Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Convergys Voice Portal with Avaya Aura® Communication Manager and Avaya Aura® Session Manager via a SIP Trunking Interface

- Issue 1.0

Abstract

These Application Notes describe the procedures required for Convergys Voice Portal to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using a SIP trunk.

Avaya SIP, H.323, and digital telephones were used to originate and terminate calls with User-to-User Information to and from the Convergys Voice Portal server. The overall objective of the interoperability compliance testing is to verify proper signaling and call establishment with the Convergys Voice Portal in an Avaya IP Telephony environment.

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 required for Convergys Voice Portal to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager (SM) using a SIP trunk. Avaya SIP, H.323, and digital telephones were used to originate and terminate calls with User-to-User Information (UUI) to and from the Convergys Voice Portal server. The overall objective of the interoperability compliance testing is to verify proper signaling and call establishment with the Convergys Voice Portal in an Avaya IP environment.

Convergys Voice Portal provides IVR and Messaging functionality via a SIP/VOIP telephony interface. Callers interact with the system via DTMF or Speech input, and may be transferred to agents, as needed.

These Application Notes assume that Communication Manager and Session Manager have already been installed and that basic configuration steps have been performed. Only steps relevant to the configuration used for compliance testing will be described in this document. For further details on configuration steps not covered in this document, consult references **[2]**, **[3]**, and **[5]**.

2. General Test Approach and Test Results

This section describes the testing used to verify the interoperability of Convergys Voice Portal with the Avaya SIP infrastructure (Communication Manager and Session Manager).

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

The interoperability compliance testing included feature and serviceability testing. Avaya SIP, H.323, and digital telephones were used to originate and terminate calls with User-to-User Information (UUI) to and from the Convergys Voice Portal server. The focus of the testing was primarily on verifying the SIP protocol messages between Session Manager and the Convergys Voice Portal server. Additionally, Convergys Voice Portal operations such as routing, DTMF tones, and transfers were tested. The serviceability testing included Communication Manager, Session Manager, and Convergys Voice Portal failure scenarios to verify that Convergys Voice Portal could properly recover from each failure.

2.2. Test Results

Convergys Voice Portal successfully passed compliance testing.

2.3. Support

Technical support for the Convergys Voice Portal can be obtained through the following:

- **Phone:** 800-955-4688
- **Web:** http://realcare.intervoice.com

3. Reference Configuration

Figure 1 illustrates the configuration used during compliance testing as described in these Application Notes. The configuration comprises of a Session Manager (with its companion System Manager), an Avaya S8300D Server running Communication Manager in an Avaya G450 Media Gateway. The non-SIP phones are supported by Communication Manager running on the S8300D Server and the G450 Media Gateway. The SIP phones register with Session Manager. The Convergys Voice Portal system was built on one physical server using VMware. One virtual machine (VM) was built to run the Convergys Control Center administration and monitoring tool. Two other VMs are built for two separate Convergys Voice Portals (IVRs). This document focuses on the integration to one Convergys Voice Portal (IP address 10.64.21.153).

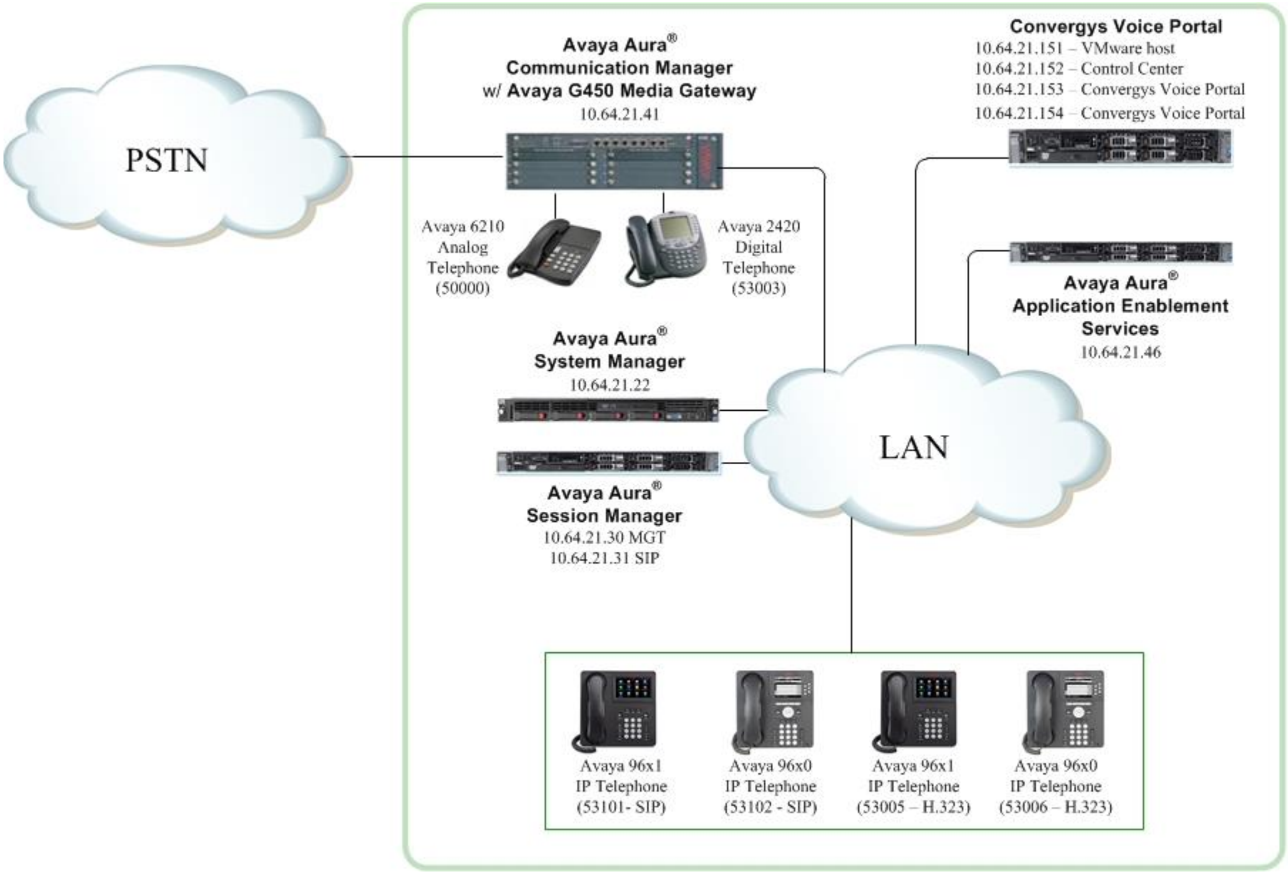


Figure 1: Convergys Voice Portal interoperating with Communication Manager and Session Manager

4. Equipment and Software Validated

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

Equipment/Software	**Release/Version**
Avaya S8300D Server with an Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.3 Patch 20850
HP Proliant DL360 G7	Avaya Aura® Session Manager 6.3 FP2
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager 6.3 SP2
Avaya 9600 Series IP Deskphones	
• 96x0 (H.323)	Avaya one-X® Deskphone Edition 3.1.5
• 96x0 (SIP)	Avaya one-X® Deskphone Edition 2.6.9
• 96x1 (H.323)	Avaya one-X® Deskphone Edition 6.2.2
• 96x1 (SIP)	Avaya one-X® Deskphone Edition 6.2.1
Avaya 6210 Analog Phone	-
Avaya 2420 Digital Phone	-
Convergys Voice Portal:	6.7.2:
• CTI Gateway	• 2.0.2

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration required to interoperate with the Session Manager. It focuses on the configuration of the SIP trunk connecting Communication Manager and Session Manager, with the following assumptions:

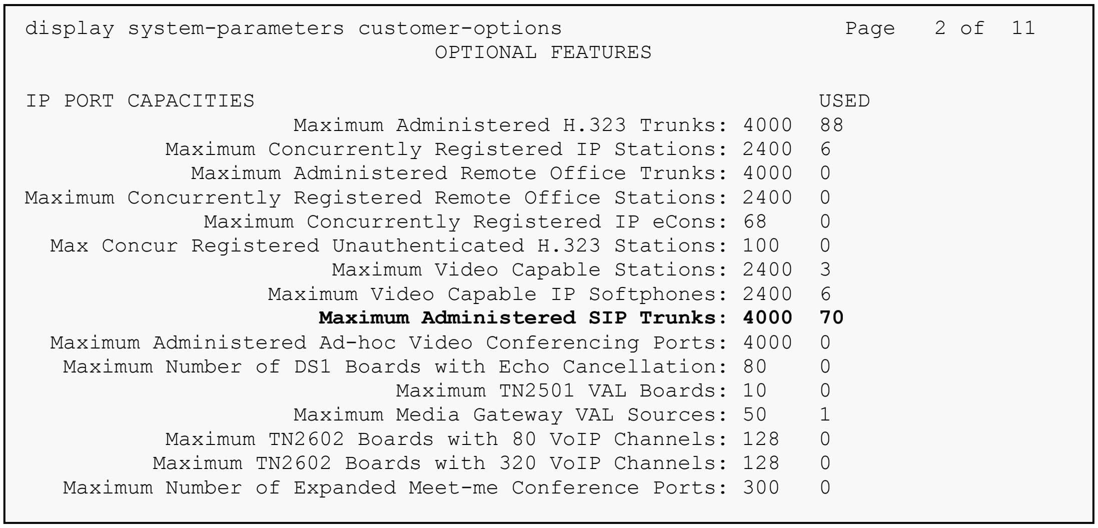
- Procedures necessary to support SIP and connectivity to Session Manager have been performed as described in references **[2]**, **[3]**, and **[5]**.
- All other components are assumed to be in place and previously configured, including the SIP and ISDN-PRI trunks that connect both sites.

The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager license (Step 1)
- Administer IP Node Names (Step 2)
- Administer IP network regions (Step 3)
- Administer IP codec set (Step 4)
- Administer SIP signaling group (Step 5)
- Administer SIP trunk group (Steps 6 – 7)
- Administer route pattern (Step 8)
- Administer AAR analysis for routing calls to Session Manager (Step 9)

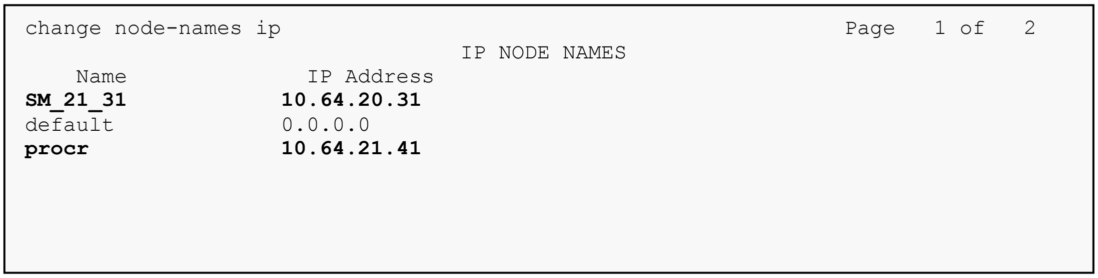
The configuration of the Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

Step	Description
1.	**Communication Manager License** Use the **display system-parameters customer-options** command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The license file installed on the system controls the maximum permitted. If there is an insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.



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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 4000  88
           Maximum Concurrently Registered IP Stations: 2400  6
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  3
                   Maximum Video Capable IP Softphones: 2400  6
                       Maximum Administered SIP Trunks: 4000  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

Step	Description
2.	**IP Node Names** Use the **change node-names ip** command to administer a **Name** and **IP Address** for Session Manager. In the configuration used for compliance testing, the ***procr*** and ***SM_21_31*** nodes were utilized to administer a SIP trunk between Communication Manager and Session Manager.



```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM_21_31            10.64.20.31
default             0.0.0.0
procr               10.64.21.41
```

Step	Description
3.	**IP Network Region – Region 1** This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. All IP endpoints were located in IP network region 1 using the parameters described below. Use the **change ip-network-region** command to view these settings. The example below shows the values used during compliance testing. ▪ The **Authoritative Domain** field was configured to match the domain name configured on Session Manager (see **Section 6**, **Step 2**). In this configuration, the domain name is ***avaya.com***. This name appears in the "From" header of SIP messages originating from this IP region. ▪ A descriptive name was entered for the **Name** field. ▪ **IP-IP Direct Audio** (Media Shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Media Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ The **Codec Set** field was set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set ***1***, configured in Step 4, was selected. ▪ The default values were used for all other fields.

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

Step	Description
4.	**Codecs** Use the **change ip-codec-set** command to verify that G.711MU is contained in the codec list. The example below shows the value used for compliance testing. Note, codecs G.711A and G.729A were also tested but not shown below.

```
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:
```

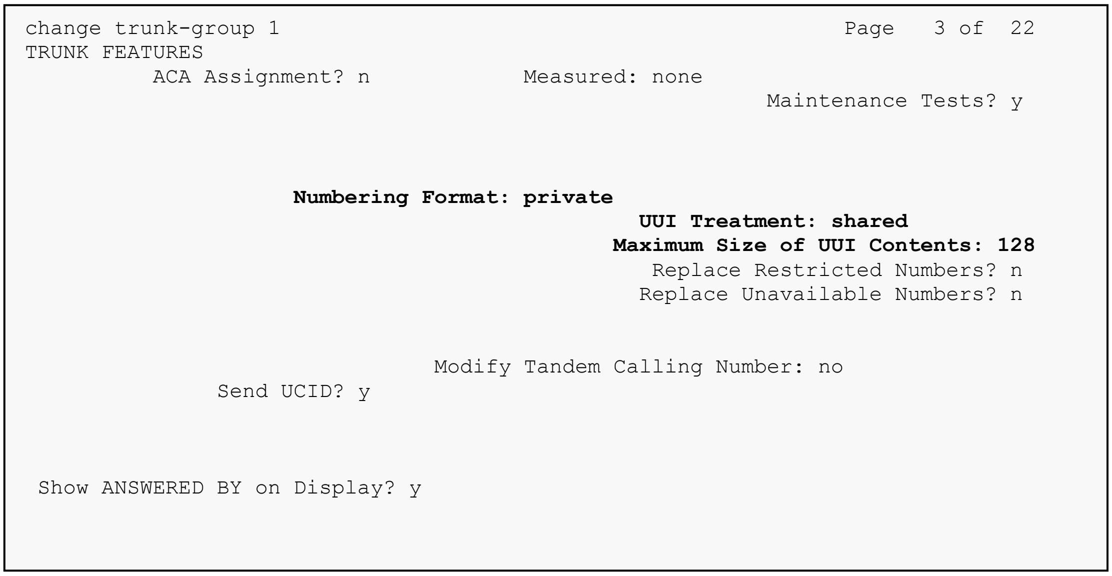
Step	Description
5.	**Signaling Group** For compliance testing, the signaling group shown below and the associated SIP trunk (administered in **Steps 6-7**) are used for routing calls to and from the Convergys Voice Portal server via Session Manager. Signaling group **1** was configured using the parameters highlighted below. All other fields were set as described in reference **[2]**. ▪ **Group Type** was set to ***sip***. ▪ **Transport Method** was set to ***tls***. As a result, **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061.*** ▪ **Peer Detection Enabled** was set to ***y***. ▪ **Near-end Node Name** was set to ***procr***. Node names are defined in **Step 2** above. ▪ **Far-end Node Name** was set to ***SM_21_41***. This node name maps to the IP address of the Session Manager as defined using the **change node-names ip** command. ▪ **Far-end Network Region** was set to ***1***. ▪ **Direct IP-IP Audio Connections** was set to ***y***. This field must be set to ***y*** to enable Media Shuffling on the trunk level (see **Step 3** on **IP-IP Direct Audio**).

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                  Far-end Node Name: SM_21_31
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain:
                                             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
```

Step	Description
6.	**Trunk Group** For compliance testing, trunk group **1** was used for the SIP trunk group for routing calls to and from the Convergys Voice Portal server via Session Manager. Trunk group **1** was configured using the parameters highlighted below. All other fields were set as described in reference **[2]**. On **Page 1**: ▪ **Group Type** field was set to ***sip***. ▪ A descriptive name was entered for the **Group Name**. ▪ An available trunk access code (TAC) that was consistent with the existing dial plan was entered in the **TAC** field. ▪ **Service Type** field was set to ***tie***. ▪ **Signaling Group** was set to the signaling group configured in the previous step. ▪ **Member Assignment method** was set to ***auto***. ▪ **Signaling Group** was set to ***1*** (see **Step 5**). ▪ The **Number of Members** field contained the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration.

```
change trunk-group 1                                            Page   1 of  22
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SM_21_31                    COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 1
                                                    Number of Members: 12
```

Step	Description
7.	**Trunk Group – continued** On **Page 3**: ▪ **Numbering Format** was set to ***private***. This field specifies the format of the calling party number sent to the far-end. ▪ **UUI Treatment** was set to ***shared***. ▪ **Maximum Size of UUI Contents** was set to ***128***. ▪ Default values may be used for all other fields.



```
change trunk-group 1                                            Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n



                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y
```

Step	Description
8.	**Route Pattern** Use the **change route-pattern** command to create a route pattern that will route calls to the SIP trunk that connects Communication Manager to Session Manager. The example below shows the route pattern used during compliance testing. A descriptive name was entered for the **Pattern Name** field. The **Grp No** field was set to the trunk group created in **Steps 6–7**. The Facility Restriction Level (**FRL**) field was set to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. **Numbering Format** was set to ***lev0-pvt***. The default values were used for all other fields.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: to SM_21_31
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
```

Step	Description
9.	**Routing Calls to Session Manager** Automatic Alternate Routing (AAR) was used to route calls to Convergys Voice Portal via Session Manager. Two places need to be changed to support this routing. First, use the **change dialplan analysis** command to create an entry in the dial plan. The example below shows entries previously created using the **display dialplan analysis** command. The 3rd entry specifies that numbers that begin with 7 are of **Call Type *aar***. Second, use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table. The example below shows entries previously created using the **display aar analysis 0** command. The entry specifies that numbers that begin with 7 and are 5 digits long use route pattern 1. Route pattern 1 routes calls to Session Manager.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 3

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           3   dac
   5           5   ext
   7           5   aar
   8           1   fac
   9           1   fac
   *           3   fac
```

```
display aar analysis 7                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd

    7                     5    5     1        aar          n
```

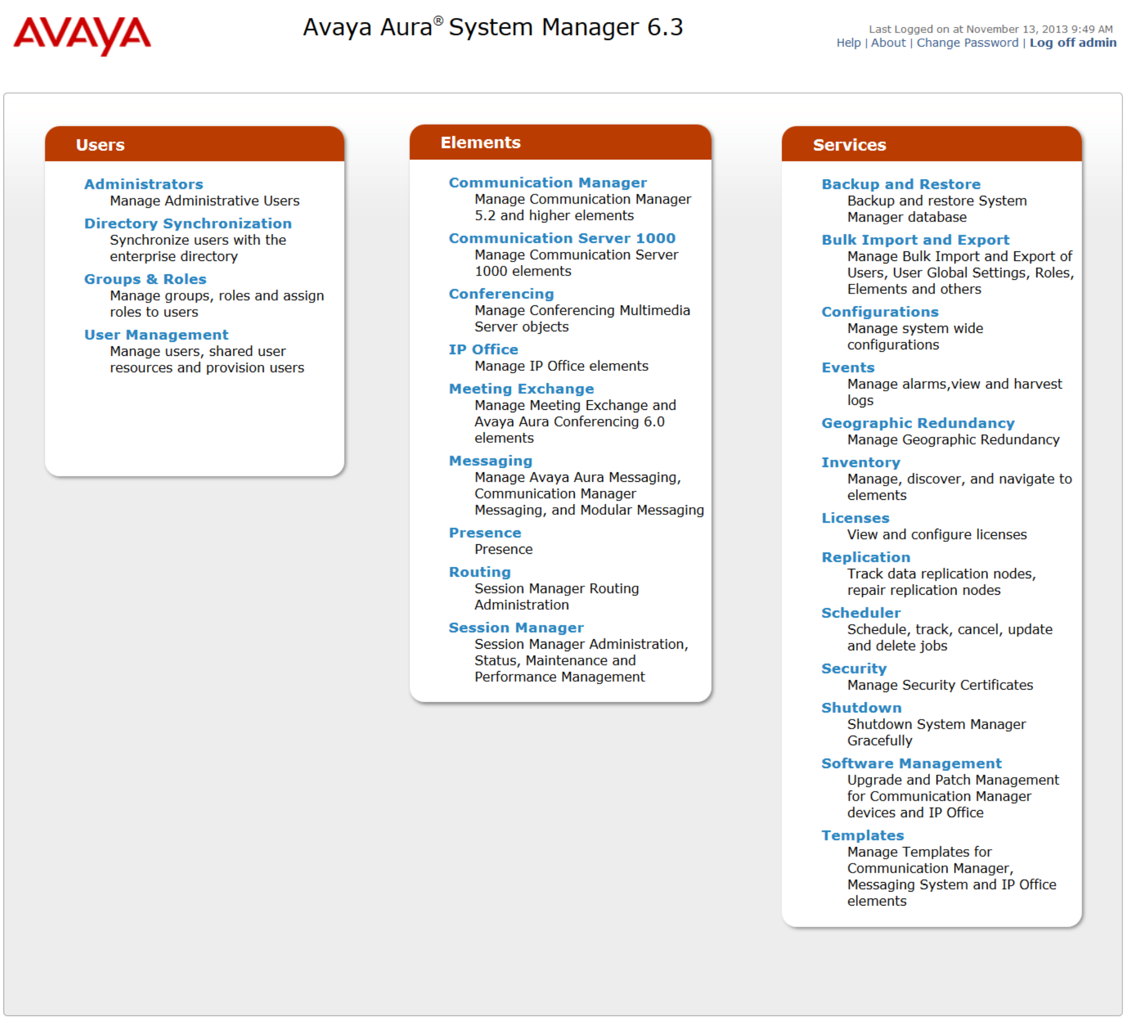
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager must be administered via System Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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

- **SIP domain**
- Logical/physical **Locations** where SIP Entities may reside
- **SIP Entities** corresponding to the SIP telephony systems including Communication Manager, the Convergys Voice Portal server, and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed
- Information corresponding to the **Session Manager** server to be managed by System Manager

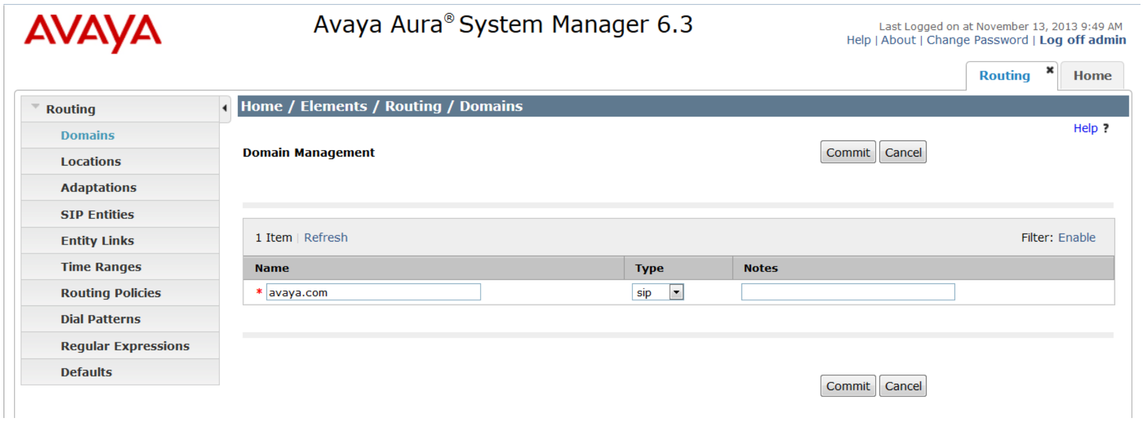
Step	Description
1.	**Log in** Access the administration web interface by entering the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials. The page below will be displayed.  Click the **Elements → Routing** link. The sub-menus displayed in the left column (see picture in **Step 2**) will be used to configure the items in **Steps 2-7**.

2. **Specify SIP Domain**

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

- **Name**: Enter the domain name specified to be the **Authoritative Domain** on the **IP Network Region** form on Communication Manager (see **Section 5, Step 3**)
- **Type**: Select ***sip***
- **Notes**: Descriptive text (optional)

Click **Commit**.



Domain Management

Name	Type	Notes
* avaya.com	sip	

3. **Add Locations**

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of routing and bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Fill in the following:

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

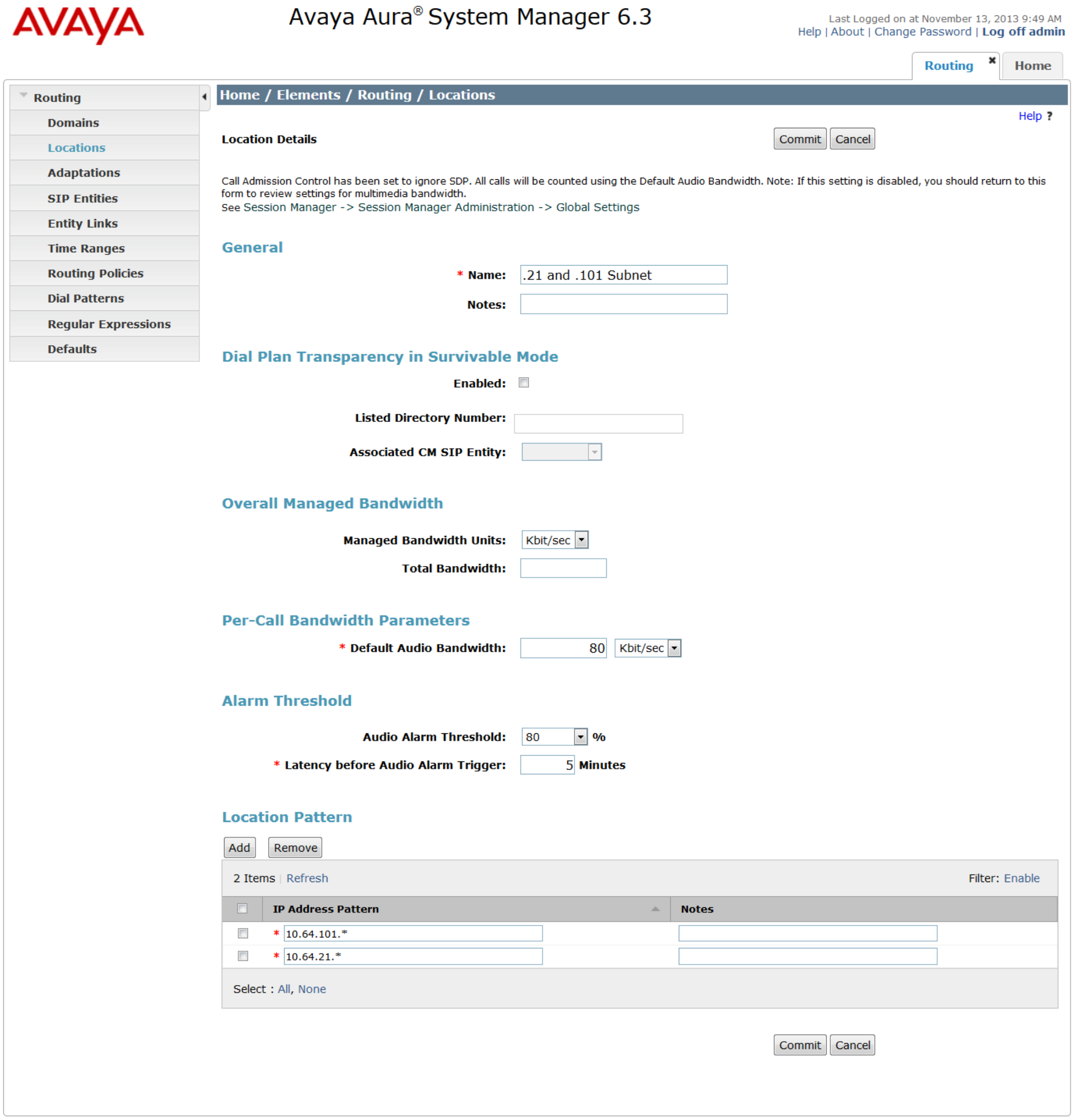
The remaining fields under *General* can be filled in to specify bandwidth management parameters between Session Manager and this location. The default values were used for compliance testing.

Next, fill in the following:

Under *Location Pattern*:
- **IP Address Pattern**: An IP address pattern used to logically identify the location
- **Notes**: Descriptive text (optional)

The screen below shows addition of the ".21 and .101 Subnet" Location which includes the Communication Manager, Session Manager, and the Convergys Voice Portal server.

Click **Commit** to save the Location definition.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
See Session Manager -> Session Manager Administration -> Global Settings

General

* Name: .21 and .101 Subnet
Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Audio Alarm Threshold: 80 %
* Latency before Audio Alarm Trigger: 5 Minutes

Location Pattern

☐	IP Address Pattern	Notes
☐	* 10.64.101.*	
☐	* 10.64.21.*	

4. **Add SIP Entities**

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the configuration used for compliance testing, a SIP Entity was added for the Session Manager itself, the processor Ethernet for the Avaya S8300D Media Server, and the Convergys Voice Portal server.

Select **SIP Entities** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

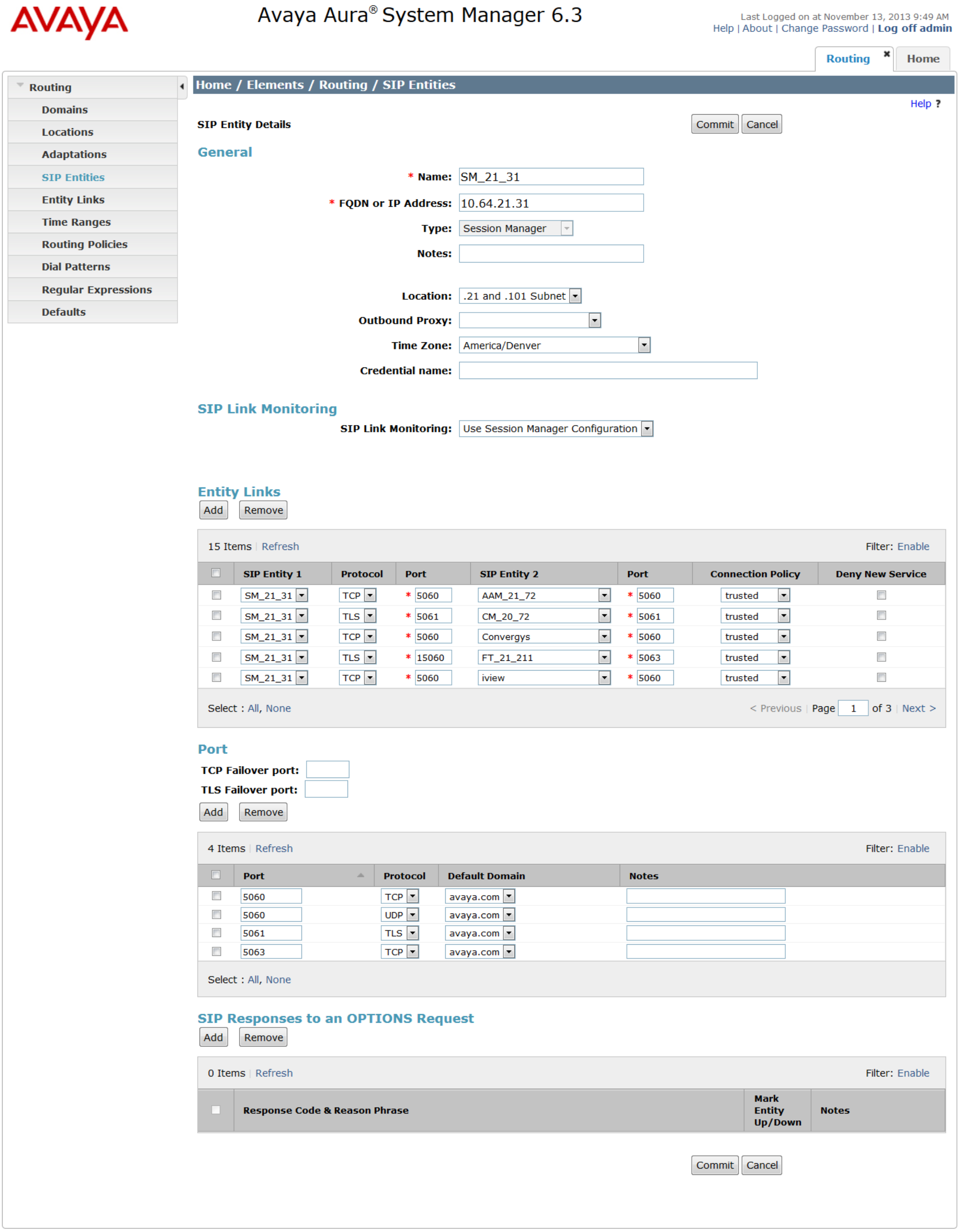
Name	A descriptive name
FQDN or IP Address:	FQDN or IP address of the signaling interface for the entity
Type:	"Session Manager" for Session Manager, "CM" for Communication Manager, or "SIP Trunk" for the Convergys Voice Portal server
Adaptation:	Leave blank
Location:	Select the appropriate Location configured in previous step
Time Zone:	Select the proper time zone for this installation

When adding a SIP Entity for Session Manager, Under *Port*, click **Add**, then edit the fields in the resulting new row as shown below:

Port:	Port number on which the system listens for SIP requests
Protocol:	Transport protocol to be used to send SIP requests
Default Domain:	Select the SIP Domain configured in **Step 2** of this section or "ALL"

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

	The following screen shows the addition of Session Manager. Two **Port** entries are added. TLS (well-known port 5061) is used for communication with Communication Manager. TCP (well-known port 5060) is used for communication with the Convergys Voice Portal server. Also note that the entries under *Entity Links* are populated automatically after the Entity Links are administered (**Step 5** below).



SIP Entity Details

General

- * **Name:** SM_21_31
- * **FQDN or IP Address:** 10.64.21.31
- **Type:** Session Manager
- **Notes:**
- **Location:** .21 and .101 Subnet
- **Outbound Proxy:**
- **Time Zone:** America/Denver
- **Credential name:**

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

15 Items | Refresh — Filter: Enable

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
☐	SM_21_31	TCP	* 5060	AAM_21_72	* 5060	trusted	☐
☐	SM_21_31	TLS	* 5061	CM_20_72	* 5061	trusted	☐
☐	SM_21_31	TCP	* 5060	Convergys	* 5060	trusted	☐
☐	SM_21_31	TLS	* 15060	FT_21_211	* 5063	trusted	☐
☐	SM_21_31	TCP	* 5060	iview	* 5060	trusted	☐

Select : All, None — < Previous | Page 1 of 3 | Next >

Port

- **TCP Failover port:**
- **TLS Failover port:**

4 Items | Refresh — Filter: Enable

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5060	UDP	avaya.com	
☐	5061	TLS	avaya.com	
☐	5063	TCP	avaya.com	

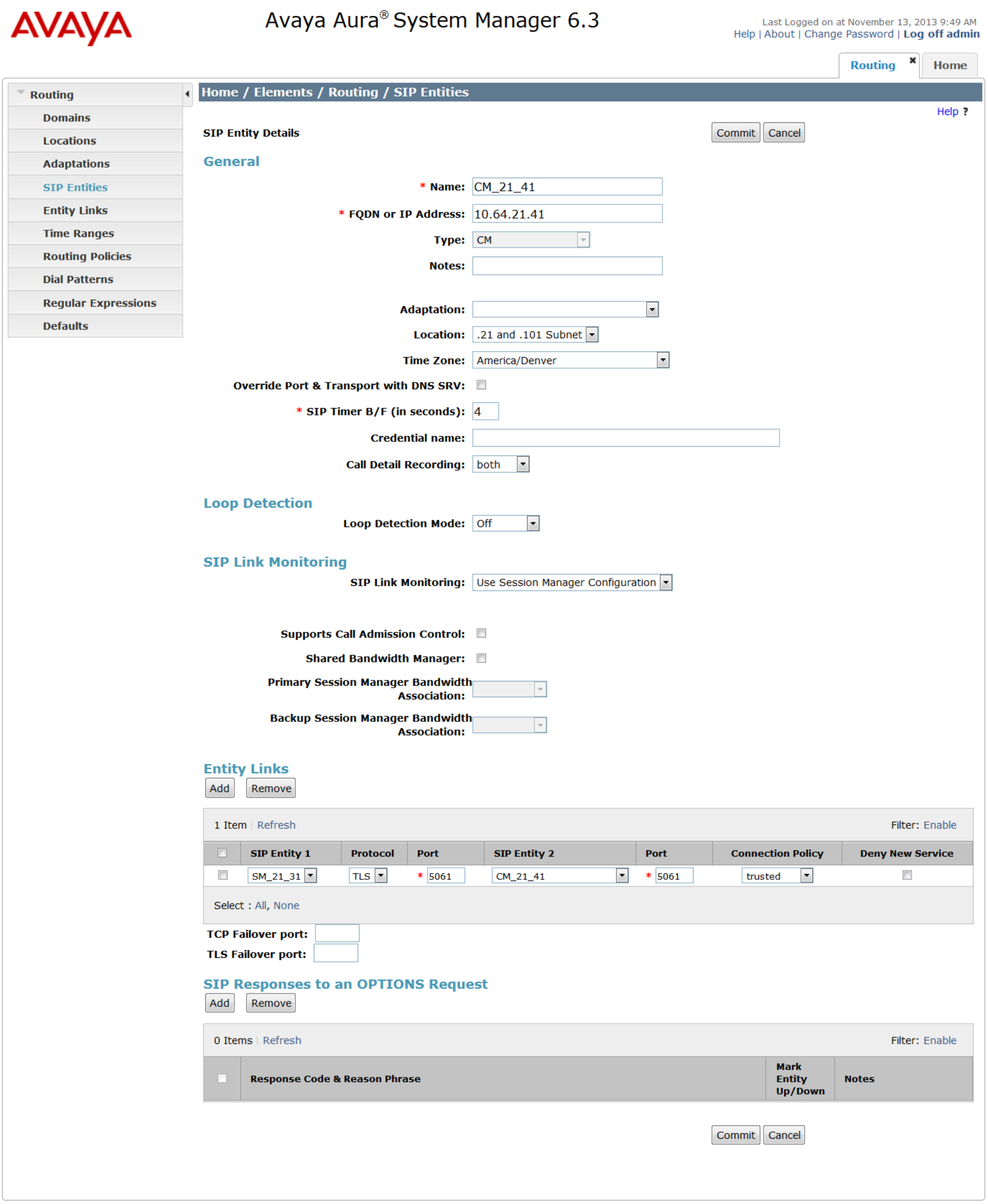
Select : All, None

SIP Responses to an OPTIONS Request

0 Items | Refresh — Filter: Enable

☐	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

The following screen shows the results of adding Communication Manager. In this case, the **FQDN or IP Address** is the IP address of the processor Ethernet for the Avaya S8300 Media Server. Note the “CM” selection for **Type**.



SIP Entity Details

General

* Name: CM_21_41

* FQDN or IP Address: 10.64.21.41

Type: CM

Notes:

Adaptation:

Location: .21 and .101 Subnet

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: both

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

1 Item

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
☐	SM_21_31	TLS	* 5061	CM_21_41	* 5061	trusted	☐

Select : All, None

TCP Failover port:

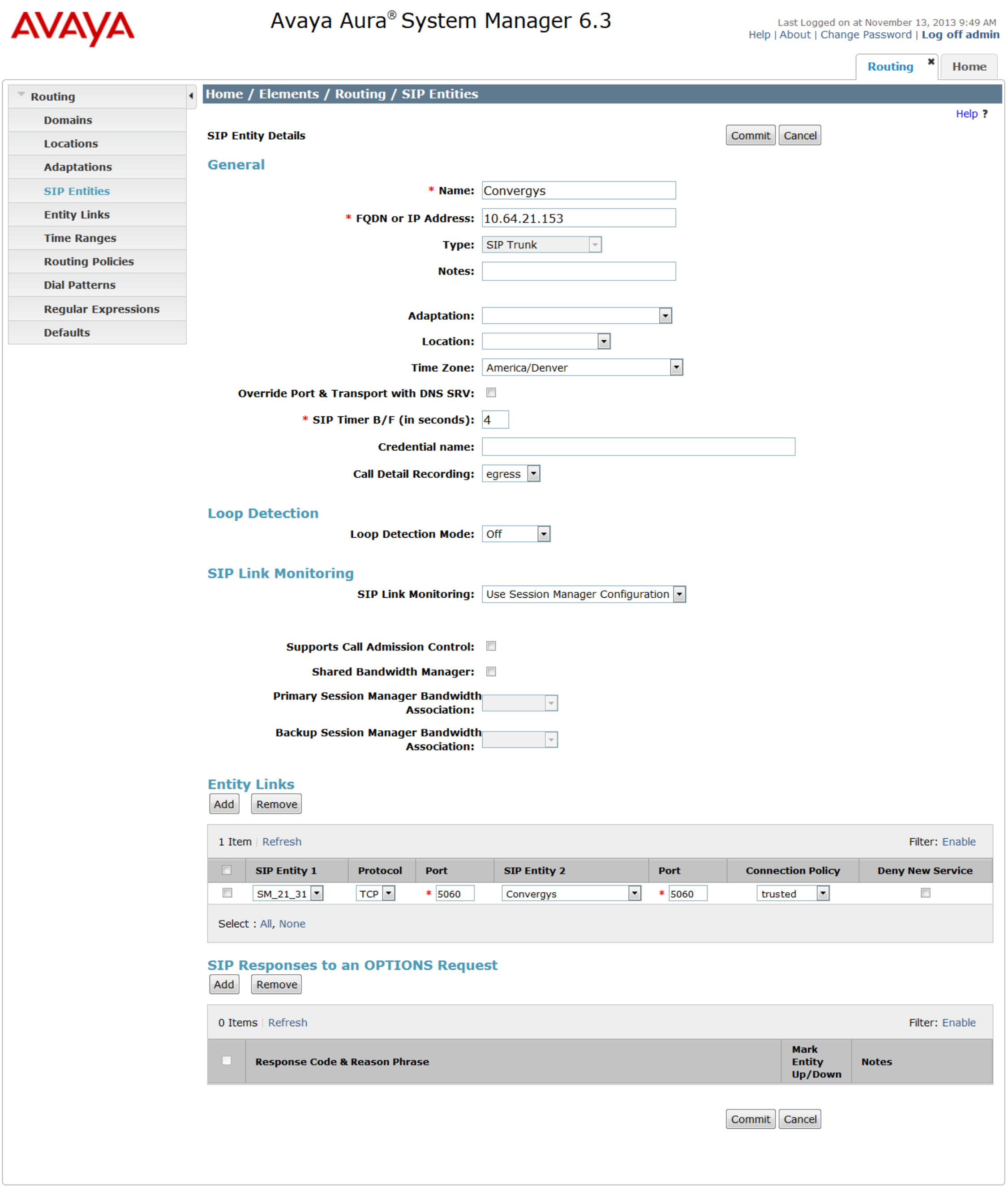
TLS Failover port:

SIP Responses to an OPTIONS Request

0 Items

☐	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

The following screen shows the results of adding the Convergys Voice Portal server. In this case, **FQDN or IP Address** is the IP address assigned to the server. Note the “SIP Trunk” selection for **Type**.



SIP Entity Details

General

* Name: Convergys

* FQDN or IP Address: 10.64.21.153

Type: SIP Trunk

Notes:

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
☐	SM_21_31	TCP	* 5060	Convergys	* 5060	trusted	☐

Select : All, None

SIP Responses to an OPTIONS Request

☐	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

5.

Add Entity Links

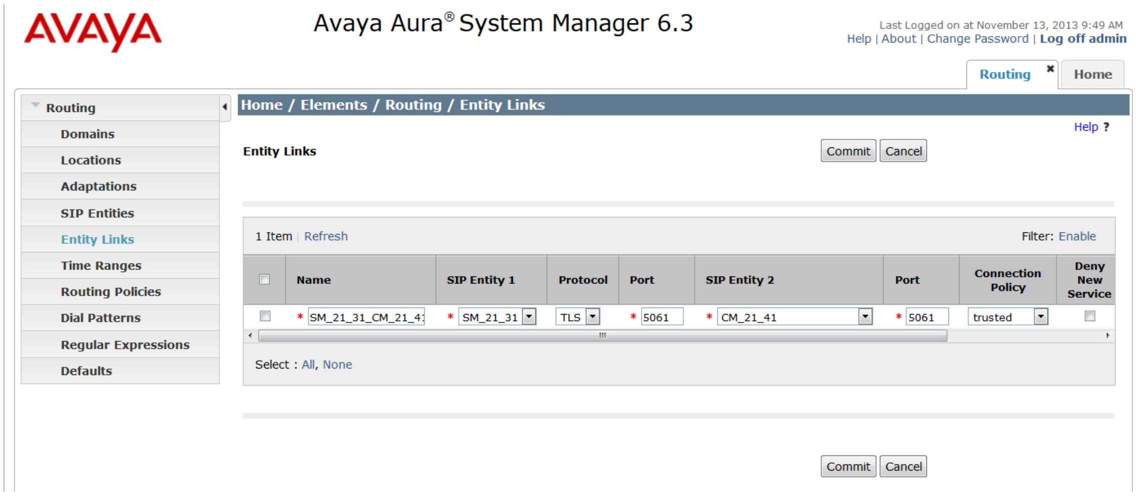
A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the configuration used for compliance testing, two Entity Links were configured; one for Session Manager to Communication Manager and one for Session Manager to the Convergys Voice Portal server.

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

- **Name**: A descriptive name
- **SIP Entity 1**: Select the Session Manager SIP Entity configured in previous step
- **Protocol**: Select "TLS"
- **Port**: Port number to which the other system sends SIP requests
- **SIP Entity 2**: Select the Communication Manager SIP Entity configured in previous step
- **Port**: Port number on which the other system receives SIP requests
- **Trusted**: Select "trusted"

Click **Commit** to save the configuration.

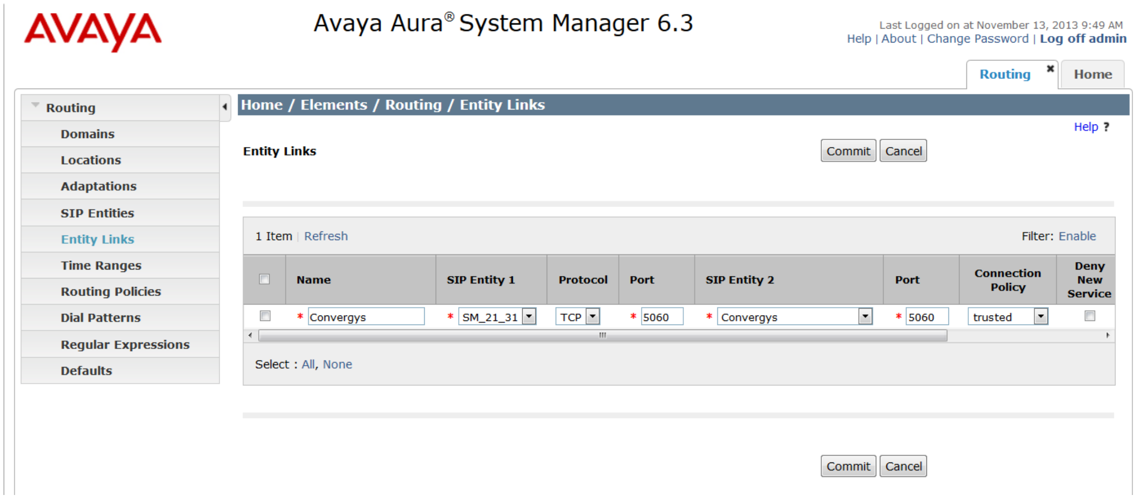
The screen below shows the first **Entity Link** configured between Session Manager and Communication Manager.



Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
☐	* SM_21_31_CM_21_4	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	trusted	☐

The second **Entity Link** between Session Manager and the Convergys Voice Portal server is similarly configured. The screen below shows the configured Entity Link. Select “TCP” for the **Protocol**, 5060 for each **Port**, and the Convergys Voice Portal server SIP Entity for **SIP Entity 2**.



☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
☐	* Convergys	* SM_21_31	TCP	* 5060	* Convergys	* 5060	trusted	☐

6. Add Routing Policy

A routing policy should be created for each “Routing Destination”. A routing policy must be added for routing calls to Communication Manager (from the Convergys Voice Portal server). Likewise, a routing policy must be added for routing calls to the Convergys Voice Portal server (from Communication Manager).

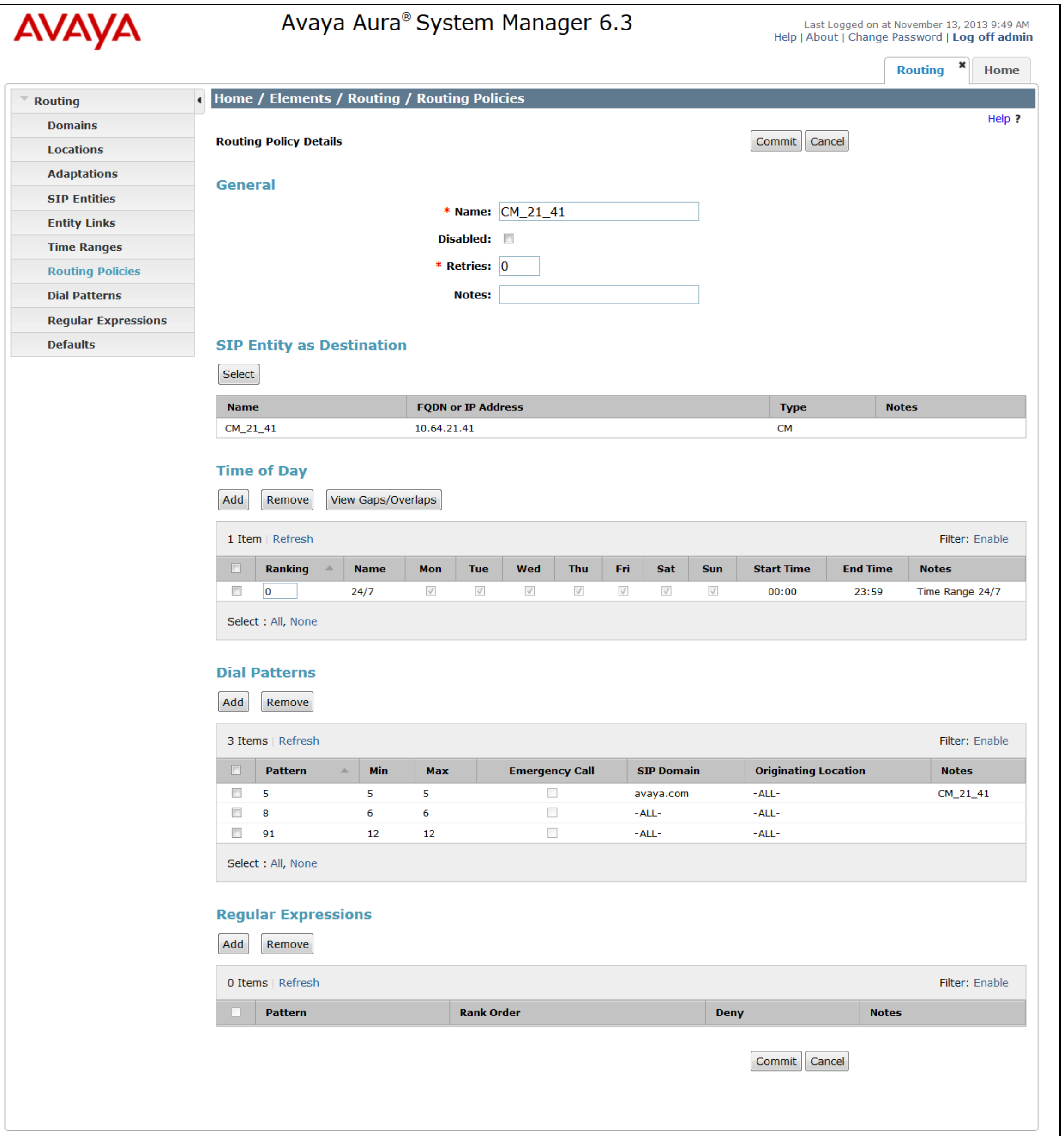
To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:
Enter a descriptive name in **Name** and optional text in **Notes**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies.

Under *Time of Day*:
Click **Add**, and select the default “24/7” time range.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy used for routing calls from the Convergys Voice Portal server to Communication Manager.



Routing Policy Details

General

* Name: CM_21_41

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM_21_41	10.64.21.41	CM	

Time of Day

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

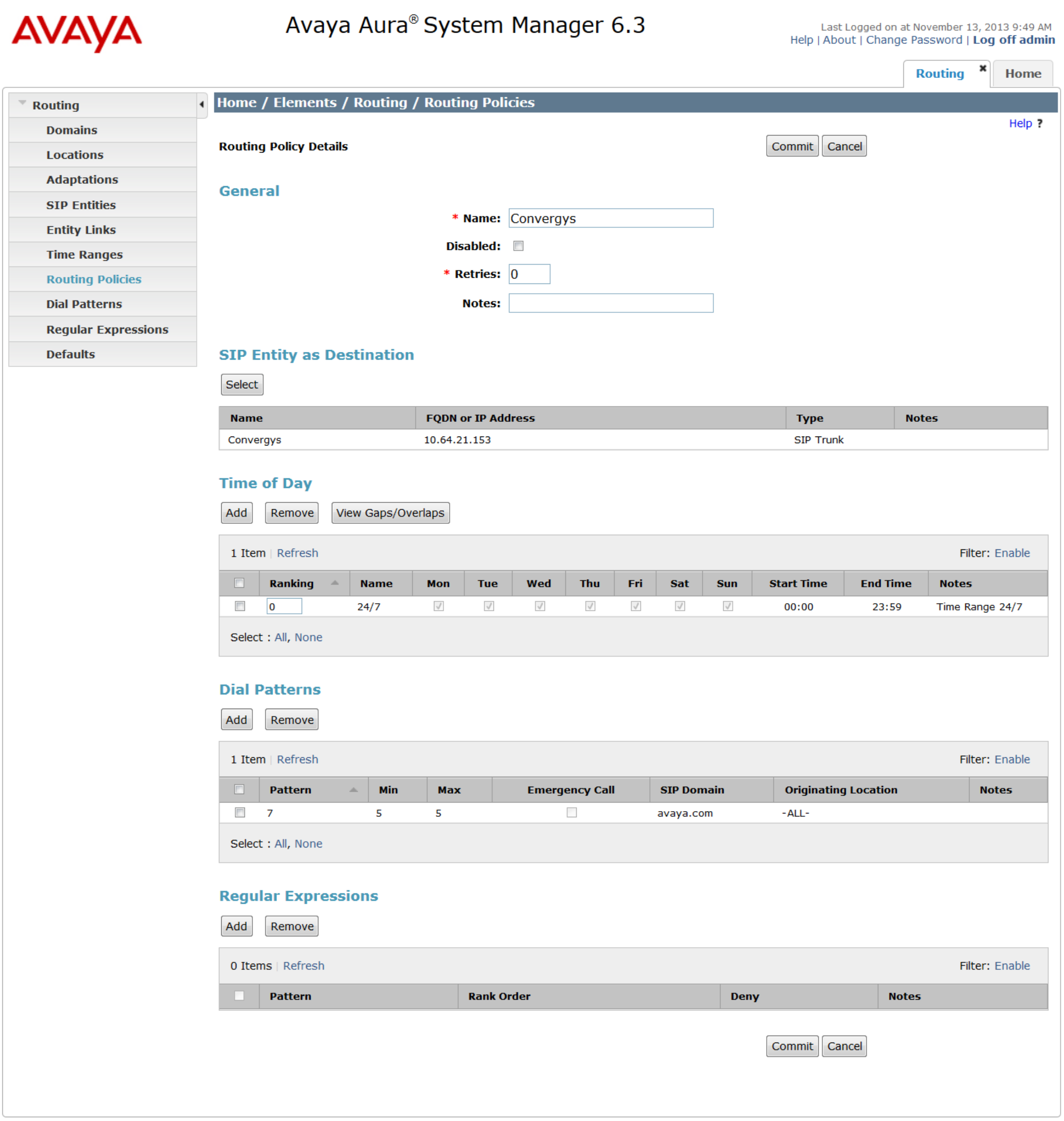
Dial Patterns

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	5	5	5	☐	avaya.com	-ALL-	CM_21_41
☐	8	6	6	☐	-ALL-	-ALL-	
☐	91	12	12	☐	-ALL-	-ALL-	

Regular Expressions

☐	Pattern	Rank Order	Deny	Notes

The following screen shows the Routing Policy used for routing calls to the Convergys Voice Portal server.



Routing Policy Details

General

* Name: Convergys

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Convergys	10.64.21.153	SIP Trunk	

Time of Day

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	7	5	5	☐	avaya.com	-ALL-	

Select : All, None

Regular Expressions

☐	Pattern	Rank Order	Deny	Notes

7. **Add Dial Patterns**

A Dial Pattern is associated with a Routing Policy to direct calls to a destination based on dialed digits.

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

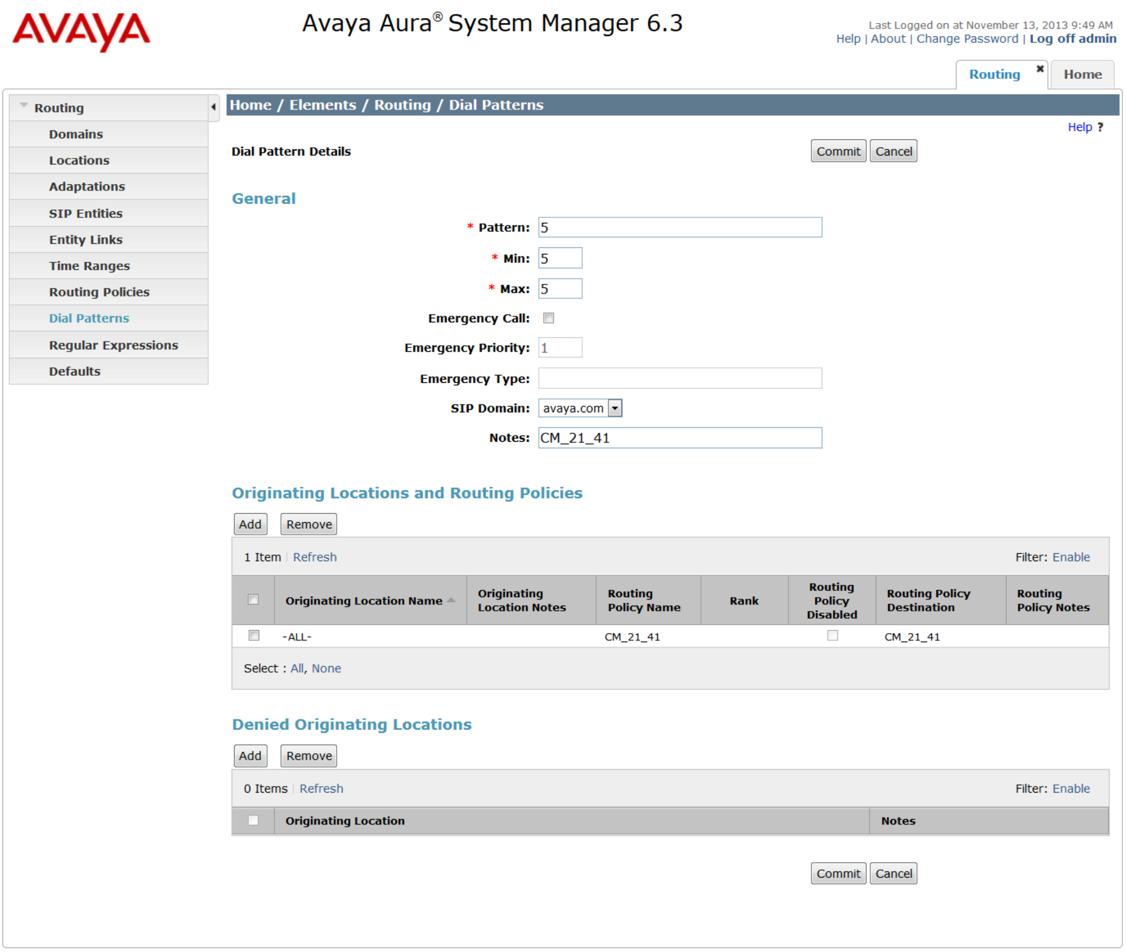
Under *General*:

- **Pattern**: Dialed number or prefix
- **Min**: Minimum length of dialed number
- **Max**: Maximum length of dialed number
- **SIP Domain**: SIP domain specified in **Step 2** of this section, or **ALL**.
- **Notes**: Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate Location (or “ALL”) for **Originating Location Name** field and select the appropriate Routing Policy from the list.

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

The entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to Communication Manager. Any call made to a 5 digit number starting with “5” will be routed to Communication Manager.



Dial Pattern Details

General

* Pattern: 5

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes: CM_21_41

Originating Locations and Routing Policies

1 Item

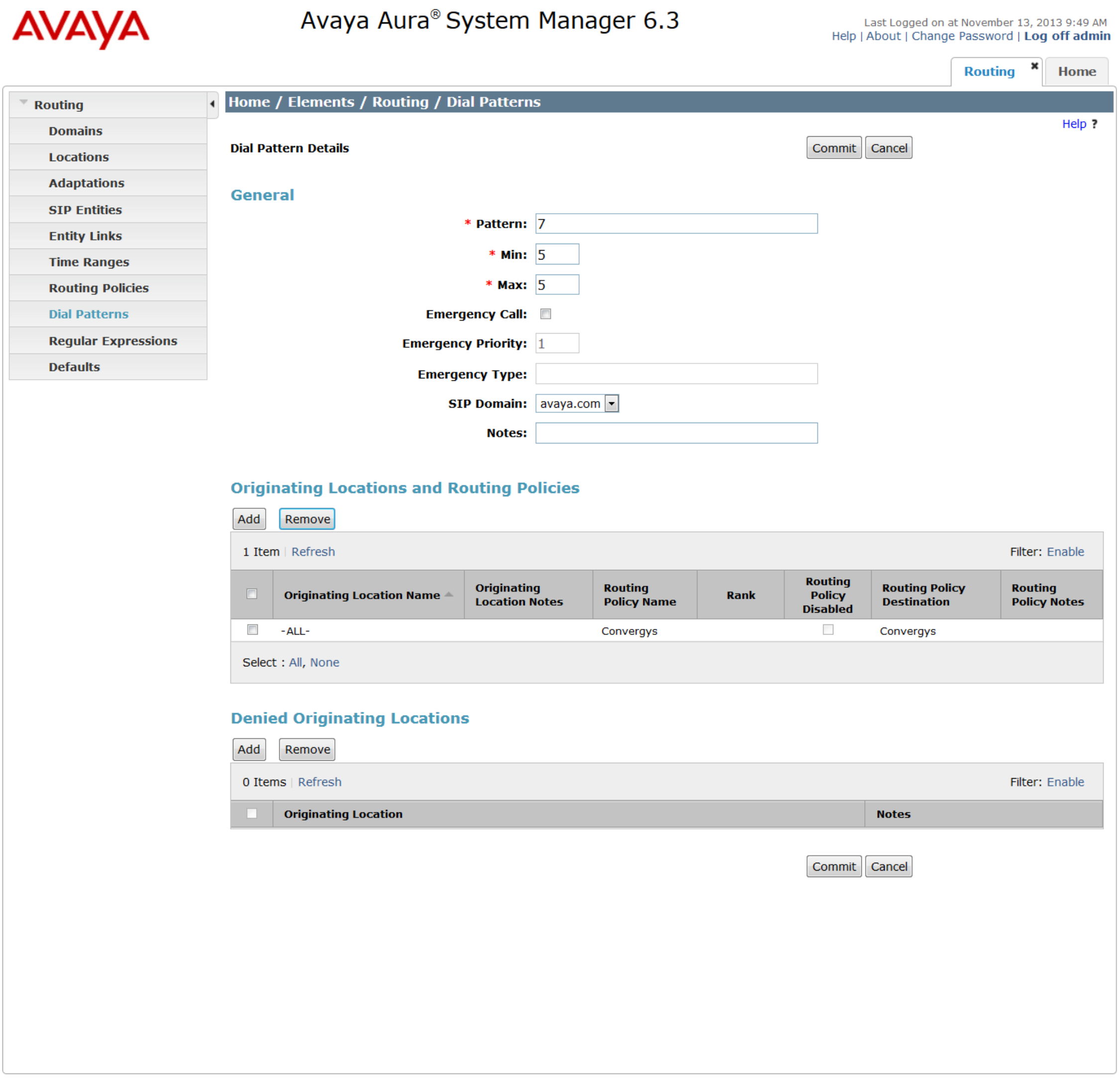
☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-		CM_21_41		☐	CM_21_41	

Denied Originating Locations

0 Items

☐	Originating Location	Notes

The entry under **Originating Locations and Routing Policies** on the following screen shows the Dial Pattern defined for routing calls to the Convergys Voice Portal server. Any call made to a 5 digit number starting with "7" will be routed to the Convergys Voice Portal server.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 7

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-		Convergys		☐	Convergys	

Select : All, None

Denied Originating Locations

0 Items | Refresh   Filter: Enable

☐	Originating Location	Notes

8. **Add Session Manager**

Adding the Session Manager provides the linkage between System Manager and Session Manager. This configuration procedure should have already been properly executed if the Session Manager used has been set up for other purposes. This configuration step is included here for reference and completeness. To add Session Manager, navitage to **Home → Elements → Session Manager → Session Manager Administration**. Click **New** under the "Session Manager Instances" section (not shown), and fill in the fields as described below and shown in the following screen (note that the screen below is for **Edit Session Manager** since it was already administered):

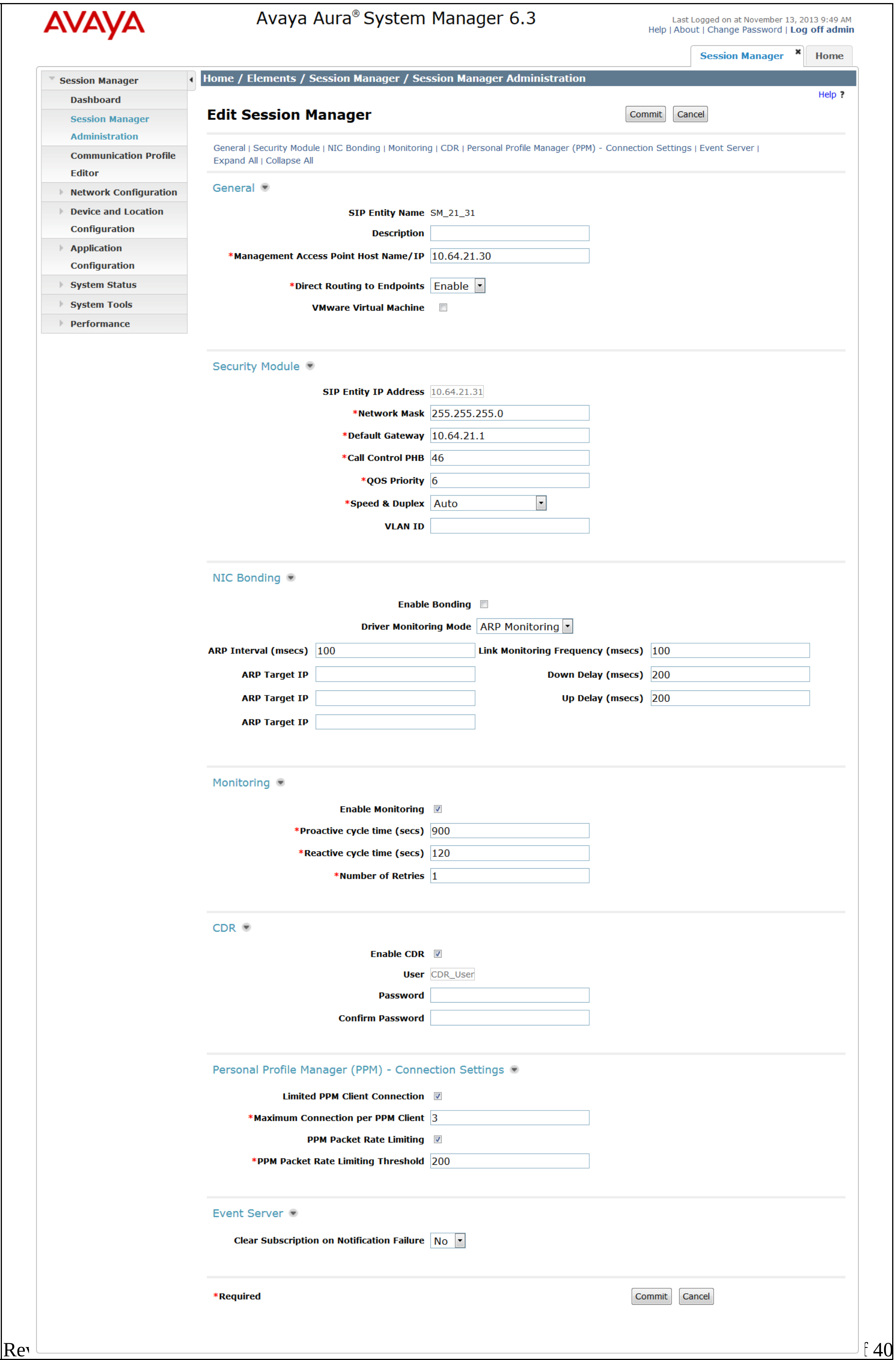
Under *General*:

- **SIP Entity Name**: Select the name of the SIP Entity created for Session Manager
- **Description**: Any descriptive text
- **Management Access Point Host Name/IP**: IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask**: Enter the proper network mask for Session Manager.
- **Default Gateway**: Enter the default gateway IP address for Session Manager

Accept default settings for the remaining fields.



Edit Session Manager

General

SIP Entity Name SM_21_31

Description

***Management Access Point Host Name/IP** 10.64.21.30

***Direct Routing to Endpoints** Enable

VMware Virtual Machine ☐

Security Module

SIP Entity IP Address 10.64.21.31

***Network Mask** 255.255.255.0

***Default Gateway** 10.64.21.1

***Call Control PHB** 46

***QOS Priority** 6

***Speed & Duplex** Auto

VLAN ID

NIC Bonding

Enable Bonding ☐

Driver Monitoring Mode ARP Monitoring

ARP Interval (msecs) 100

Link Monitoring Frequency (msecs) 100

ARP Target IP

Down Delay (msecs) 200

ARP Target IP

Up Delay (msecs) 200

ARP Target IP

Monitoring

Enable Monitoring ☑

***Proactive cycle time (secs)** 900

***Reactive cycle time (secs)** 120

***Number of Retries** 1

CDR

Enable CDR ☑

User CDR_User

Password

Confirm Password

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection ☑

***Maximum Connection per PPM Client** 3

PPM Packet Rate Limiting ☑

***PPM Packet Rate Limiting Threshold** 200

Event Server

Clear Subscription on Notification Failure No

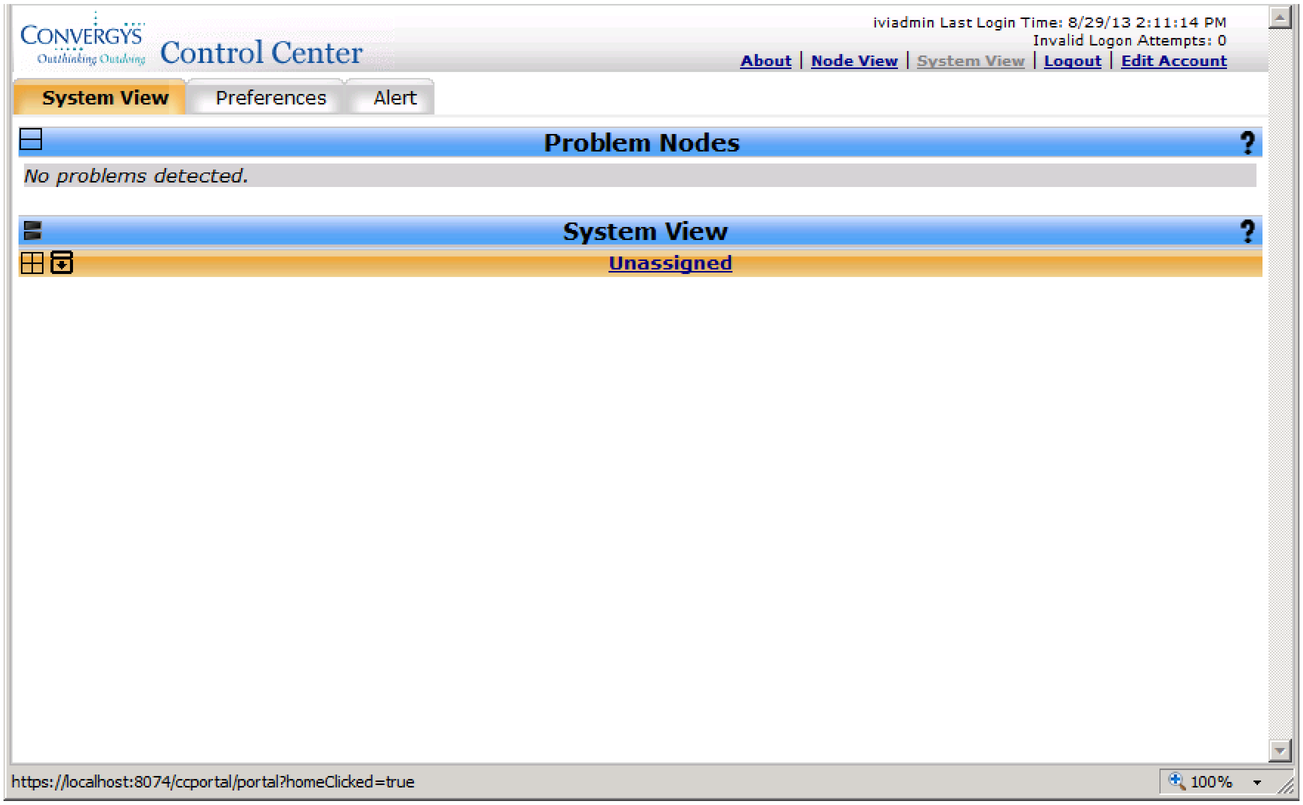
***Required**

7. Configure Convergys Voice Portal

This section provides steps to configure Convergys Voice Portal. Convergys installs, configures, and customizes the Voice Portal application for end customers. This section describes the initial Voice Portal configuration.

Launch a web browser, enter http://localhost:8070/ccportal/portal in the URL. Log in with the appropriate credentials and click the **Accept** button on the following screen (not shown) to access the **System View** page.

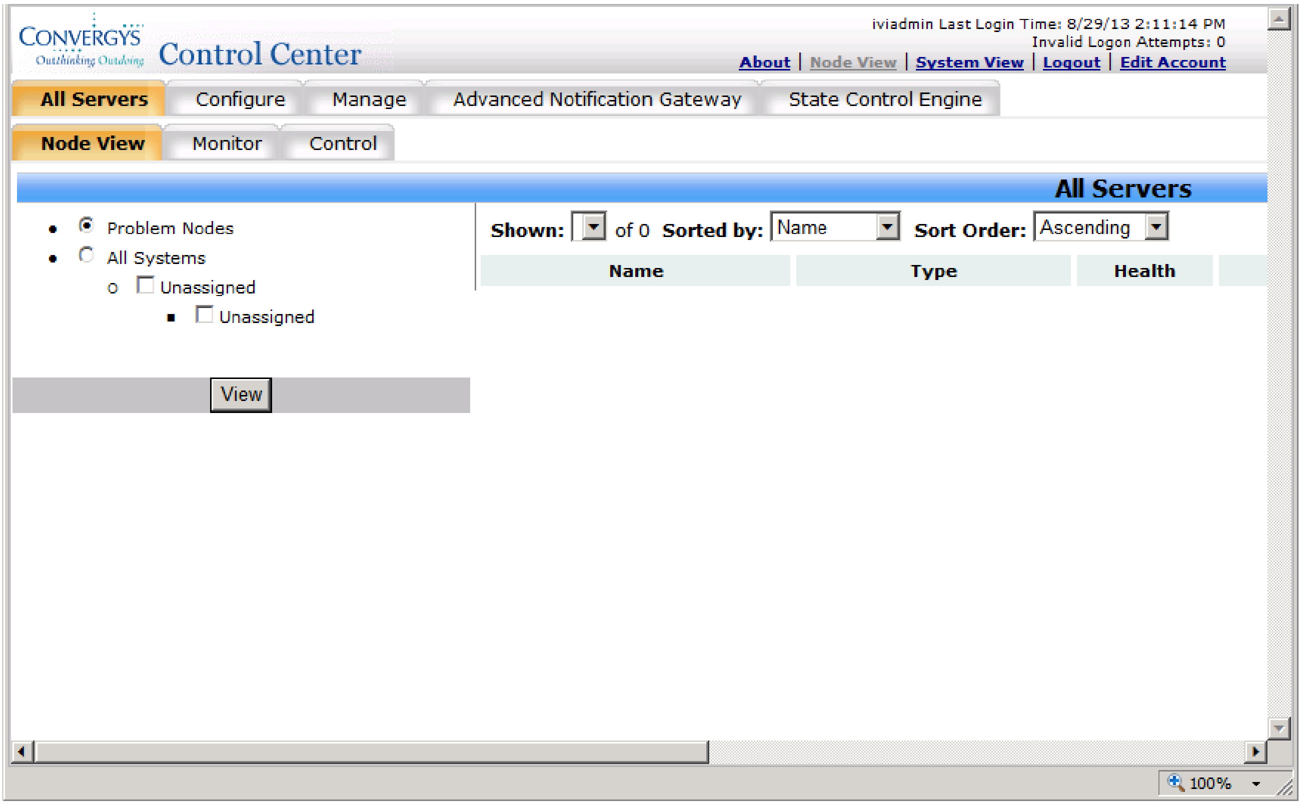
Select the **Node View** link at the top right.



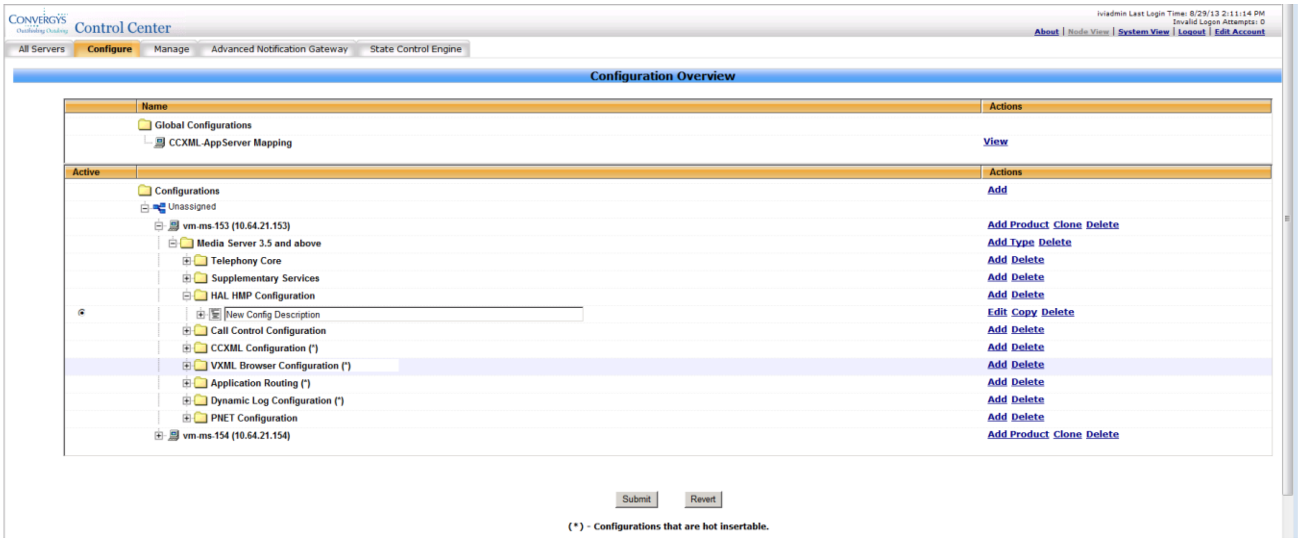
No problems detected.

https://localhost:8074/ccportal/portal?homeClicked=true

Click the **Configure** tab on the top left to start configuring Convergys Voice Portal.



Expand and navigate to **Unassigned → vm-ms-153 (10.64.21.153) → Media Server 3.5 and above → HAL HMP Configuration → New Config Description.** Click the **Edit** link next to the **New Config Description** field.



Control Center

iviadmin Last Login Time: 8/29/13 2:11:14 PM
Invalid Logon Attempts: 0

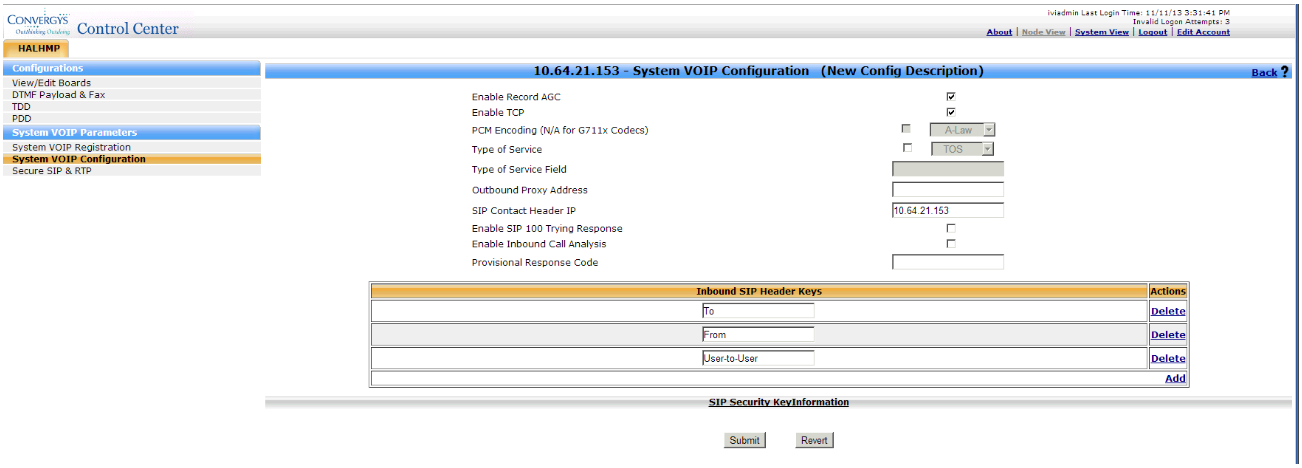
Configuration Overview

Name	Actions
Global Configurations	
CCXML-AppServer Mapping	View

Active		Actions
	Configurations	Add
	Unassigned	
	vm-ms-153 (10.64.21.153)	Add Product Clone Delete
	Media Server 3.5 and above	Add Type Delete
	Telephony Core	Add Delete
	Supplementary Services	Add Delete
	HAL HMP Configuration	Add Delete
●	New Config Description	Edit Copy Delete
	Call Control Configuration	Add Delete
	CCXML Configuration (*)	Add Delete
	VXML Browser Configuration (*)	Add Delete
	Application Routing (*)	Add Delete
	Dynamic Log Configuration (*)	Add Delete
	PNET Configuration	Add Delete
	vm-ms-154 (10.64.21.154)	Add Product Clone Delete

(*) - Configurations that are hot insertable.

Select **System VOIP Configuration** under the System VOIP Parameters menu on the left. Under **Inbound SIP Header Keys**, add a **User-to-User** key. This will make the contents of the User-to-User header of the SIP INVITE available to Voice Portal applications processing inbound calls.



Control Center

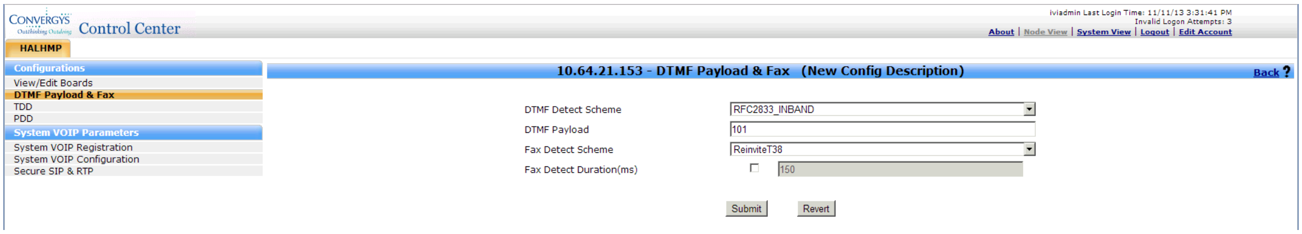
iviadmin Last Login Time: 11/11/13 3:31:41 PM
Invalid Logon Attempts: 3

10.64.21.153 - System VOIP Configuration (New Config Description)

Enable Record AGC	☑
Enable TCP	☑
PCM Encoding (N/A for G711x Codecs)	☐ A-Law
Type of Service	☐ TOS
Type of Service Field	
Outbound Proxy Address	
SIP Contact Header IP	10.64.21.153
Enable SIP 100 Trying Response	☐
Enable Inbound Call Analysis	☐
Provisional Response Code	

Inbound SIP Header Keys	Actions
To	Delete
From	Delete
User-to-User	Delete
	Add

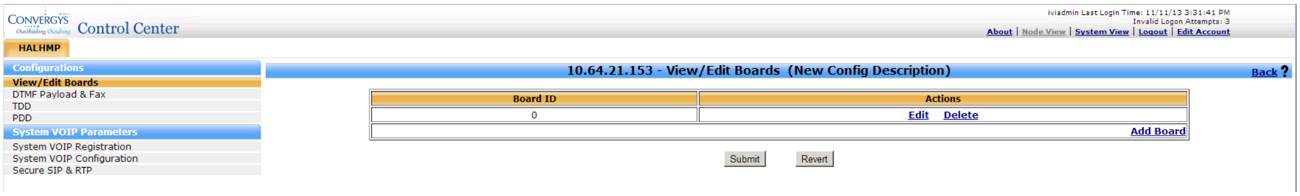
Select **DTMF Payload and Fax** under the Configurations menu on the left. Use the **DTMF Detect Scheme** drop down menu to select the appropriate setting (***RFC2833 INBAND*** is shown in the example below).



10.64.21.153 - DTMF Payload & Fax (New Config Description)

DTMF Detect Scheme: RFC2833_INBAND
DTMF Payload: 101
Fax Detect Scheme: ReinviteT38
Fax Detect Duration(ms): ☐ 150

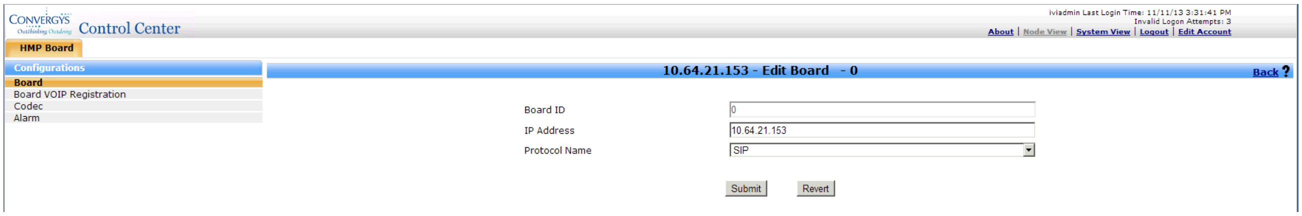
Select **View/Edit Boards** under the Configurations menu on the left. Select the **Edit** link for the board.



10.64.21.153 - View/Edit Boards (New Config Description)

Board ID	Actions
0	Edit Delete
	Add Board

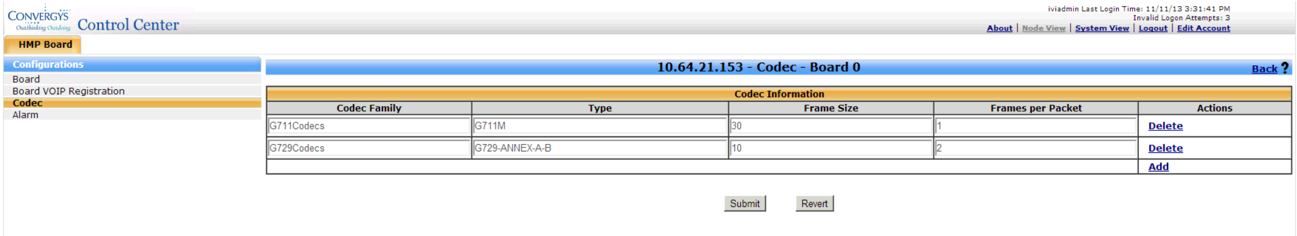
Set the **IP Address** for the board and use the drop down menu to select ***SIP*** for the **Protocol Name**.



10.64.21.153 - Edit Board - 0

Board ID: 0
IP Address: 10.64.21.153
Protocol Name: SIP

Select **Codec** under the Configurations menu on the left. Click the **Add** link.

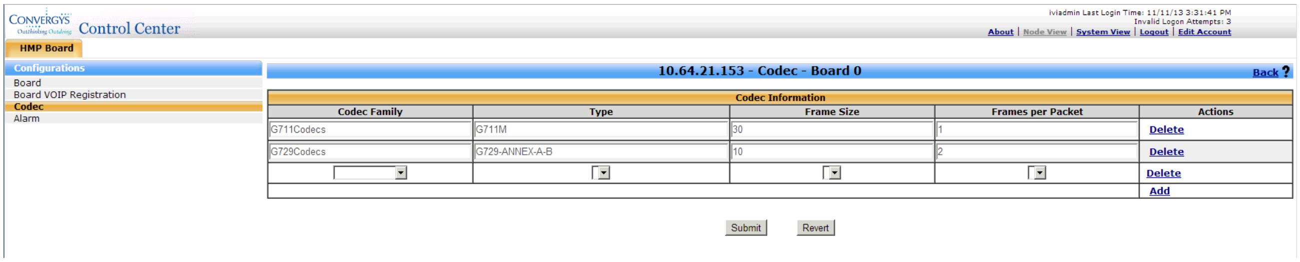


10.64.21.153 - Codec - Board 0

Codec Information

Codec Family	Type	Frame Size	Frames per Packet	Actions
G711Codecs	G711M	30	1	Delete
G729Codecs	G729-ANNEX-A-B	10	2	Delete
				Add

Use the drop down menus to select the appropriate settings for **Codec Family**, **Type**, **Frame Size**, and **Frames per Packet**.



10.64.21.153 - Codec - Board 0

Codec Information				
Codec Family	Type	Frame Size	Frames per Packet	Actions
G711Codecs	G711M	30	1	Delete
G729Codecs	G729-ANNEX-A-B	10	2	Delete
				Delete
				Add

This completes the administration of the Convergys Voice Portal Server.

8. Verification Steps

The following steps may be used to verify the configuration:

- End-to-end verification: Place a call to the Convergys Voice Portal server. Verify the call is answered and voice prompts are played. Verify the SIP messages using a network protocol analyzer.
- DTMF Tones: Place a call to the Convergys Voice Portal server and select the appropriate prompt to enter DTMF tones. Verify Convergys Voice Portal properly identified each DTMF tone.
- Transfer: Place a call to Convergys Voice Portal and select the appropriate prompt to have the call transferred to an Agent. Verify the call is delivered to an Agent and answer the call. Verify there is a two-way talk path.

9. Conclusion

These Application Notes describe the procedures required to configure Convergys Voice Portal to interoperate with an Avaya SIP infrastructure (Communication Manager and Session Manager). Convergys Voice Portal successfully passed compliance testing.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com:

[1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 11, Release 6.3, October 2013.
[2] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013.
[3] *Avaya Aura® Communication Manager Screen Reference*, Document 03-602878, Issue 5, October 2013.
[4] *Deploying Avaya Aura® Session Manager*, Issue 1, Release 6.3, October 2013.
[5] *Administering Avaya Aura® Session Manager*, Document 03-603324, Issue 3, Release 6.3, October 2013.
[6] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Document 03-603325, Issue 3, Release 6.3, October 2013.

The following documents were provided by Convergys:

[7] *Media Server 4.0 (VoIP) Installation Guide*, Document Number 60001490
[8] *Media Server VoiceXML Browser Technical Reference,* Document Number 60001390

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 DevConnect Program at devconnect@avaya.com.