Avaya Solution & Interoperability Test Lab

Application Notes for Biscom FAXCOM Server with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager Using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Biscom FAXCOM Server to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager using SIP trunks. Biscom FAXCOM Server is a fax solution that utilizes a SIP trunk to Avaya Aura™ Session Manager to send and receive faxes.

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 configuration steps required for Biscom FAXCOM Server to interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager using SIP trunks. Biscom FAXCOM Server is a fax solution that utilizes a SIP trunk to Avaya Aura™ Session Manager to send and receive faxes.

Biscom FAXCOM Server utilizes the Dialogic Brooktrout SR140 Virtual Fax Board to support T.38 fax over the IP network, and integration with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager is achieved through SIP trunks.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on the Biscom FAXCOM Server:

- Proper handling of faxes via SIP trunks, including: sending/receiving faxes, intra-site faxes, inter-site faxes over ISDN (PRI), inter-site over IP (SIP), different media processor boards, simultaneous bi-directional faxes, and miscellaneous failure scenarios.

- Proper handling of faxes with different pages, resolution, complexity, format, and data rates.

- No adverse impact on intra and inter-site VoIP calls during faxes.

The serviceability testing focused on verifying the ability of the Biscom FAXCOM Server to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable and stopping/starting the fax service on the Biscom FAXCOM Server.

1.2. Support

Technical support on Biscom FAXCOM Server can be obtained through the following:

- **Phone:** (978) 250-8355
- **Web:** www.biscom.com/support

2. Reference Configuration

As shown in **Figure 1**, both the Local and Remote sites have a Biscom FAXCOM Server. SIP trunks are used to connect each Biscom FAXCOM Server with the local Avaya Aura^{TM} Communication Manager via the local Avaya Aura^{TM} Session Manager server. Routing between the two sites include both ISDN PRI and SIP trunks.

The Remote site consists of two Avaya G650 Media Gateways, with each media gateway configured as a separate port network in a separate IP network region.

The detailed administration of routing between the two sites and basic connectivity between Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Session Manager are not the focus of these Application Notes and will not be described.

The administration procedures in these Application Notes are shown for the Local site. Unless specified otherwise, the same procedures need to apply to the Remote site using appropriate values for the Remote site from **Figure 1**.

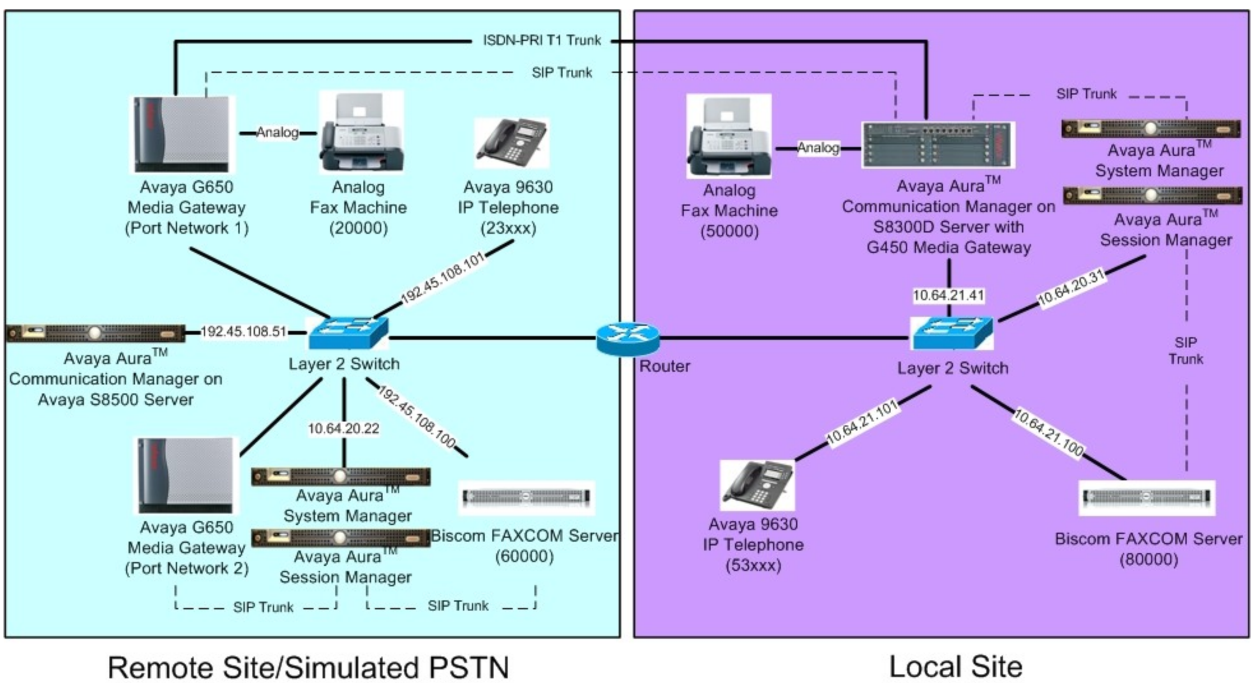


Figure 1: Biscom FAXCOM Server with Communication Manager and Session Manager Using SIP Trunks

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8300 Server with Avaya G450 Media Gateway (Local site)	Avaya Aura™ Communication Manager 6.0, R016x.00.0.345.0, Update 18444 (Avaya Aura™ System Platform: 6.0.1.0.5)
Avaya S8800 Server (Local site)	Avaya Aura™ System Platform: 6.0.1.0.5 Avaya Aura™ System Manager: 6.0.7.0
Avaya S8800 Server (Local site)	Avaya Aura™ System Platform: 6.0.1.0.5 Avaya AuraTM Session Manager 6.0.0.0.600020
Avaya S8500 Server (Remote site)	Avaya Aura™ Communication Manager 5.2.1, R015x.02.1.016.4, Update 18433
Avaya G650 Media Gateways (Remote Site) • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor • TN2602AP IP Media Processor	 HW01 FW024 HW20 FW120 HW02 FW051
Avaya 9600 Series IP Telephones (H.323)	3.1.1
Biscom FAXCOM Server Dialogic Brooktrout SR140 SDK	6.1.9 6.2.4

4. Configure Avaya Aura™ Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer IP codec set
- Administer IP network region
- Administer IP node names
- Administer SIP signaling group
- Administer SIP trunk group
- Administer route pattern
- Administer public unknown numbering
- Administer AAR analysis

4.1. Verify Communication Manager License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. 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 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  100
           Maximum Concurrently Registered IP Stations: 2400  2
             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  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  280
  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    0
           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

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

4.2. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number that will be used for integration with the Biscom FAXCOM Server. Enter the audio codec type “G.711MU” in the **Audio Codec** fields. Retain the default values in the remaining fields.

```
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:
```

Navigate to **Page 2**, and enter “t.38-standard” for the **FAX Mode** field. Retain the default values in the remaining fields.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

4.3. Administer IP Network Region

Use the "change ip-network-region n" command, where "n" is an existing network region that will be used for integration with the Biscom FAXCOM Server. For the **Codec Set** field, enter the codec set number from **Section 4.2**. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to "no" (this is required for inter-site fax calls over the SIP trunks).

```
change ip-network-region 1                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Compliance Testing
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   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
```

4.4. Administer IP Node Names

Use the "change node-names ip" command, and add an entry for the local Session Manager. In this case, "SM2" and "10.64.20.31" are entered as **Name** and **IP Address**. Note the "procr" / "10.64.21.41" entry, which is the node name to the processor board, and will be used later to configure the SIP trunk to Session Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AcmePacket          10.64.20.106
CM-B1               192.45.108.55
CM-B2               192.45.108.57
FaxServer           10.64.21.100
SES-A               10.64.21.61
SM1                 10.64.40.42
SM2                 10.64.20.31
VoicePortal         10.64.10.32
default             0.0.0.0
procr               10.64.21.41
procr6              ::
```

4.5. Administer SIP Signaling Group

Administer a SIP signaling group for a new trunk that will be created for the connection between Communication Manager and Session Manager. Use the "add signaling-group n" command, where "n" is an available signaling group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** "sip"
- **Near-end Node Name:** Processor node name from **Section 4.4**.
- **Far-end Node Name:** Session Manager node name from **Section 4.4**.
- **Far-end Network Region:** The IP network region number from **Section 4.3**.
- **Far-end Domain:** "avaya.com"

```
change signaling-group 8                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 8             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                            SIP Enabled LSP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM2
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

4.6. Administer SIP Trunk Group

Administer a SIP trunk group to interface with the Session Manager. Use the "add trunk-group n" command, where "n" is an available trunk group number. Set the **Group Type** to "sip", and **Service Type** to "tie". Enter a descriptive **Group Name**, and an available trunk access code for the **TAC** field. Set **Member Assignment Method** to "auto", **Signaling Group** to the signaling group number from **Section 4.5**, and enter a desired value for number of trunk group members for **Number of Members**.

```
add trunk-group 8                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 8                   Group Type: sip           CDR Reports: y
  Group Name: demoSM (avaya.com)        COR: 1        TN: 1        TAC: 108
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 8
                                                   Number of Members: 10
```

Navigate to **Page 3**, and enter "public" for the **Numbering Format** field as shown below.

```
add trunk-group 8                                              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
```

4.7. Administer Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the "change route-pattern n" command, where "n" is an available route pattern. Enter a descriptive **Pattern Name**. In the **Grp No** field, enter the trunk group number from **Section 4.6**. In the **FRL** field, enter a level that allows access to this trunk with "0" being least restrictive.

```
change route-pattern 8                                          Page   1 of   3
                    Pattern Number: 8   Pattern Name: ToFaxServer
                             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: 8    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
```

4.8. Administer Public Unknown Numbering

Use the "change public-unknown-numbering 0" command, to define the calling party number to send to the local Session Manager. Add an entry for the trunk group defined in **Section 4.6**. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed over any trunk group will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                  Total Administered: 1
 5  5                                        5       Maximum Entries: 240
```

4.9. Administer AAR Analysis

This section provides a sample AAR routing used for routing calls with dialed digits 8xxxx to the local Session Manager. Note that other methods of routing may be used. Use the "change aar analysis 0" command, and add an entry to specify how to route calls to 8xxxx. In the example shown below, calls with digits 8xxxx will be routed as an AAR call using route pattern "8" from **Section 4.7**.

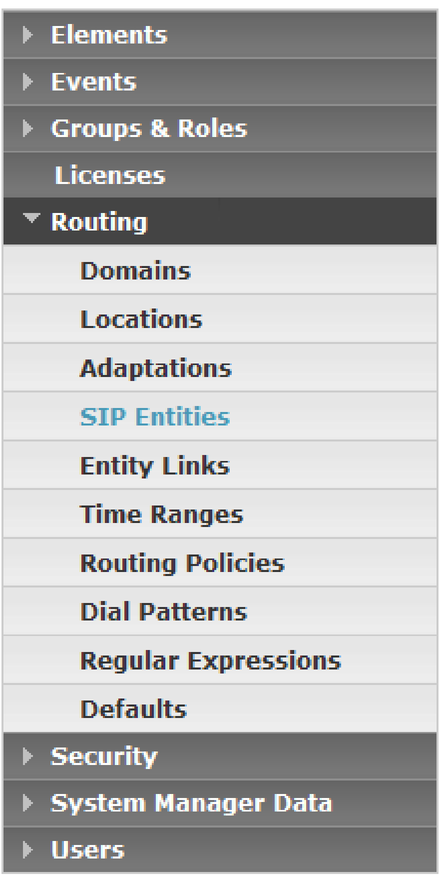
```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern    Type   Num   Reqd
    2                    5    5      1        aar          n
    6                    5    5      1        aar          n
    8                    5    5      8        aar          n
```

5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Avaya Aura™ Session Manager. The procedures include adding the following items:

- Administer Domain
- SIP Entities corresponding to the SIP telephony systems and Avaya Aura™ Session Manager
- Entity Links, which define the SIP trunk parameters used by Avaya Aura ™ Session Manager when routing calls to/from SIP Entities
- Time Ranges during which routing policies are active
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura™ System Manager, using the URL "http://<ip-address>/SMGR", where "<ip-address>" is the IP address of Avaya Aura™ System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The left menu shown below is displayed. Expand the **Routing** Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all of the above items (**Sections 5.1** through **5.6**).

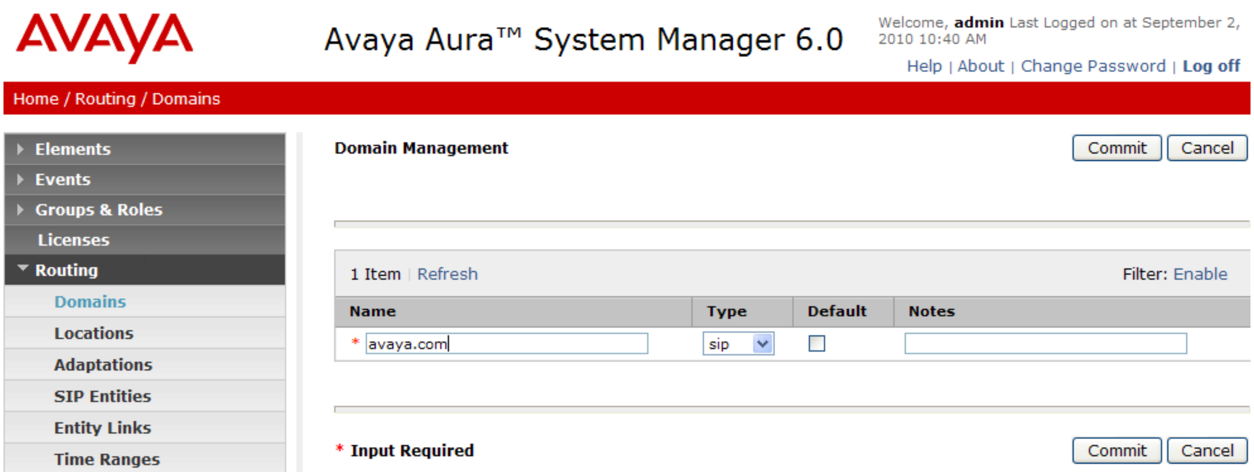


5.1. Specify Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., "avaya.com").
- **Notes:** Descriptive text (optional).

Click **Commit**.



5.2. Add SIP Entities

A SIP Element must be added for Avaya Aura™ Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration a SIP Element is added for the Session Manager, Communication Manager, and the Biscom FAXCOM Server. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under *General*:

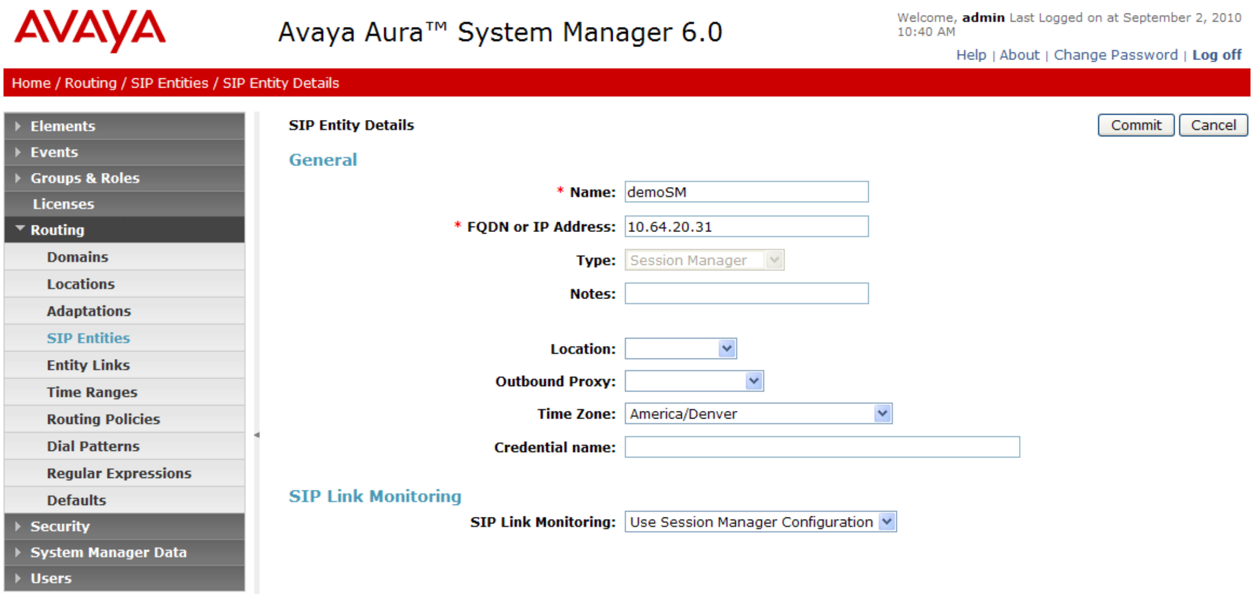
- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the SM or the signaling interface on the telephony system.
- **Type:** Select "Session Manager" for Avaya Aura™ Session Manager, "CM" for Communication Manager, and "other" for the fax server.

Under *SIP Link Monitoring*:

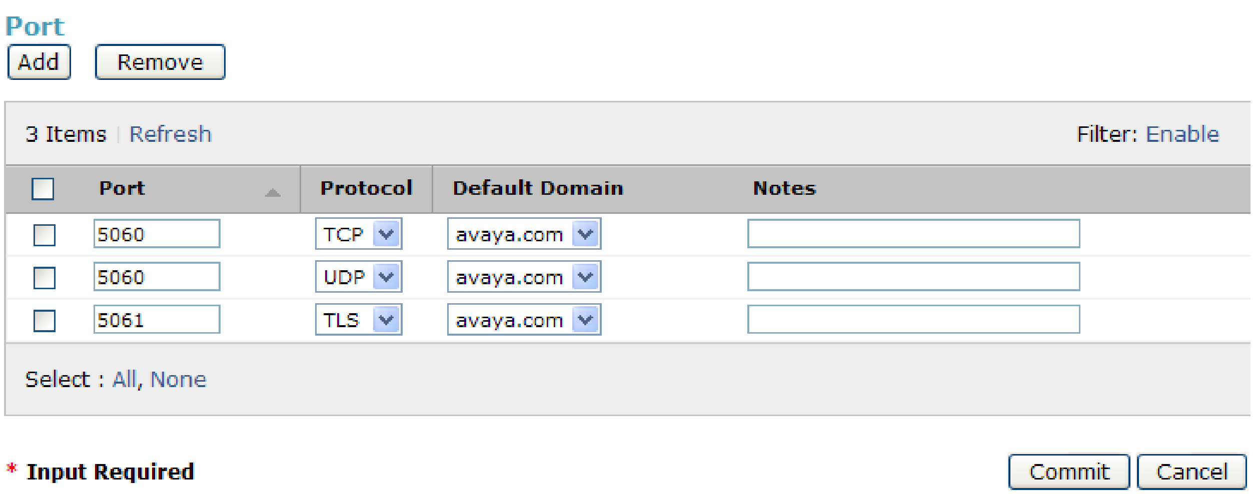
- **SIP Link Monitoring:** Select "Use Session Manager Configuration" or "Link Monitoring Enabled"

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

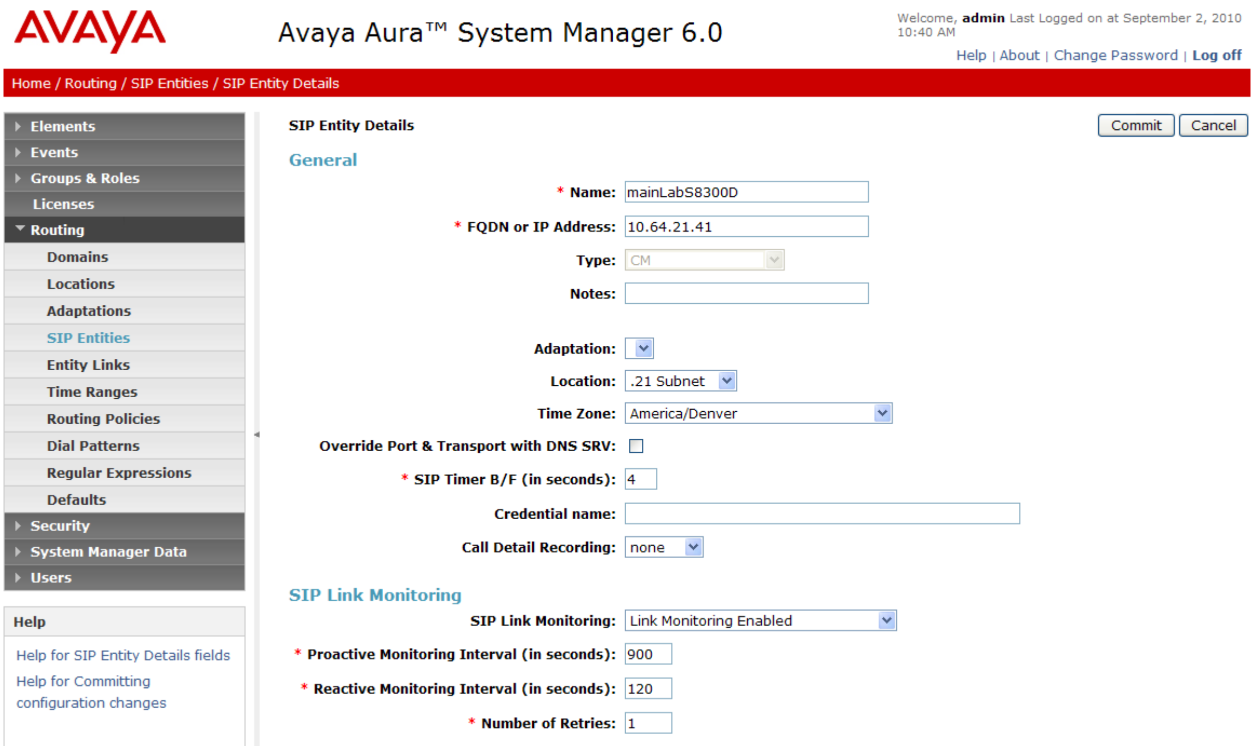
The following screen shows addition of Avaya Aura ™ Session Manager. The IP address used is that of the virtual SM-100 Security Module.



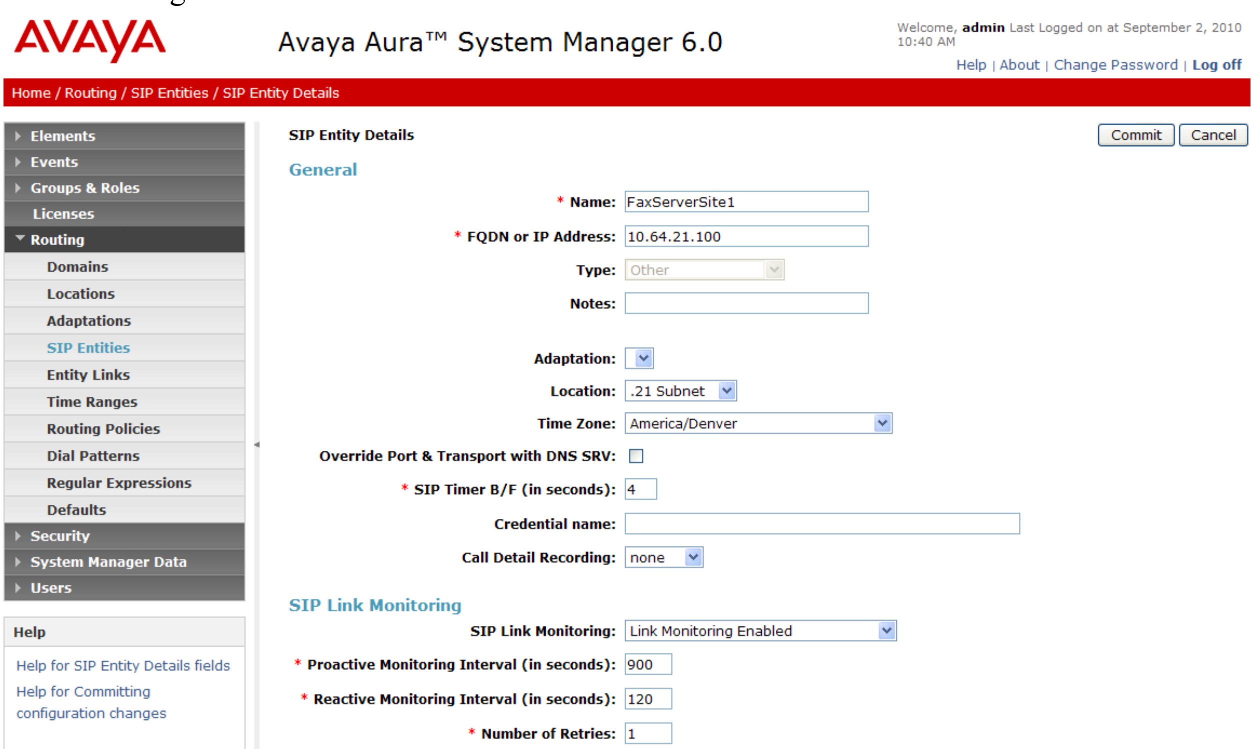
Under **Ports**, add the required listening port(s) for Session Manager.



The following screen shows addition of Communication Manager.



The following screen shows addition of the Biscom FAXCOM Server.



5.3. Add Entity Links

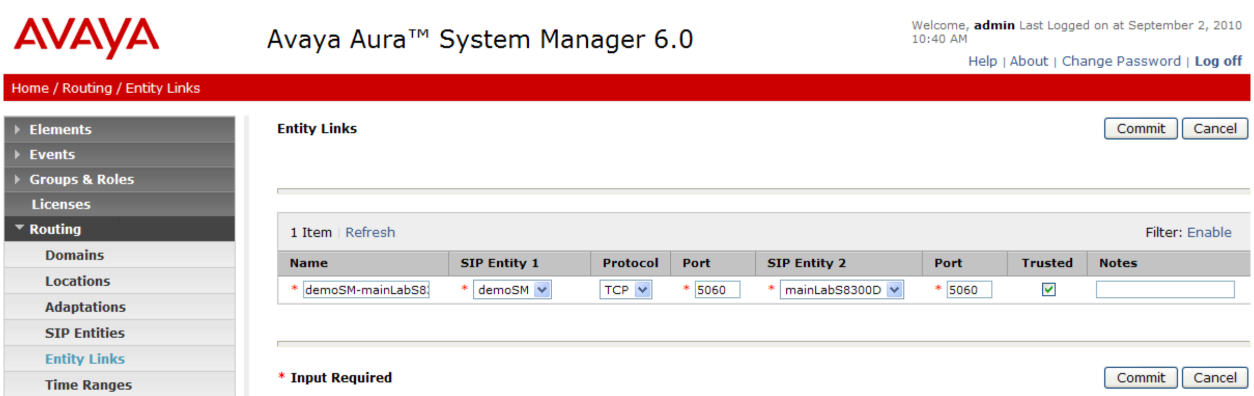
A SIP trunk between Avaya Aura™ Session Manager and a telephony system is described by an Entity link. To add an Element Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Avaya Aura™ Session Manager.
- **Port:** Port number to which the other system sends SIP requests In the sample configuration, TCP Protocol was used.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box. ***Note**:* If this box is not checked, calls from the associated SIP Element specified in **Section 5.2** will be denied.

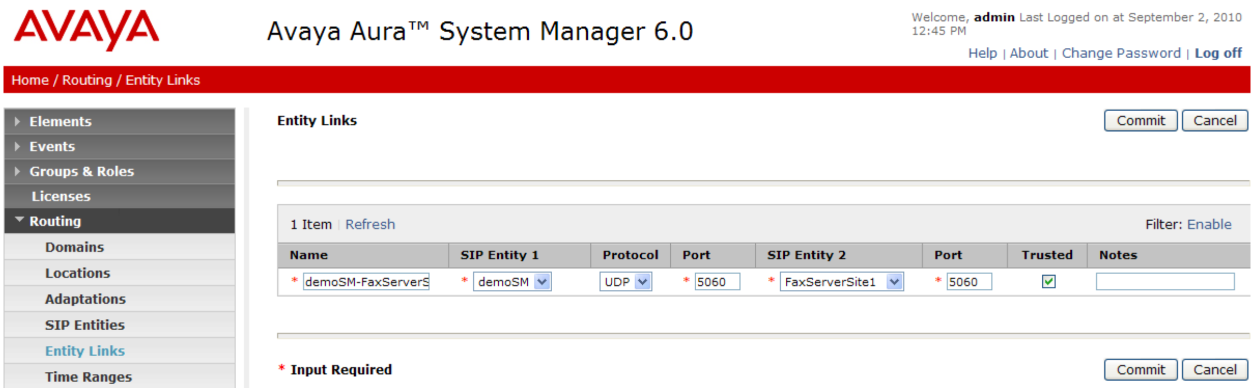
Click **Commit** to save each Entity Link definition.

The following screens illustrate adding the two Entity Links for:

1. Communication Manager
2. Biscom FAXCOM Server



Note, UDP must be selected as the protocol between Session Manager and the Biscom FAXCOM Server.

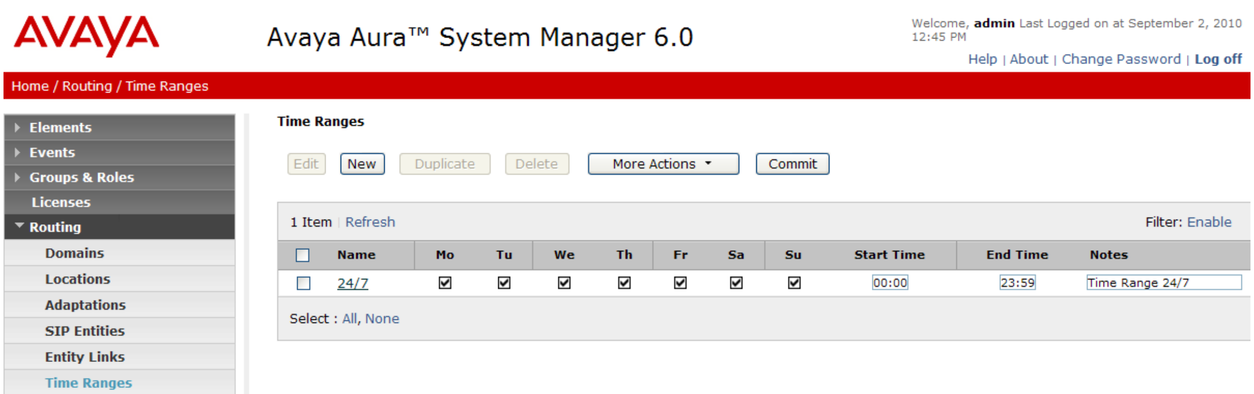


5.4. Add Time Ranges

Before adding routing policies (see next section), time ranges must be defined during which the policies will be active. In the sample configuration, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges**, and click on the left and click on the **New** button on the right. Fill in the following:

- **Name:** A descriptive name (e.g., "24/7").
- **Mo** through **Su** Check the box under each of these headings
- **Start Time** Enter 00:00.
- **End Time** Enter 23:59

Click **Commit** to save this time range.



5.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.2**. One routing policy must be added for routing calls to the Biscom FAXCOM Server. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

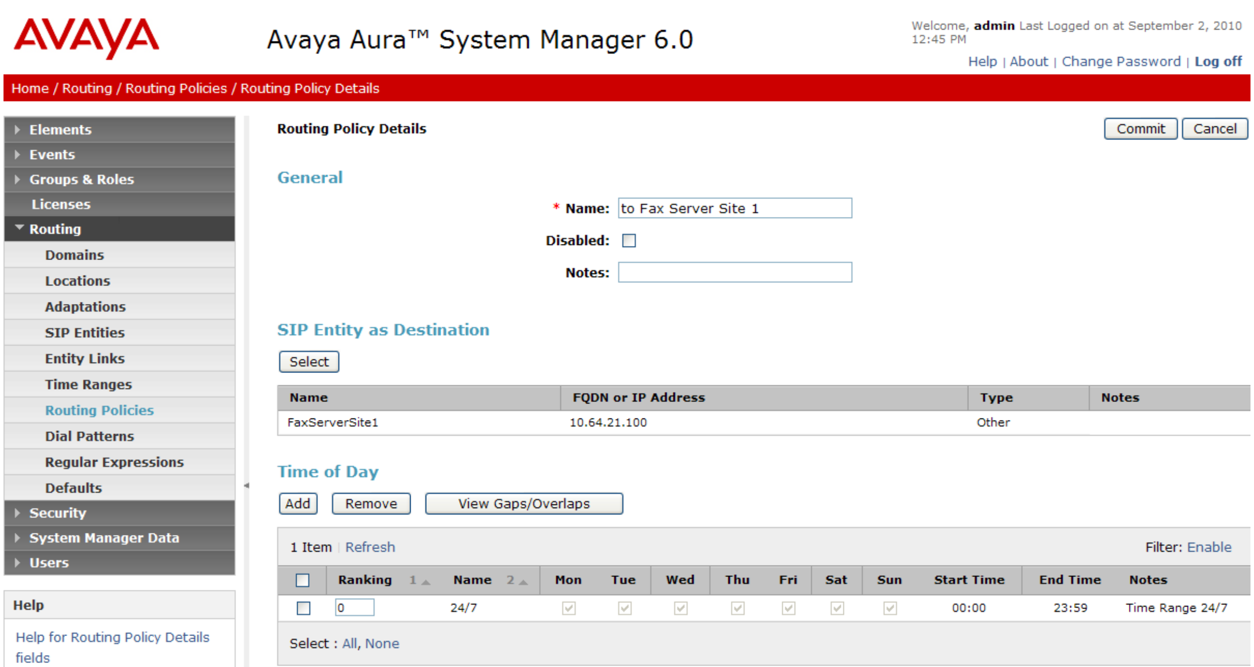
Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Enity 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 time range configured in the previous section.

Defaults can be used for the remaining fields. Click **Commit** to save Routing Policy definition.

The following screen shows the Routing Policy for routing calls to the Biscom FAXCOM Server.



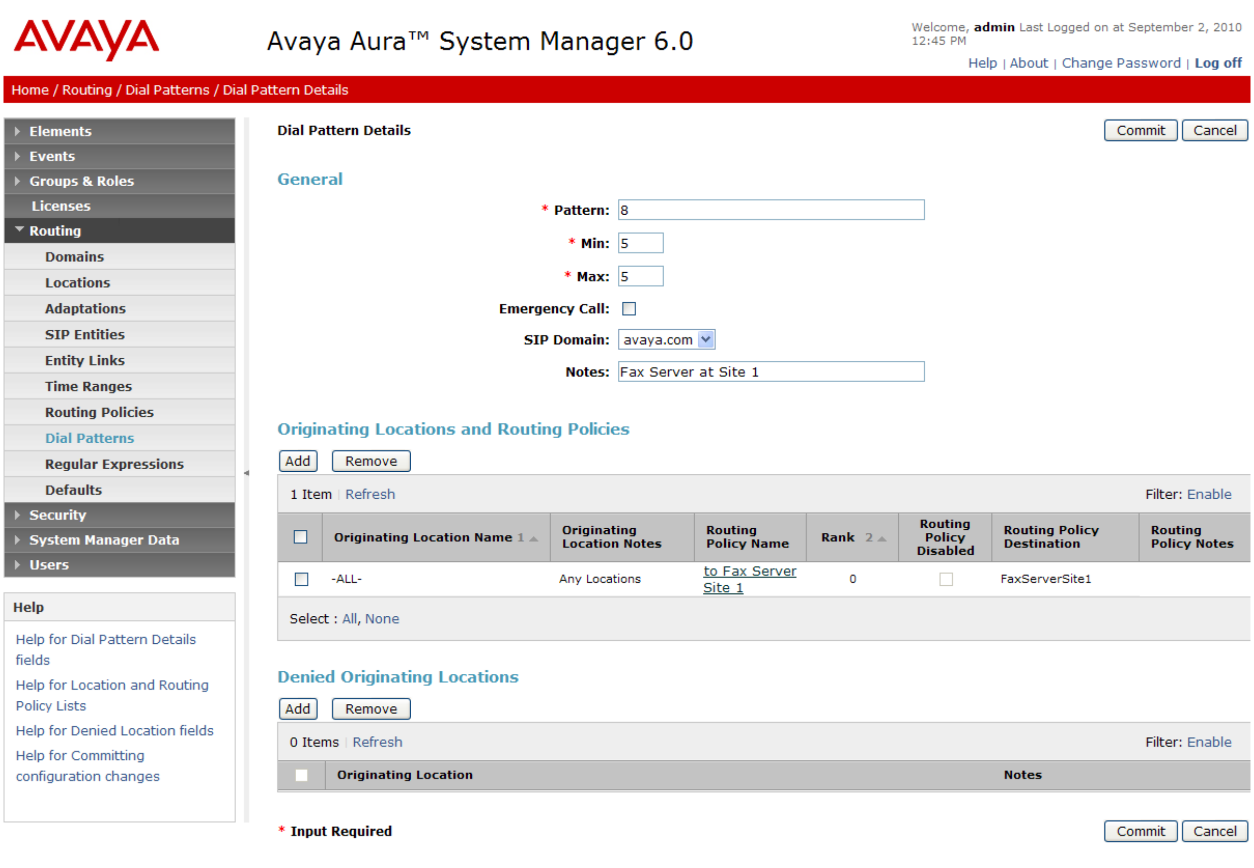
5.6. Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to the Biscom FAXCOM Server:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **Domain** SIP domain specified in **Section 5.1**
- **Notes** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.



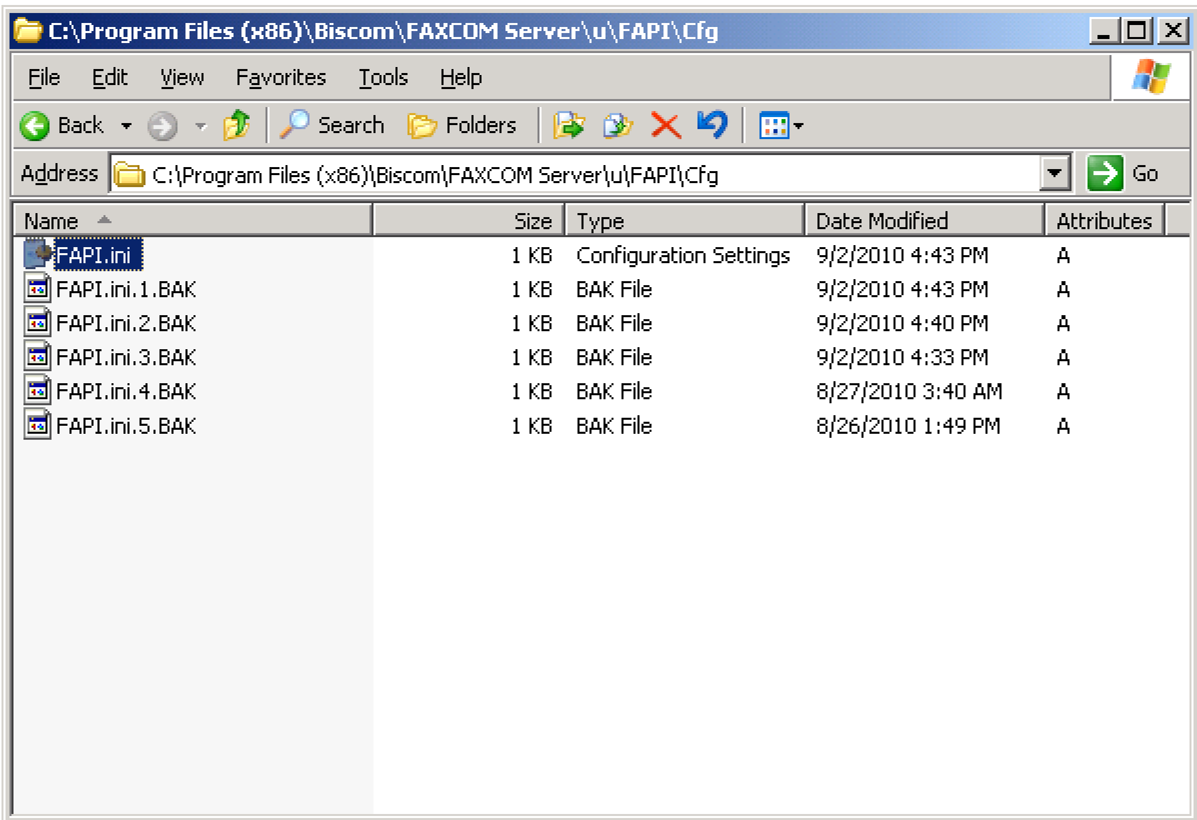
6. Configure Biscom FAXCOM Server

This section provides the procedures for configuring the Biscom FAXCOM Server. The procedures include the following areas:

- Administer FAPI.ini
- Start fax service

6.1. Administer FAPI.ini

Navigate to the **Cfg** directory to edit the **FAPI.ini** file, as shown below.



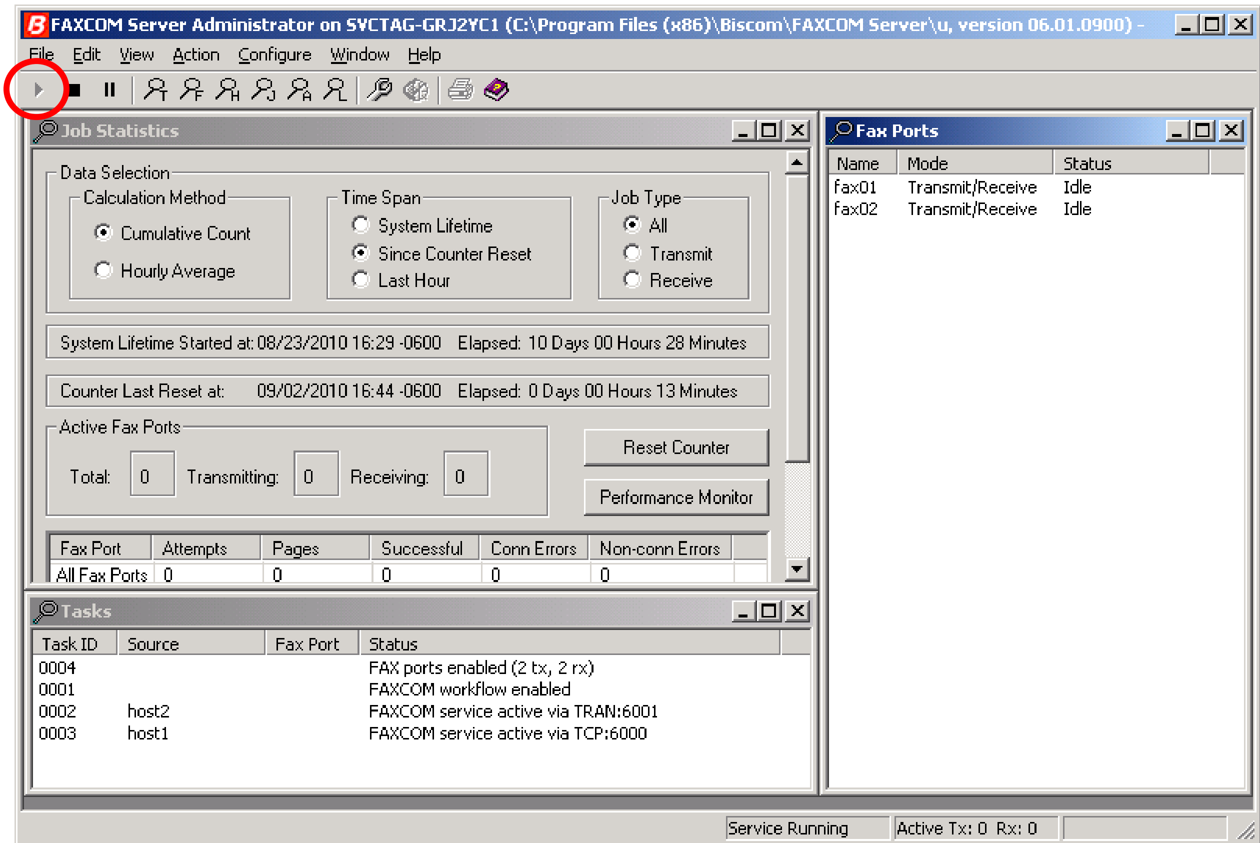
The **FAPI.ini** file contains a list of configurable parameters. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **FOIP_CALL_CONTROL:** "SIP"
- **FOIP_GATEWAY_IP_ADDRESS:** The Session Manager IP address.
- **FOIP_LOCAL_SYSTEM_IP_ADDRESS:** The local FAXCOM Server IP address.

```
#
# Cfg\FAPI.ini generated by fapiconfig, Wed Aug 25 09:39:34 2010
#
[configuration]
BOARD_COUNT                  = 1
BOARD_TYPE                   = SR140
DID_DIGITS                   = 4
FOIP_CALL_CONTROL            = SIP
FOIP_CALL_CONTROL_VARIANT    = DEFAULT
FOIP_GATEWAY_IP_ADDRESS      = 10.64.20.31
FOIP_LOCAL_SYSTEM_IP_ADDRESS = 10.64.21.100
LOG_LEVEL                    = BASIC
MAXIMUM_FAX_RESOLUTION       = 200_DPI
MODE                         = T38
SHORT_DID                    = REJECT
SR140_IP_INTERFACE           = DEFAULT
SR140_LICENSED_CHANNELS      = 2
SR140_VIRTUAL_BOARD_41_SIZE  = 2
T38_FAX_VERSION              = VERSION_0
```

6.2. Start Fax Service

From the Biscom FAXCOM Server, select **Start → All Programs → FAXCOM → FAXCOM Server Administrator**. If the service is not already running, click the "Start or Resume Service" button in the top left corner.



7. General Test Approach and Test Results

7.1. General Test Approach

The feature test cases were performed manually. Intra-site and inter-site fax calls to and from the local Biscom FAXCOM Server were made. The fax calls were sent and received by using the “Send A Test Fax” utility at the local Biscom FAXCOM Server and the analog fax machine at the Remote site. The Biscom FAXCOM Server at the remote site was used for testing simultaneous send/receive of fax calls.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cables and stop/start the fax service on the Biscom FAXCOM Server.

7.2. Test Results

All test cases were executed. The one observation noted from the compliance test is that for inter-site fax calls over the SIP trunks, the media shuffling for the SIP trunk between the two sites has to be turned off.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and the Biscom FAXCOM Server.

8.1. Verify Avaya Aura™ Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section 4.5**. Verify that the signaling group is "in-service" as indicated in the **Group State** field shown below.

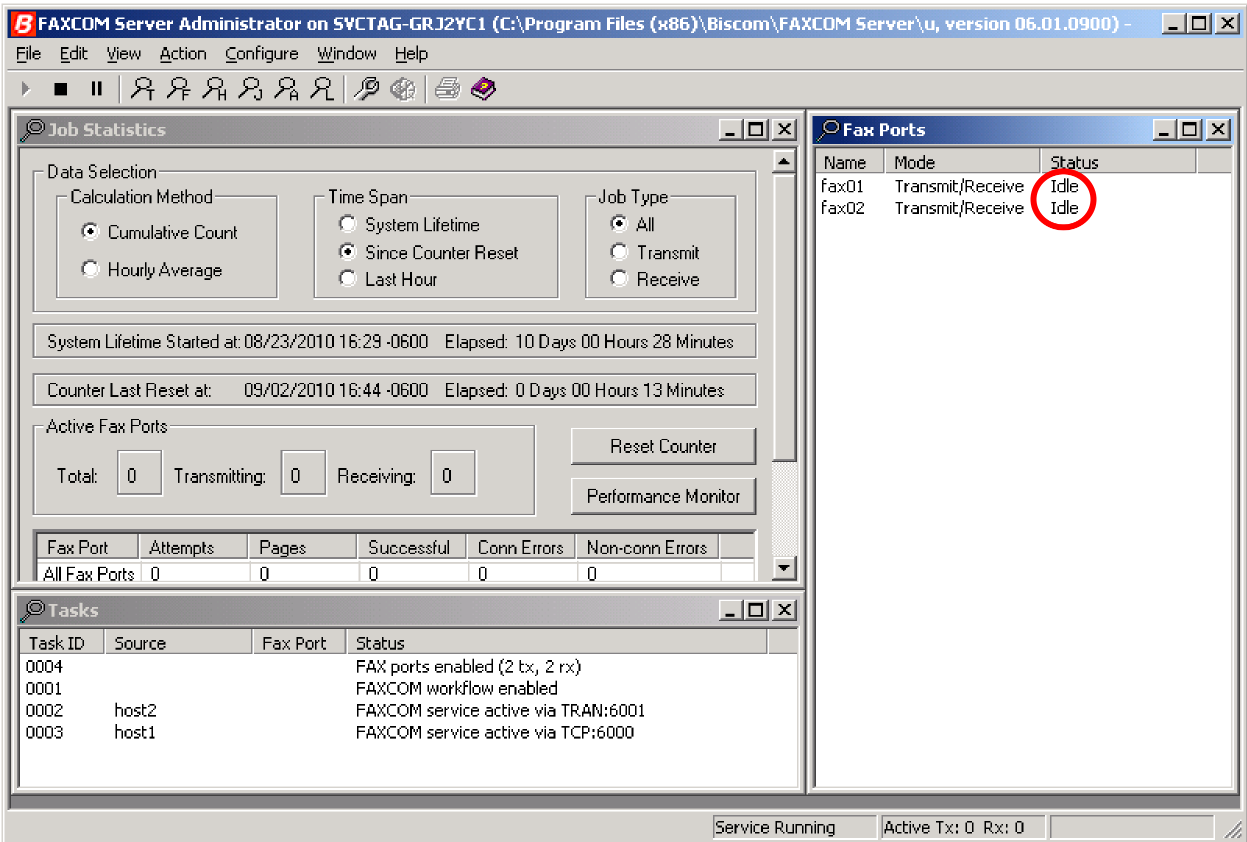
```
status signaling-group 13
                         STATUS SIGNALING GROUP

        Group ID: 13                               Active NCA-TSC Count: 0
      Group Type: h.323                             Active CA-TSC Count: 0

     Group State: in-service
```

Verify the status of the local SIP trunk group by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 4.6**. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 13                                                        Page   1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0013/001 T00377   in-service/idle    no
0013/002 T00378   in-service/idle    no
0013/003 T00379   in-service/idle    no
0013/004 T00380   in-service/idle    no
0013/005 T00381   in-service/idle    no
0013/006 T00382   in-service/idle    no
0013/007 T00383   in-service/idle    no
0013/008 T00384   in-service/idle    no
0013/009 T00385   in-service/idle    no
0013/010 T00386   in-service/idle    no
0013/011 T00387   in-service/idle    no
0013/012 T00388   in-service/idle    no
0013/013 T00389   in-service/idle    no
0013/014 T00390   in-service/idle    no
```

8.2. Verify Biscom FAXCOM Server

From the Biscom FAXCOM Server, select **Start → All Programs → FAXCOM → FAXCOM Server Administrator**. The **FAXCOM Server Administrator** screen is displayed, as shown below. Verify that the status of all configured ports is "Idle". During compliance testing, two fax ports were pre-configured on the FAXCOM Server.



9. Conclusion

These Application Notes describe the configuration steps required for Biscom FAXCOM Server to successfully interoperate with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager using SIP trunks. All feature and serviceability test cases were completed.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, August 2010, available at http://support.avaya.com.

2. *Administering Avaya Aura™ Session Manager*, Document 03-603324, Issue 3, Release 6.0, August 2010, available at http://support.avaya.com

3. *FAXCOM Server Administrator's Guide*, February 2010 Revised Edition, available from Biscom Technical Support.

4. *KB Avaya 20100518*, Knowledge Base article under "SR140 Avaya 6.x", available from Biscom Technical Support.