Integra Suite

This section details the essential portion of the Integra Suite configuration to interoperate with 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 **[5]**.

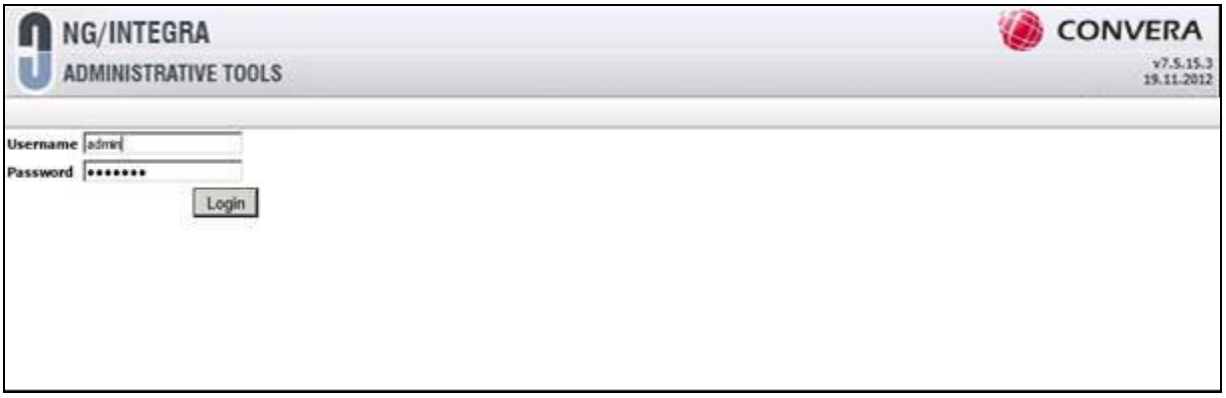
7.1. PMS interface

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.

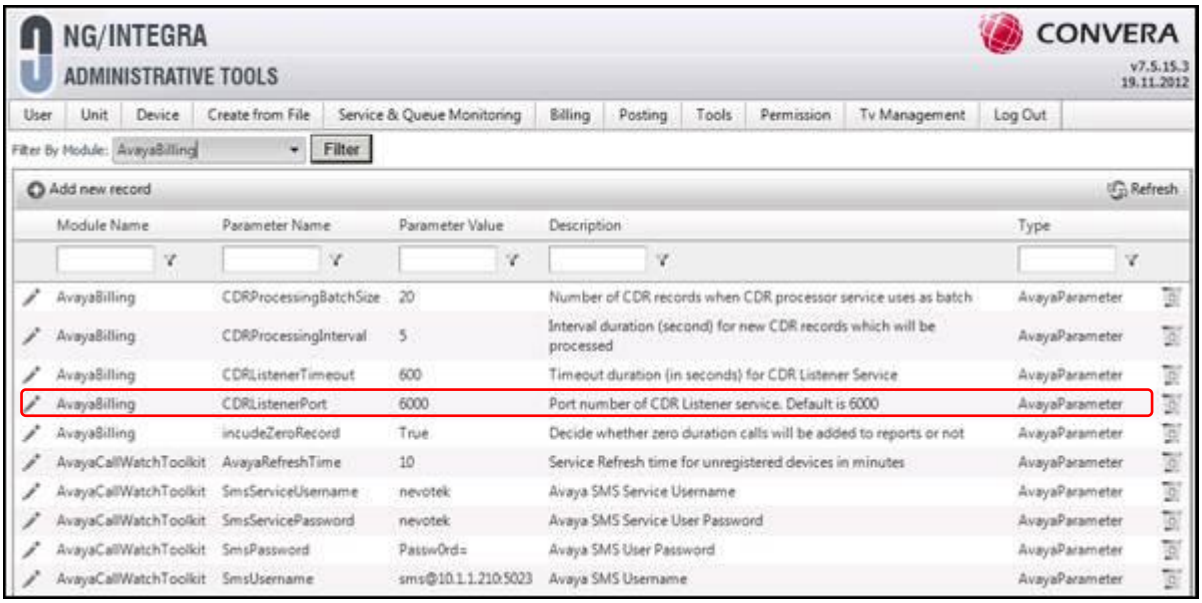


7.2. CDR Interface

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

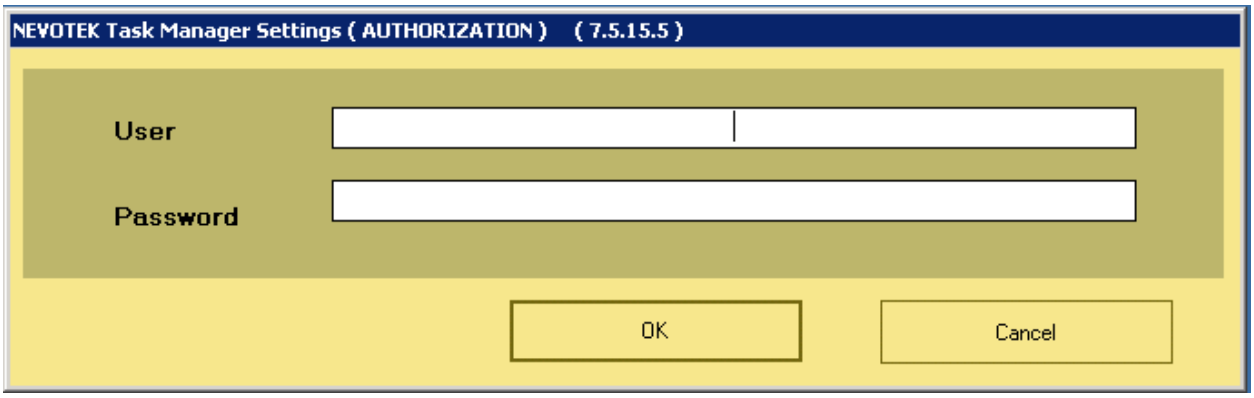


The Integra CDR listening port is configured as **6000** in **Section 5.4.** The parameter can be verified from the Administrative Tools. Navigate to "**Tools → Parameter Maintenance**" and select from the drop down menu for **AvayaBilling.** The "**CDRListenerPort**" under the **Parameter Name** column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

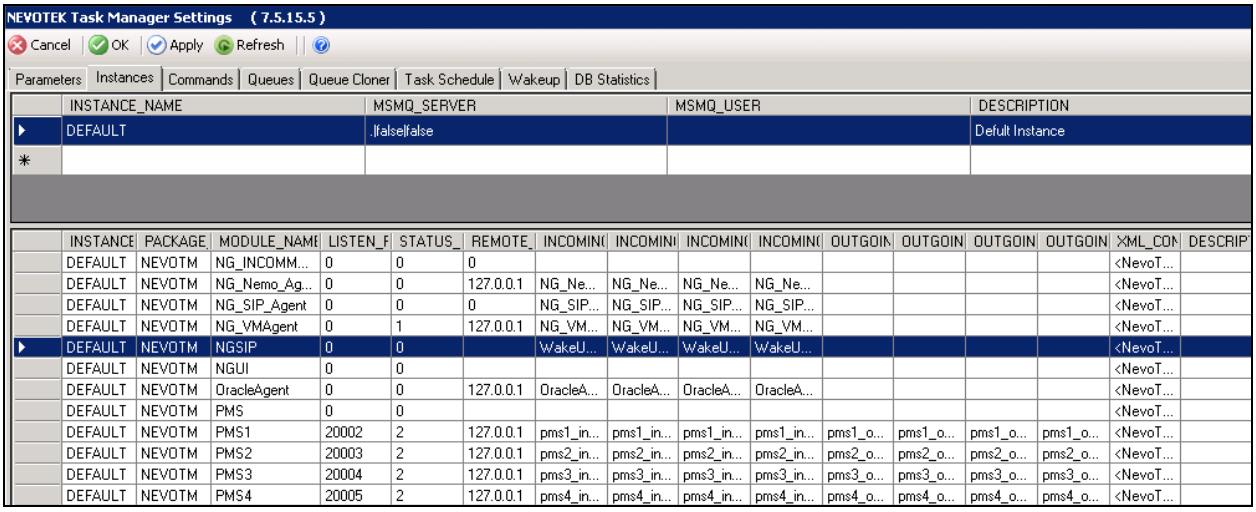


7.3. SIP Trunking

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 log in with the appropriate credentials.

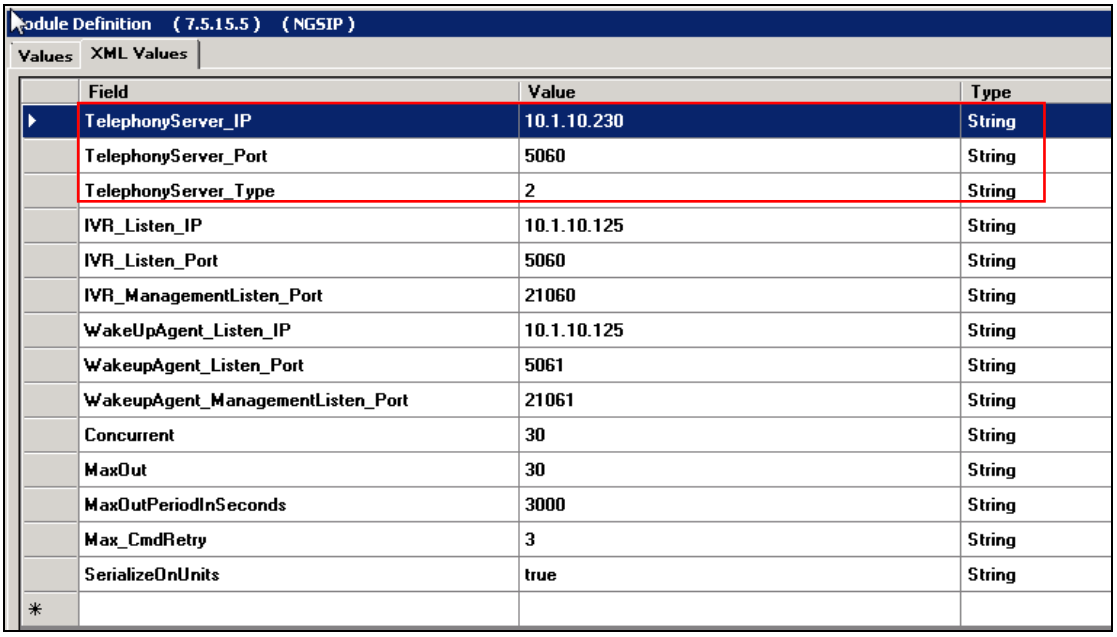


The following is the resulting screen after login. Click on the **Instances** tab and navigate to **NGSIP** under the **MODULE_NAME** column and click on the line.



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
*		

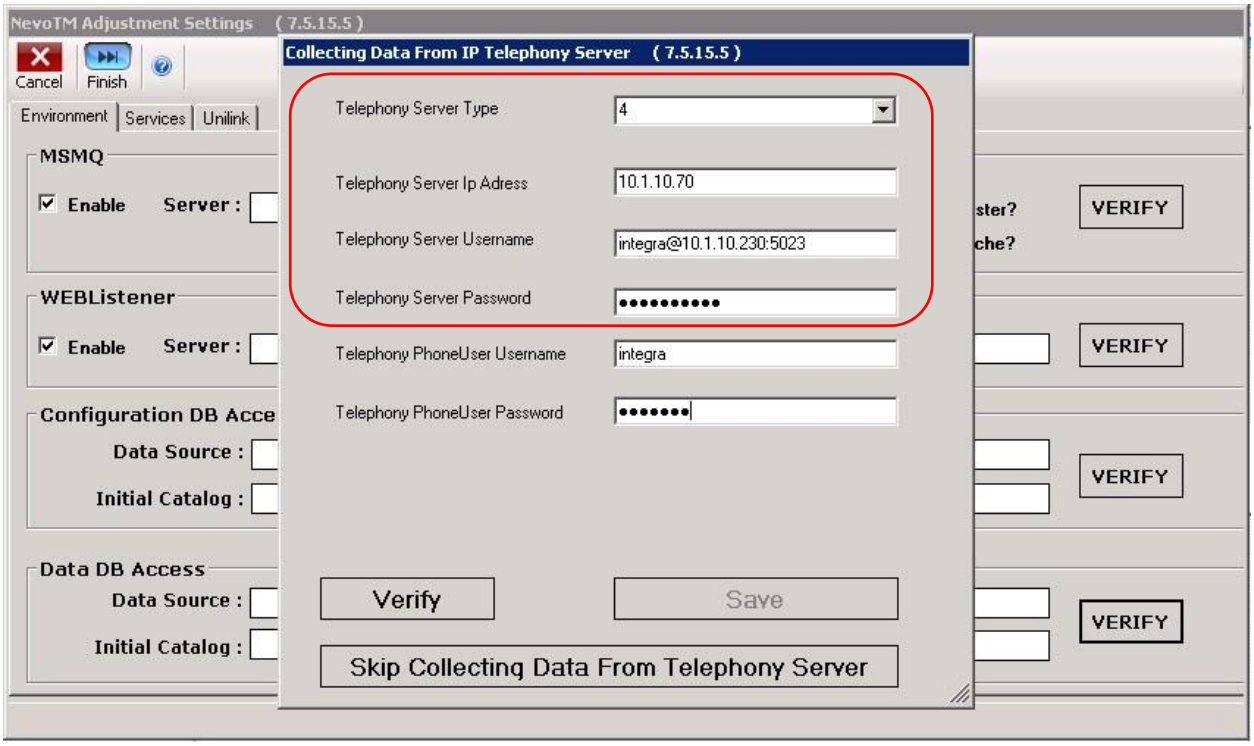
7.4. System Management Services (SMS)

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.



8. 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, activate DND for a guest room 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
```

9. Conclusion

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

10. 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

The following documents are provided from Convera Systems FZ-LLC.
[5] *Integra Installation Guide V1.0*, 26 June 2012
[6] *Integra Administration Guide V1.0 draft*, 29 May 2012

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.