Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Biscom FAXCOM with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes contains interoperability instructions for configuring Biscom FAXCOM with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Compliance testing was conducted to verify the interoperability.

For this compliance testing, Biscom FAXCOM was configured to receive and send faxes over a SIP trunk connected to Avaya Aura® Session Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

Biscom has developed expertise and solutions for enterprise fax, secure file transfer,synchronization, file translation, and mobile devices for small, medium and large corporations. Biscom FAXCOM is configured to communicate with Avaya Aura® Session Manager over SIP. T.38 and G.711 protocols were used to send and receive fax calls.

2. General Test Approach and Test Results

This section details the general approach used to verify the interoperability between Biscom FAXCOM with Avaya Aura® Session Manager and Avaya Aura® Communication Manager, and the test results.

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 for 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

General test approach was to test fax calls in both an inter-site and intra-site environment. As displayed in the referenced configuration in **Figure 1**, Biscom FAXCOM was connected to Site 1, main enterprise site, and Site 2 servered as a simulated PSTN or a remote enterprise site. Inter-site calls were made over an ISDN-PRI trunk and SIP trunk between Communication Managers. Faxes were sent with various page lengths and resolution, and at various fax data speeds. SIP connectivity was tested using both UDP between Avaya Aura® Session Manager and Biscom FAXCOM. Error Correction Mode (ECM) was also tested, but please note that ECM is supported for Avaya G430 and G450 only.

2.2. Test Results

All executed test cases were passed.

2.3. Support

Biscom support is available Mon-Fri, 8:30AM-7:00PM Eastern time. Extended support hours are available via a support plan upgrade. Biscom support may be contacted by phone at (978) 250-8355, or by email at support@biscom.com.

3. Reference Configuration

Test configuration used during compliance testing consisted of the following:

- Avaya G450 Media Gateway with Avaya 8300D Media Server running Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Analog fax machines
- Biscom FAXCOM Server running on a Windows 2008 R2 server (Virtual Machine)

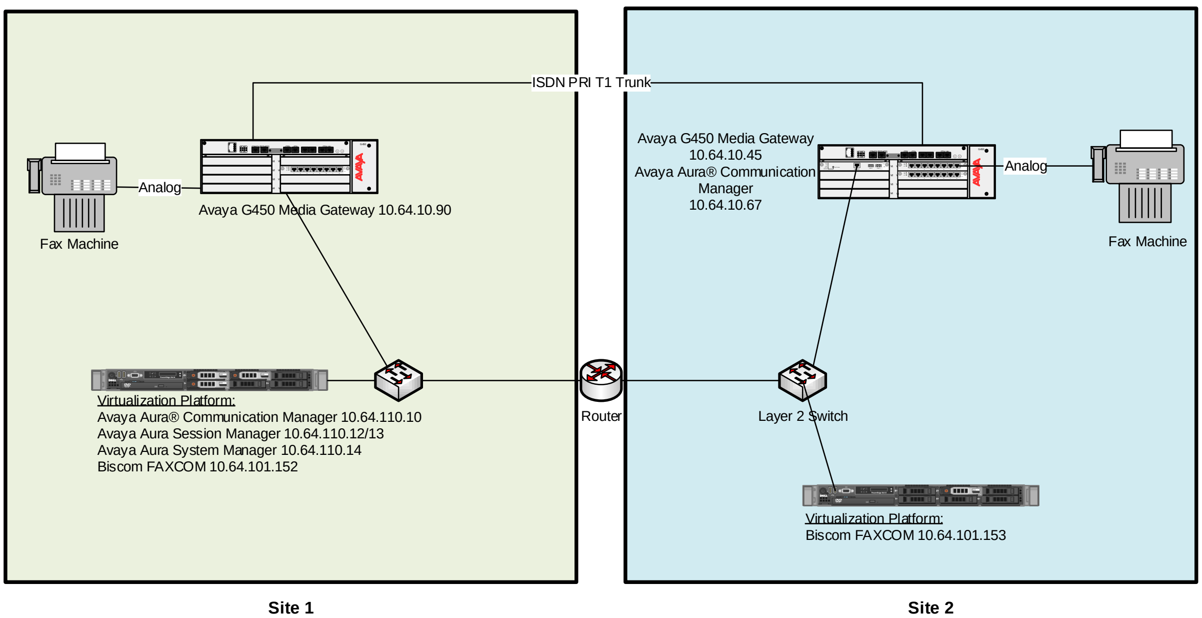


Figure 1: Reference Configuration

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	7.0 SP1
Avaya Aura® Session Manager	7.0
Avaya Aura® System Manager	7.0
Avaya G450 Media Gateway	39.18.0
Biscom FAXCOM Server	6.5.5.11
Dialogic Brooktrout SR140	6.7.2

5. Configure Avaya Aura® Communication Manager

This section provides steps for configuring Communication Manager. All configuration for Communication Manager is done through System Access Terminal (SAT).

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameters customer-options** command to verify options.

On **Page 2,** verify that there is sufficient capacity for SIP trunks by comparing **Maximum Administered SIP Trunks** field with corresponding **USED** column field.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  1
             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  45
  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
```

On **Page 4,** verify **ISDN/PRI** field is set to **y**.

```
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? y
  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
```

5.2. Administer IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where ***n*** is an existing network region.

Configure this network region as follows:

- Set **Location** to **1**.
- Set **Codec Set** to **1**.
- Set **Intra-region IP-IP Direct Audio** to **yes**.
- Set **Inter-region IP-IP Direct Audio** to **yes**.
- Enter an **Authoritative Domain**, e.g., avaya.com.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main                  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.3. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where ***n*** is an existing codec set number.

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1** to **G.711MU**.

```
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:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1:
 2:
 3:
```

On **Page 2**:

- Set **Fax Mode** to **t.38-standard**.
- Set **ECM** to **y**.

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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? n



                                                                    Packet
                          Mode                    Redundancy        Size(ms)
    FAX                   t.38-standard            0         ECM: y
    Modem                 off                      0
    TDD/TTY               US                       3
    H.323 Clear-channel   n                        0
    SIP 64K Data          n                        0                 20
```

5.4. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, a**sm** and **biscom** with IP Address of **10.64.110.13** and **10.64.101.152,** respectively, entries were added.

```
change node-names ip
                                    IP NODE NAMES
    Name              IP Address
acms                10.64.110.18
aes                 10.64.110.15
ams                 10.64.110.16
asm                 10.64.110.13
biscom              10.64.101.152
default             0.0.0.0
procr               10.64.110.10
```

5.5. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number.

Configure this signaling group as follows:

- Set **Group Type** to **sip**.
- Set **Near-end Node Name** to **procr.**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.4**, i.e., **asm**.
- Set **Far-end Network region** to the configured region in **Section 5.2**, i.e., **1**.
- Specify a **Far-end Domain,** e.g., **avaya.com**.

```
add signaling-group 1                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP 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
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: asm
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                        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
```

Note: Signaling Group, Trunk Group, and Route Pattern for simulated PSTN calls for inter-site calls over ISDN/PRI and SIP were pre-configured and are not shown in this document.

5.6. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where ***n*** is an available trunk group number.

Configure this trunk group as follows on **Page 1**:

- Set **Group Type** to **sip**.
- Specify a **Group Name**, e.g., **asm**.
- Specify a valid **TAC**, e.g., **101**.
- Set **Service Type** to **tie**.
- Set **Member Assignment Method** to **auto**.
- Specify the **Signaling Group** value as the signaling group configured in **Section 5.5**, i.e., **1**.
- Specify an appropriate number in the **Number of Member** field.

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: asm                        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: 10
```

On **Page 3**:

- Set **Number Format** to private.

```
add trunk-group 1                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                     Maintenance Tests? y



                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

5.7. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where ***n*** is an available route pattern.

Configure this route pattern as follows:

- Specify a name in the **Pattern Name** field.
- For line 1, set **Grp No** to the trunk group configured in **Section 5.6**, i.e., **1**.
- For line 1, set **FRL** to **0**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Voice and Fax
                             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
```

5.8. Administer Private Numbering

Use the **change private-numbering 0** command to define the calling party number to send to Session Manager.

Configure private numbering as follows:

- Add entries for trunk group configured in **Section 5.6**.

```
change private-numbering 0                                      Page   1 of   2

                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  1                                            5     Total Administered: 3
 11 1                                            11       Maximum Entries: 540
```

5.9. Administer AAR Analysis

Use the **change aar analysis *n*** command to configure routing for extensions starting with ***n***. Add two entries, one for voice and fax calls, and another one for modem calls. For compliance testing, extension 11111 was used for routing calls to FAXCOM.

- Set **Dialed String** to the starting digits of extensions to be used, e.g., **1**.
- Set **Min** and **Max** to **5** for 5-digit extensions.
- Set **Route Pattern** to the pattern configured in **Section 5.7**, i.e., 1.
- Set **Call Type** to **aar**.

Note: An entry must be added to the dial plan for the extension range used in this step.

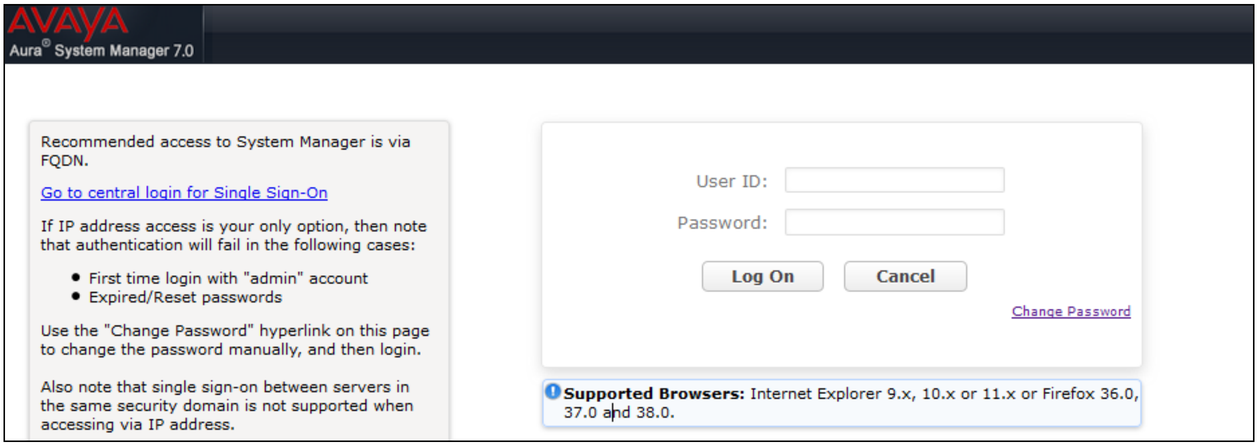
```
change aar analysis 1                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    11111                 5    5     1        aar          n
```

5.10. Administer Stations

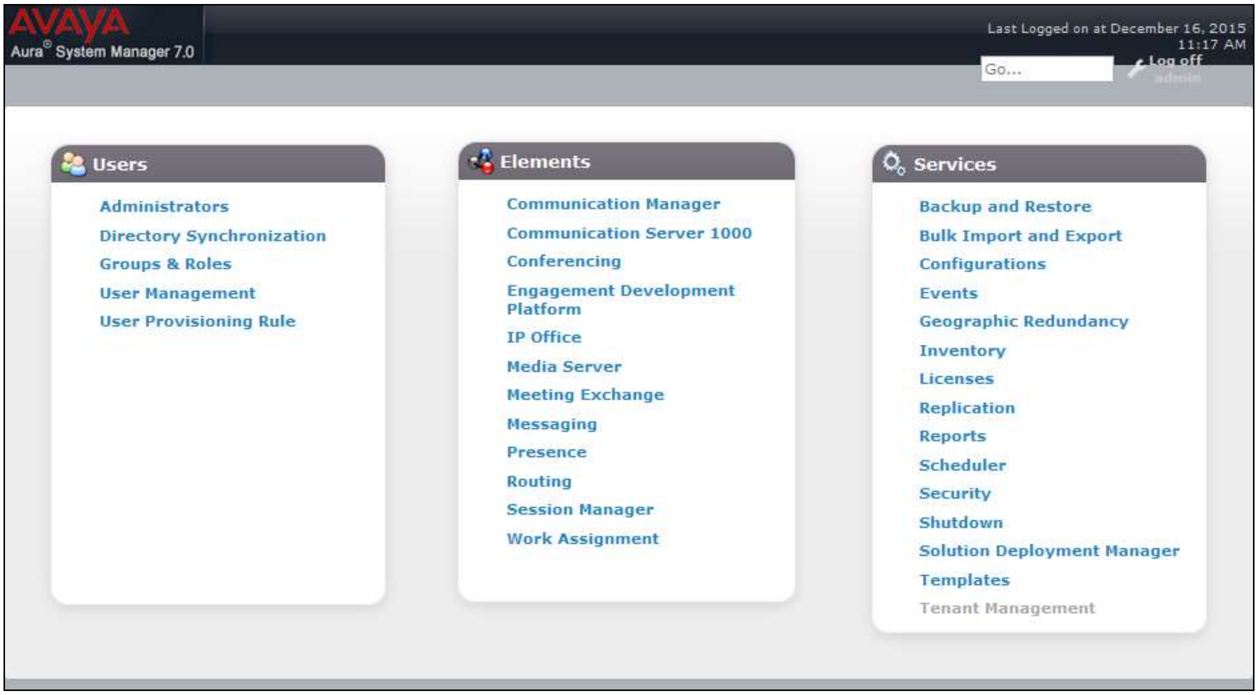
Administration of Avaya Stations/Extensions in Communication Manager and Session Manager is not shown in this document. Please refer to **[1]** and/or **[2]** in References section.

6. Configure Avaya Aura® Session Manager

Configuration of Avaya Aura® Session Manager is performed via Avaya Aura® System Manager. Access the System Manager administration Web interface, enter the https://<*ip-address*>/SMGR URL in a Web browser, where <*ip-address*> is the IP address of System Manager.



Log in using appropriate credentials.

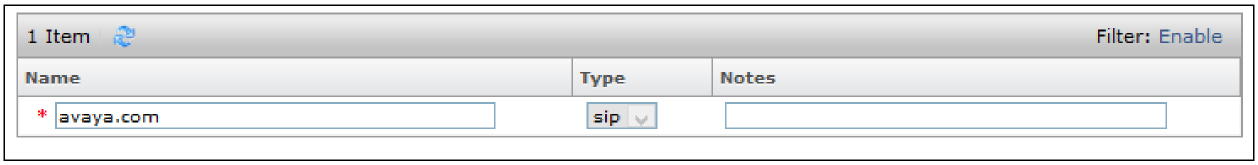


6.1. Add SIP Domain

Navigate to **Home → Elements → Routing → Domains**, click the **New** button (not shown) and configure as follows:

- In the **Name** field specify a domain (authoritative domain used in **Section 5**) i.e., **avaya.com**.
- Set **Type** to **sip**.

Click **Commit** to save changes.



6.2. Add Location

Navigate to **Home → Elements → Routing → Location**, click the **New** button (not shown), and configure as follows:

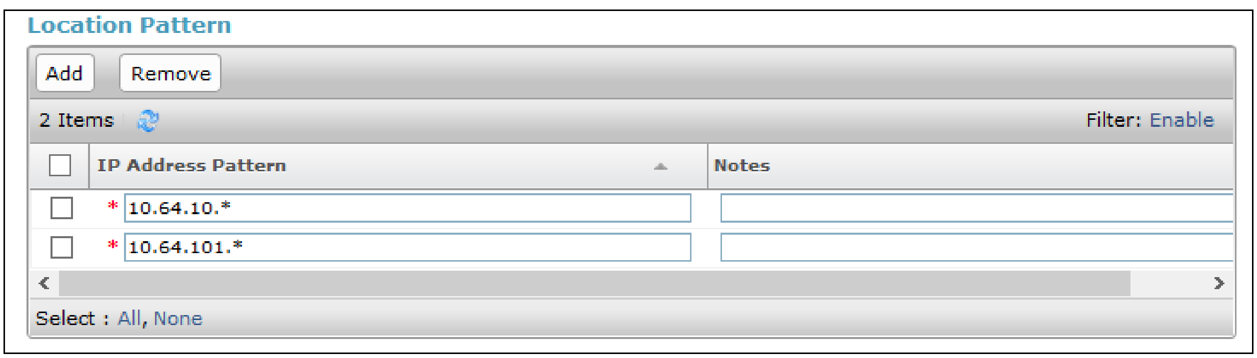
Under **General**:

- Specify a descriptive **Name** (not shown).

Under **Location Pattern** click **Add**:

- Specify an **IP Address Pattern**, e.g.,10.64.10.*

Click **Commit** to save changes.



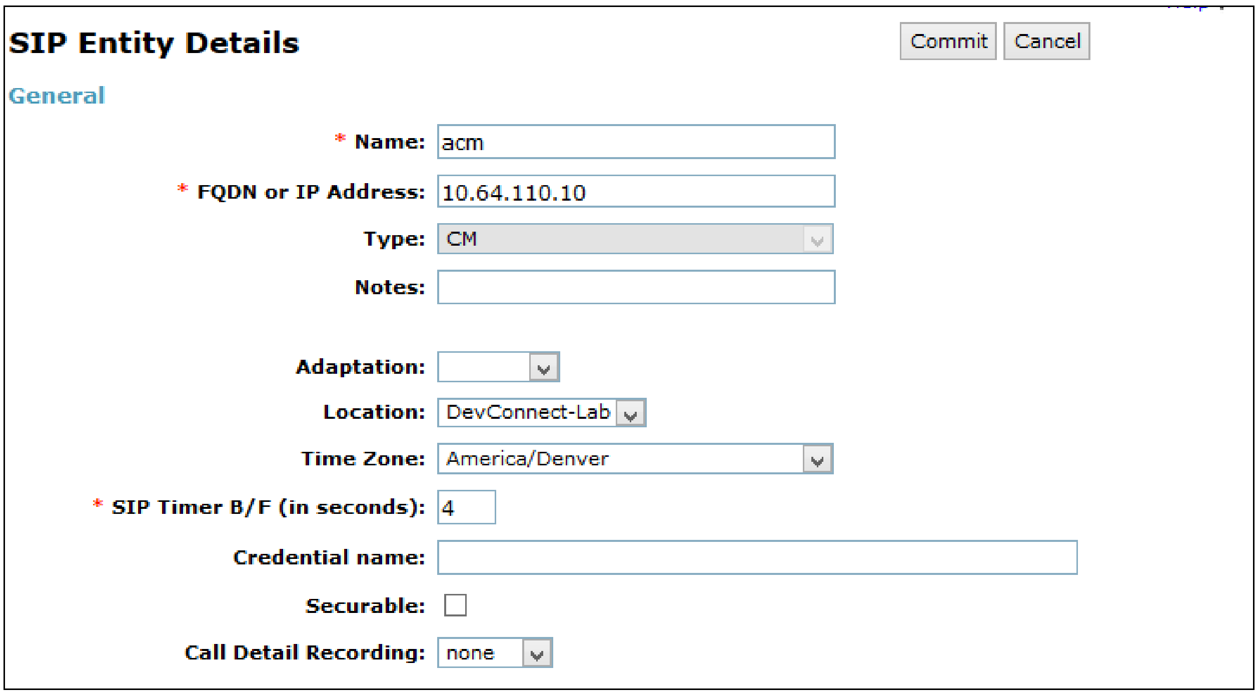
6.3. Add SIP Entity – Communication Manager

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field.
- Specify the IP address or FQDN of Communication Manager in the **FQDN or IP Address** field.
- Set **Type** to **CM.**
- Set **Location** to the location configured in **Section 6.2**.

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has already been configured.

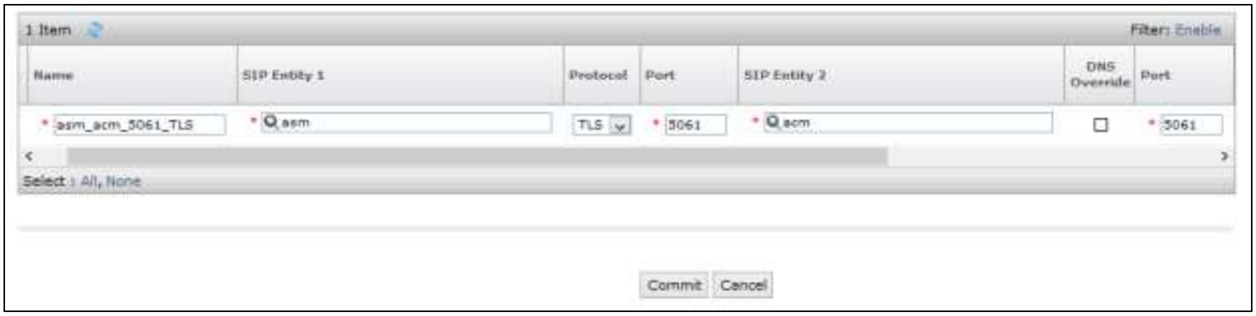


6.4. Add Entity Link – Communication Manager

Navigate to **Home → Elements → Routing → Entity Links**, click **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity.
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.3**.

Click **Commit** to save changes.



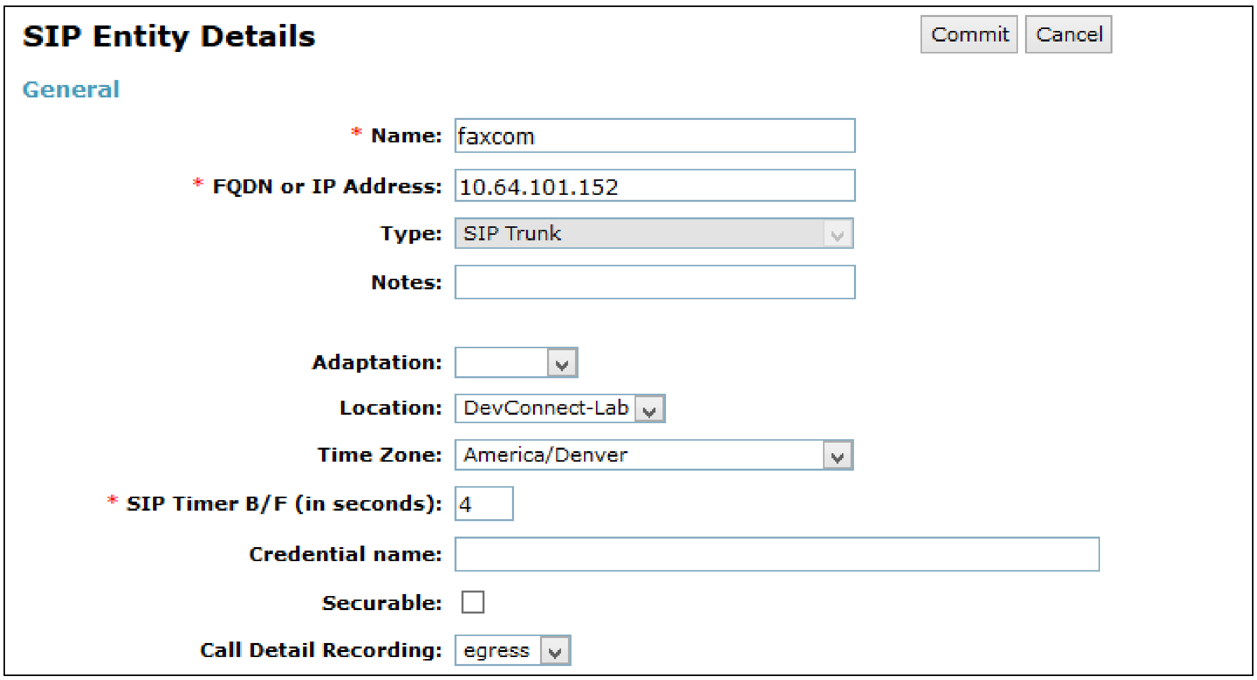
6.5. Add SIP Entity – FAXCOM

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field.
- Specify the IP address or FQDN of FAXCOM in the **FQDN or IP Address** field.
- Set **Type** to **SIP Trunk**.
- Set **Location** to the location configured in **Section 6.2**.

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has already been configured.

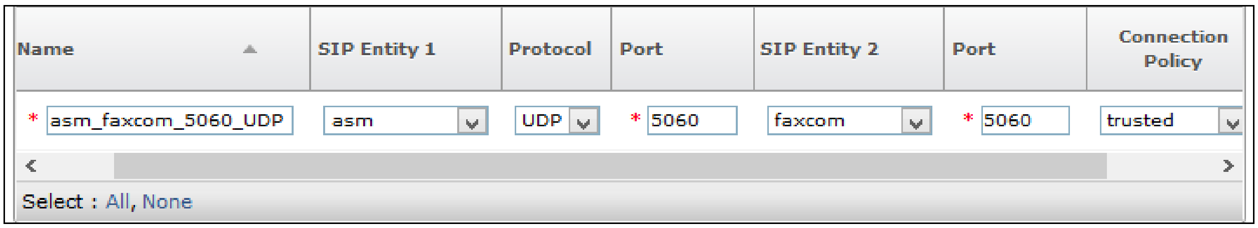


6.6. Add Entity Link – FAXCOM

Navigate to **Home → Elements → Routing → Entity Links**, click **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field.
- Set **SIP Entity 1** to the name of Session Manager SIP Entity.
- Set **SIP Entity 2** to FAXCOM SIP Entity configured in **Section 6.5**.
- Set **Protocol** to **UDP**.

Click **Commit** to save changes.

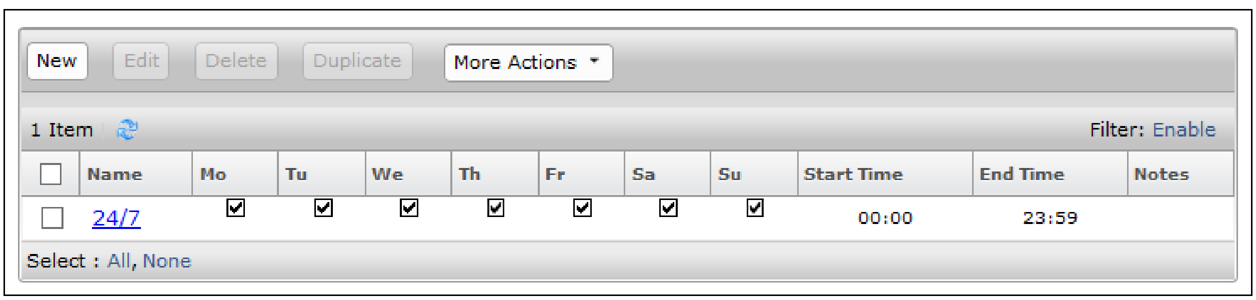


6.7. Add Time Ranges

Navigate to **Home → Elements → Routing → Time Ranges**, click **New** (now shown), and configure as follows:

- Specify a descriptive name in the **Name** field

Click **Commit** to save changes.

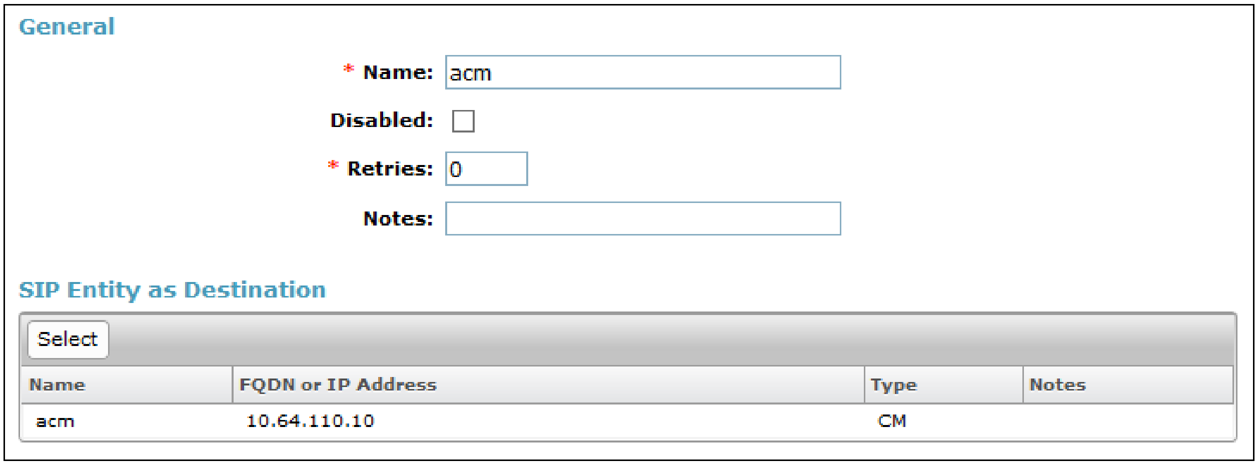


6.8. Add Routing Policy – Communication Manager

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select** (not shown):
    - Select Communication Manager SIP entity added in **Section 6.3**.

Click **Commit** to save changes.

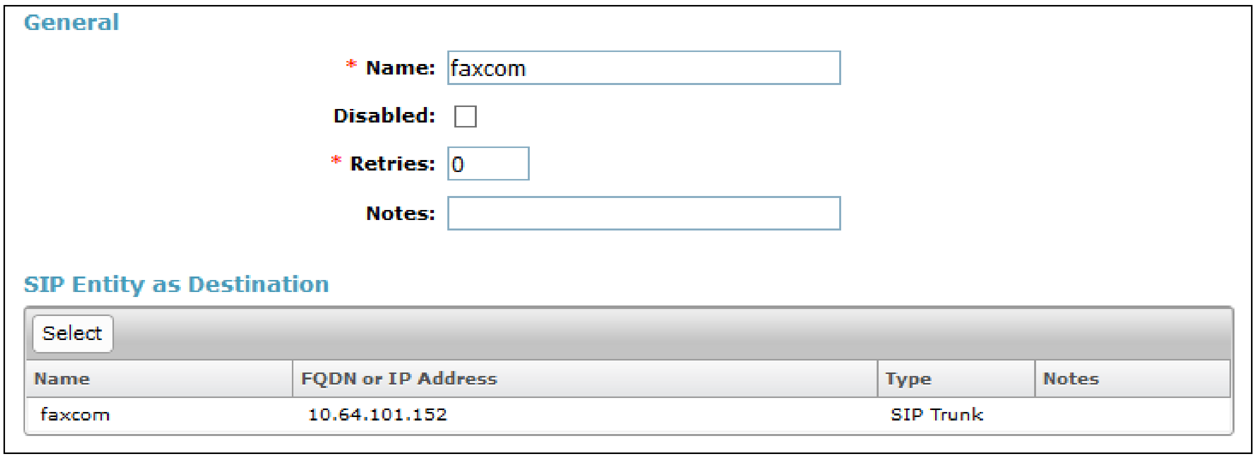


6.9. Add Routing Policy – FAXCOM

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown), and configure as follows:

- Specify a descriptive name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select** (not shown).
  - Select FAXCOM SIP entity added in **Section 6.5**.
- Under **Time of Day**, click **Add** (not shown).
  - Select time range added in previous step.

Click **Commit** to save changes.



6.10. Add Dial Patterns – Communication Manager

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown), and configure as follows:

Under **General:**

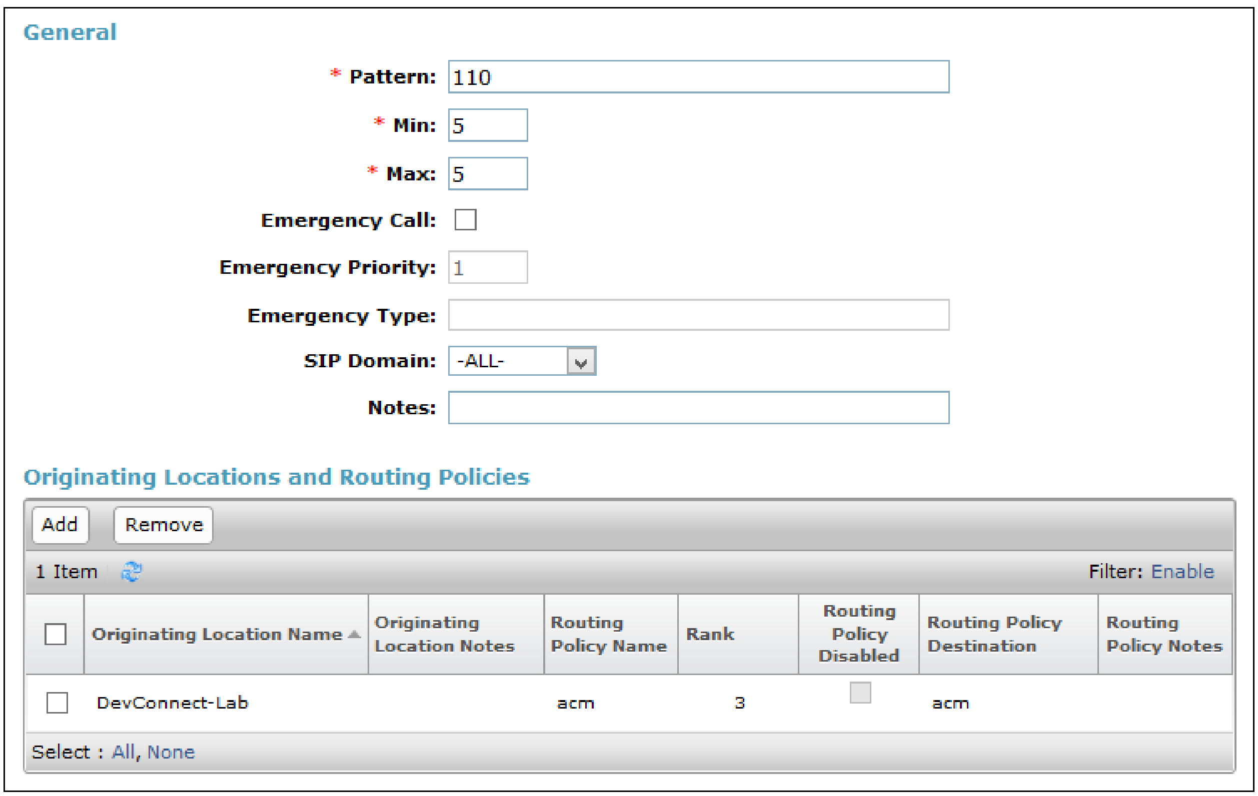
- Set **Pattern** to prefix of dialed number.
- Set **Min** to minimum length of dialed number.
- Set **Max** to maximum length of dialed number.

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and Communication Manager routing policy as configured in **Section 6.8**.

Click **Commit** to save changes.

Note: For compliance testing, the dialed number of 110XX was used to route calls to Communication Manager. The Pattern, Min and Max values were, therefore, all set to **5**.



6.11. Add Dial Patterns – FAXCOM

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown), and configure as follows:

Under **General:**

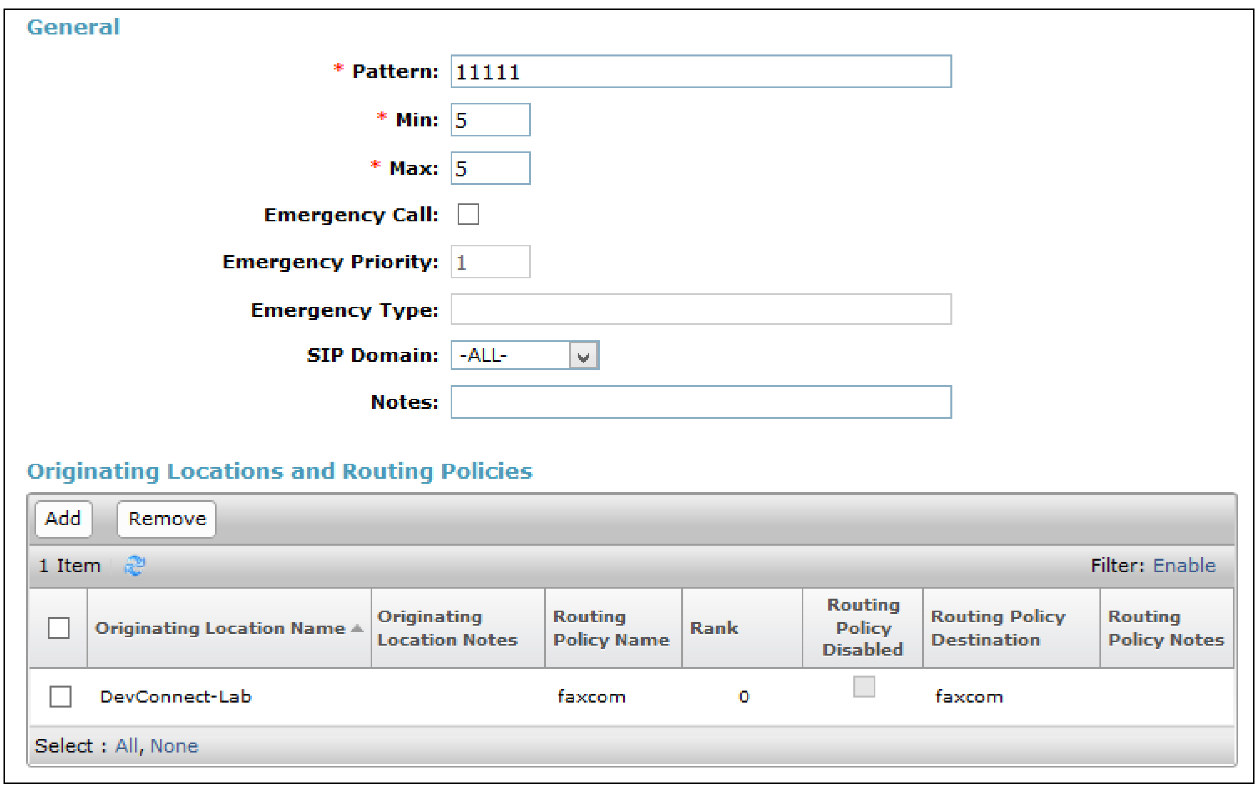
- Set **Pattern** to prefix of dialed number.
- Set **Min** to minimum length of dialed number.
- Set **Max** to maximum length of dialed number.
- Set SIP **Domain** to **–All-**.

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and FAXCOM routing policy as configured in **Section 6.9**.

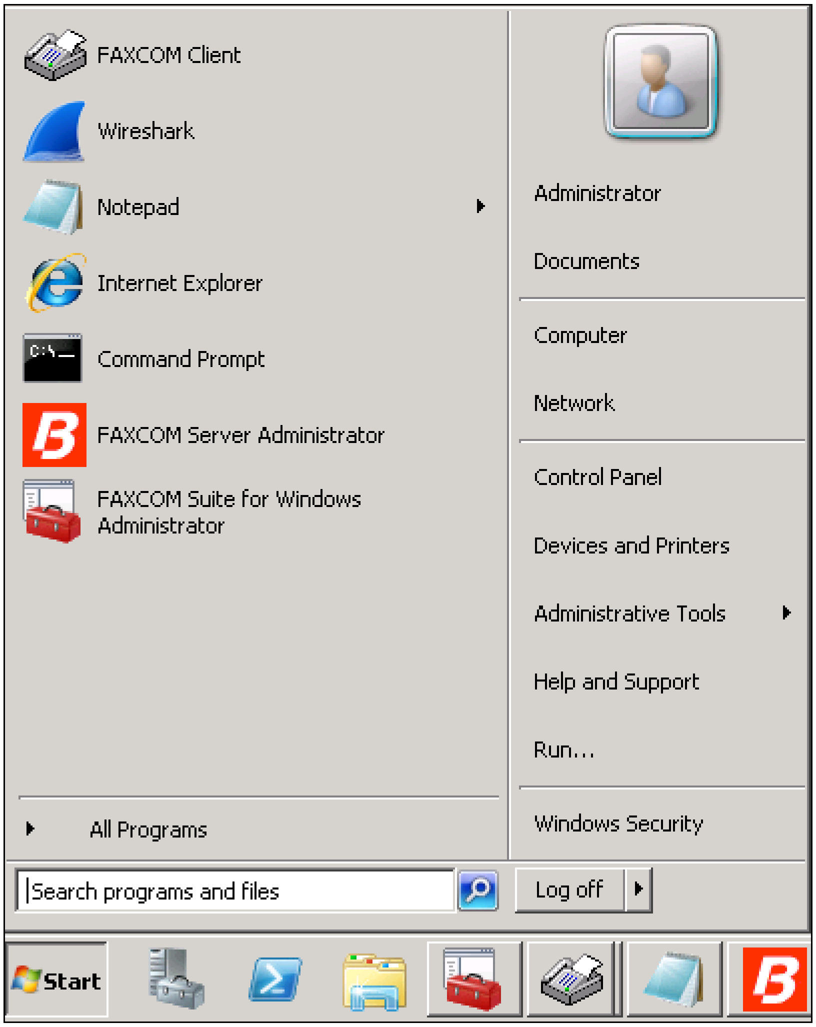
Click **Commit** to save changes.

Note: For compliance testing, the dialed number of 11111 was used to route calls to FAXCOM. The Pattern, Min and Max values were, therefore, all set to **5**.

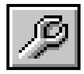


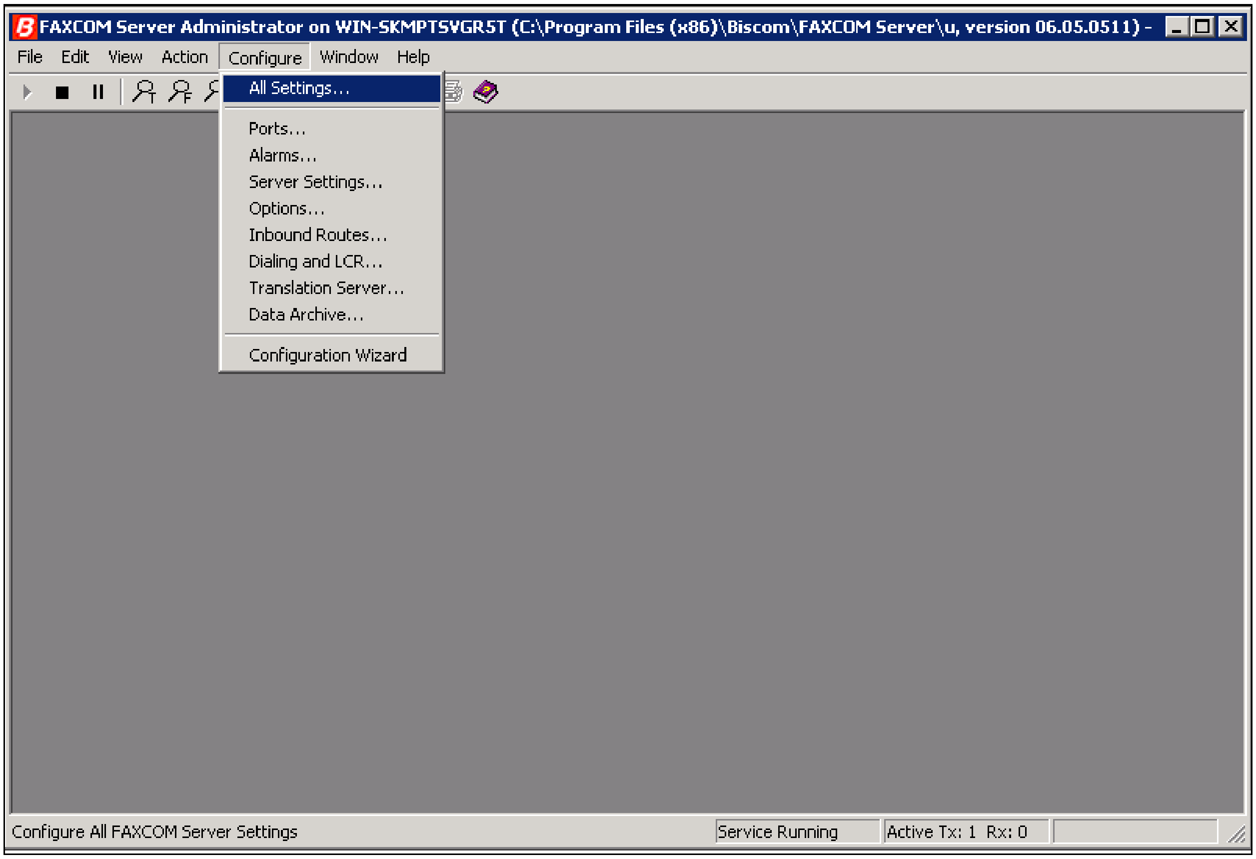
7. Configure FAXCOM

From the Biscom fax server, launch the **Biscom FAXCOM Server Administrator** application.



Select **Configure… All Settings**.

Note: Alternatively, click the Configure toolbar button  to display the **Configure All Settings** dialog.

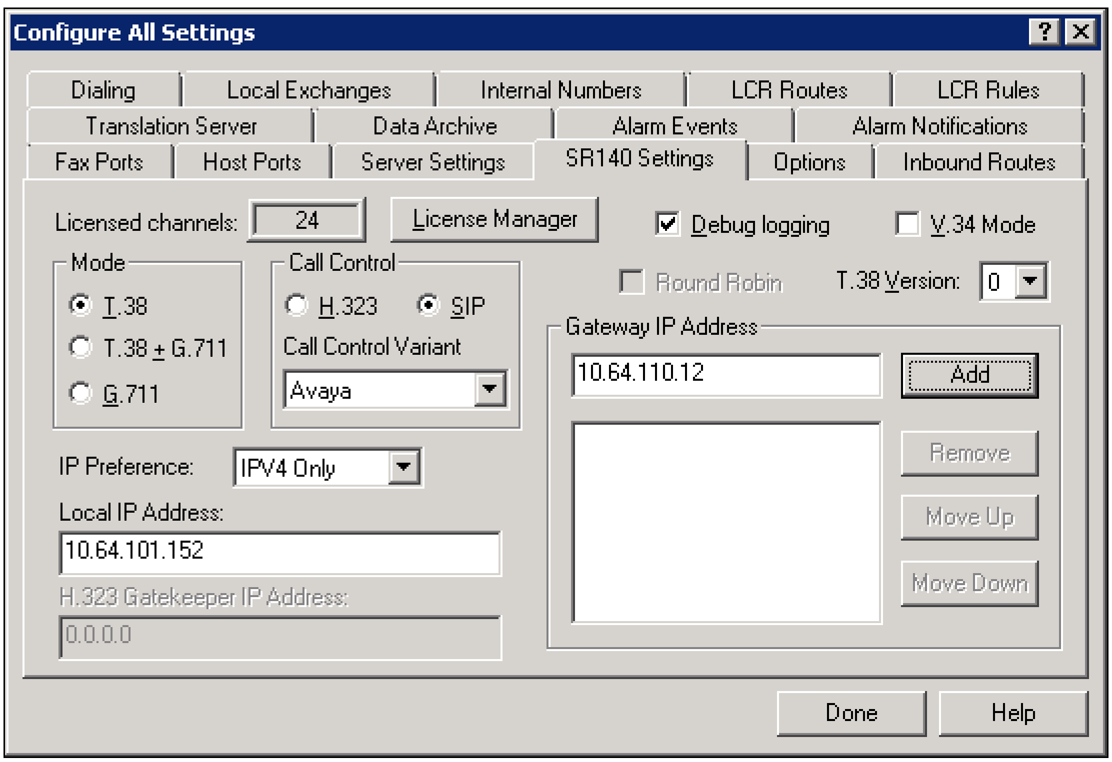


Select the **SR140 Settings** tab to configure the Dialogic SR140 fax over IP software license (which is the actual direct interface to the Avaya) as follows:

- Uncheck **Debug logging** and **V.34 Mode** check boxes.
- Set **T.38 Version** to **0** from the drop down menu.
- Set **Mode** to **T.38**.
- Set **Call Control** to **SIP**.
  - Set **Call Control Variant** to **Avaya** from the drop down menu.
- In the **Local IP Address** field, specify the IP address of the fax server.
- In the **Gateway IP Address** field, specify the IP address of Session Manager; then click the **Add** button.

Once the values are configured, click **Done**. When prompted to restart the FAXCOM service in order for the values to take effect, click restart the service now or later (not shown).

Note that the screen capture below shows **Debug Logging** checked, but in a production environment, uncheck the box.



8. Verification Steps

8.1. Avaya Aura® Session Manager

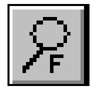
From the System Manager Web page, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Under the **All Monitoring SIP Entities**, select the FAXCOM SIP entity that was configured in this document (not shown).

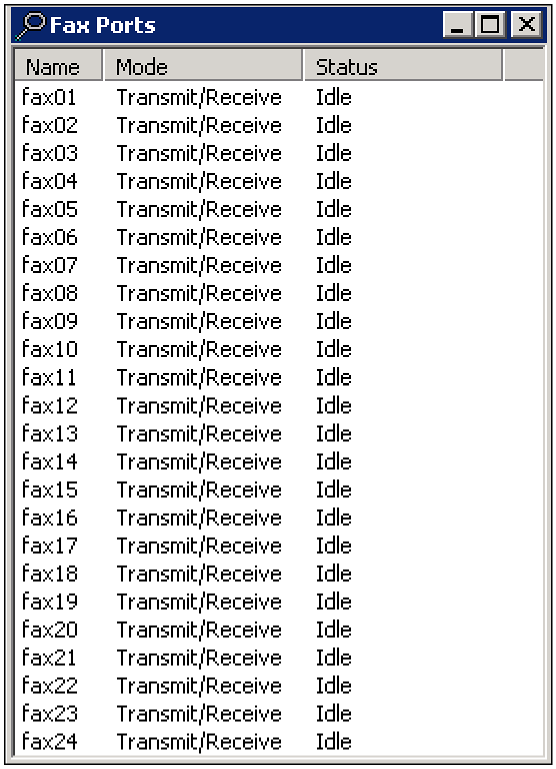
Ensure that **Conn. Status** is **UP**, and **Reason Code** is **200 OK** in order to verify that the connection between Session Manager and Biscom Server is successful.

1 Items | Refresh Filter: Enable

	Session Manager	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
	asm	10.64.101.1	5060	UDP	FALSE	UP	200 OK	UP

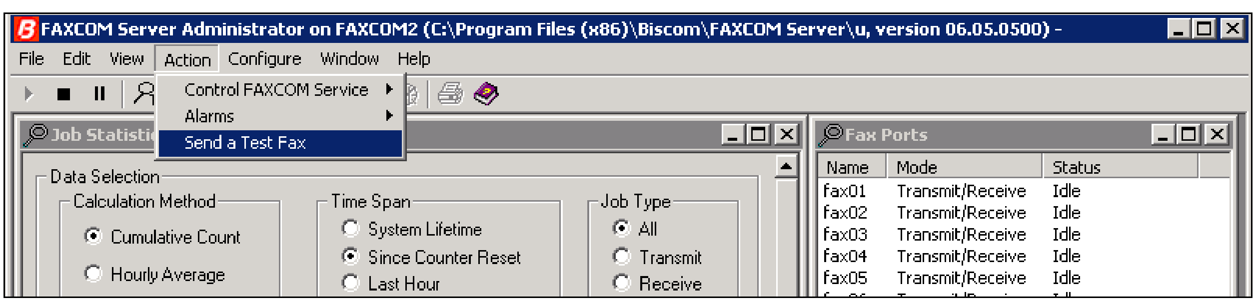
8.2. FAXCOM

From the FAXCOM Server Administrator application, click  **(or select View…Fax Ports) to display a list of** all licensed fax ports, with each port's status. All ports should be in **idle** state.



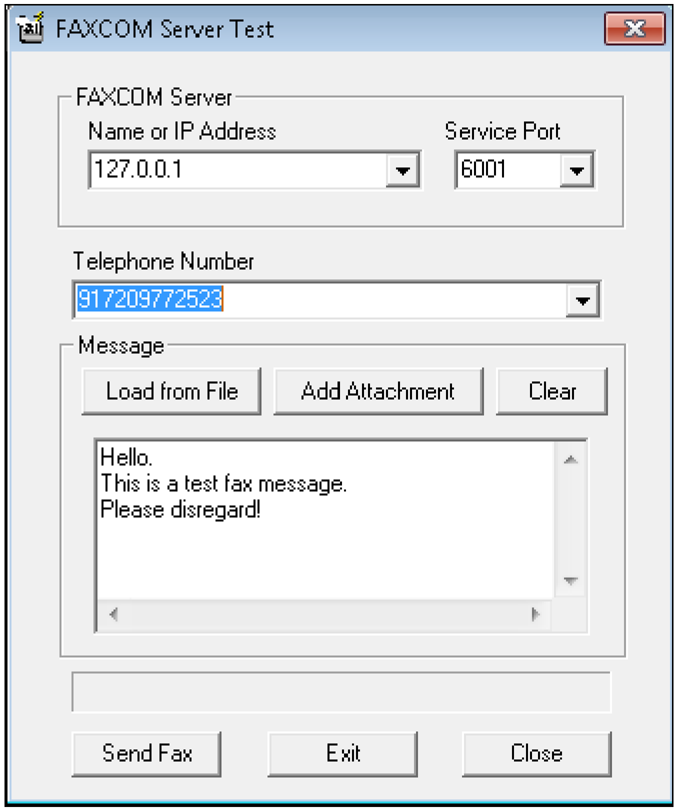
Name	Mode	Status
fax01	Transmit/Receive	Idle
fax02	Transmit/Receive	Idle
fax03	Transmit/Receive	Idle
fax04	Transmit/Receive	Idle
fax05	Transmit/Receive	Idle
fax06	Transmit/Receive	Idle
fax07	Transmit/Receive	Idle
fax08	Transmit/Receive	Idle
fax09	Transmit/Receive	Idle
fax10	Transmit/Receive	Idle
fax11	Transmit/Receive	Idle
fax12	Transmit/Receive	Idle
fax13	Transmit/Receive	Idle
fax14	Transmit/Receive	Idle
fax15	Transmit/Receive	Idle
fax16	Transmit/Receive	Idle
fax17	Transmit/Receive	Idle
fax18	Transmit/Receive	Idle
fax19	Transmit/Receive	Idle
fax20	Transmit/Receive	Idle
fax21	Transmit/Receive	Idle
fax22	Transmit/Receive	Idle
fax23	Transmit/Receive	Idle
fax24	Transmit/Receive	Idle

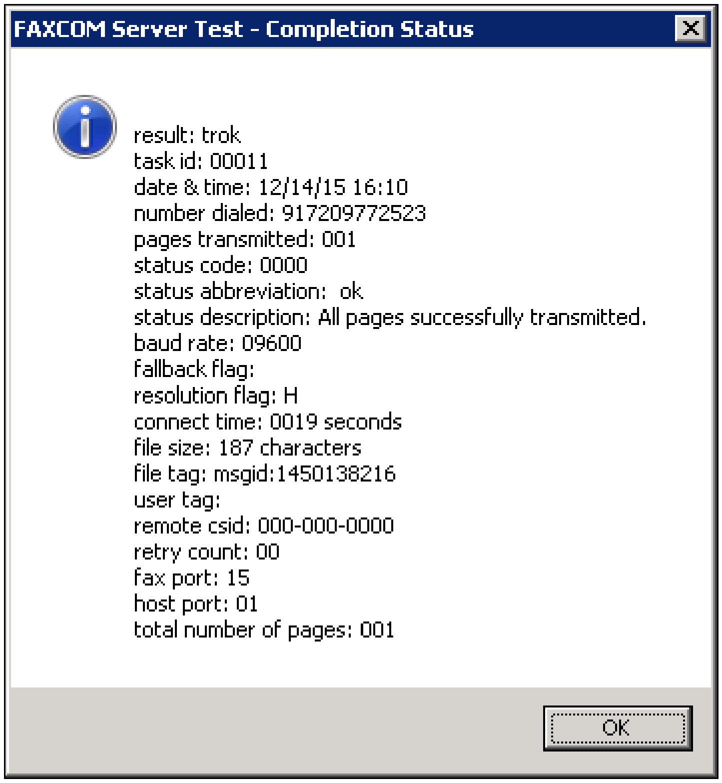
To check connectivity, do the following to send a test fax.
From the FAXCOM Server Administrator application select **Action…Send a Test Fax**.



Configure the **FAXCOM Server Test** dialog as follows:

- Leave the **FAXCOM Server: Name or IP Address** field default of 127.0.0.1 unchanged. Specify 6001 in the **FAXCOM Server: Service Port** field.
- In the **Telephone Number** field, specify the phone number of a fax device (including the necessary prefix if sending to an external number).
- In the **Message** box, leave or replace the sample text.
  Click the **Send Fax** button to send a one-page test fax to Communication Manager. If successful, the Completion Status returned will display **result:trok**, as shown in the example on next page.




FAXCOM Server Test - Completion Status
result: trok
task id: 00011
date & time: 12/14/15 16:10
number dialed: 917209772523
pages transmitted: 001
status code: 0000
status abbreviation: ok
status description: All pages successfully transmitted.
baud rate: 09600
fallback flag:
resolution flag: H
connect time: 0019 seconds
file size: 187 characters
file tag: msgid:1450138216
user tag:
remote csid: 000-000-0000
retry count: 00
fax port: 15
host port: 01
total number of pages: 001
OK

9. Conclusion

Compliance testing has verified the interoperability of Biscom FAXCOM with Avaya Aura® Session Manager and Avaya Aura® Communication Manager, and these Application Notes explain the procedures required to implement the interoperability (as depicted in **Figure 1**).

10. Additional References

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

[1] *Administering Avaya Aura® Session Manager, Release 7.0,* August 2015
[2] *Administering Avaya Aura® Communication Manager, Release 7.0,* Document 03-300509, August 2015

Product documentation for Biscom products may be obtained directly from Biscom.

[3] *FAXCOM Server Administrator's Guide*, October 2015 Revised Edition, © Biscom, Inc., 1995-2015

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.