



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.

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 around enterprise fax, secure file transfer, synchronization, file translation, and mobile devices for small, medium and large corporation. Biscom FAXCOM is configured to communicate with Avaya Aura® Session Manager using SIP. T.38 Protocol was 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 and 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 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 an inter-site and intra-site environment. As displayed in the reference configuration, Biscom FAXCOM was connected to Site 1, main enterprise site, and site 2 servers 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, resolution and at various fax data speeds. SIP connectivity was tested using both TCP and UDP between Avaya Aura® Session Manager and Biscom FAXCOM. Error Correction Mode (ECM) was also tested, but please note that ECM is only supported for Avaya G430 and G450.

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 zone. 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 following:

- Avaya G430 Media Gateway with Avaya 8300D Media Server running Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya G650 Media Gateway
- Analog Fax Machines
- Biscom FAXCOM Server running on a Windows 2008 R2 server (Virtual Machine)

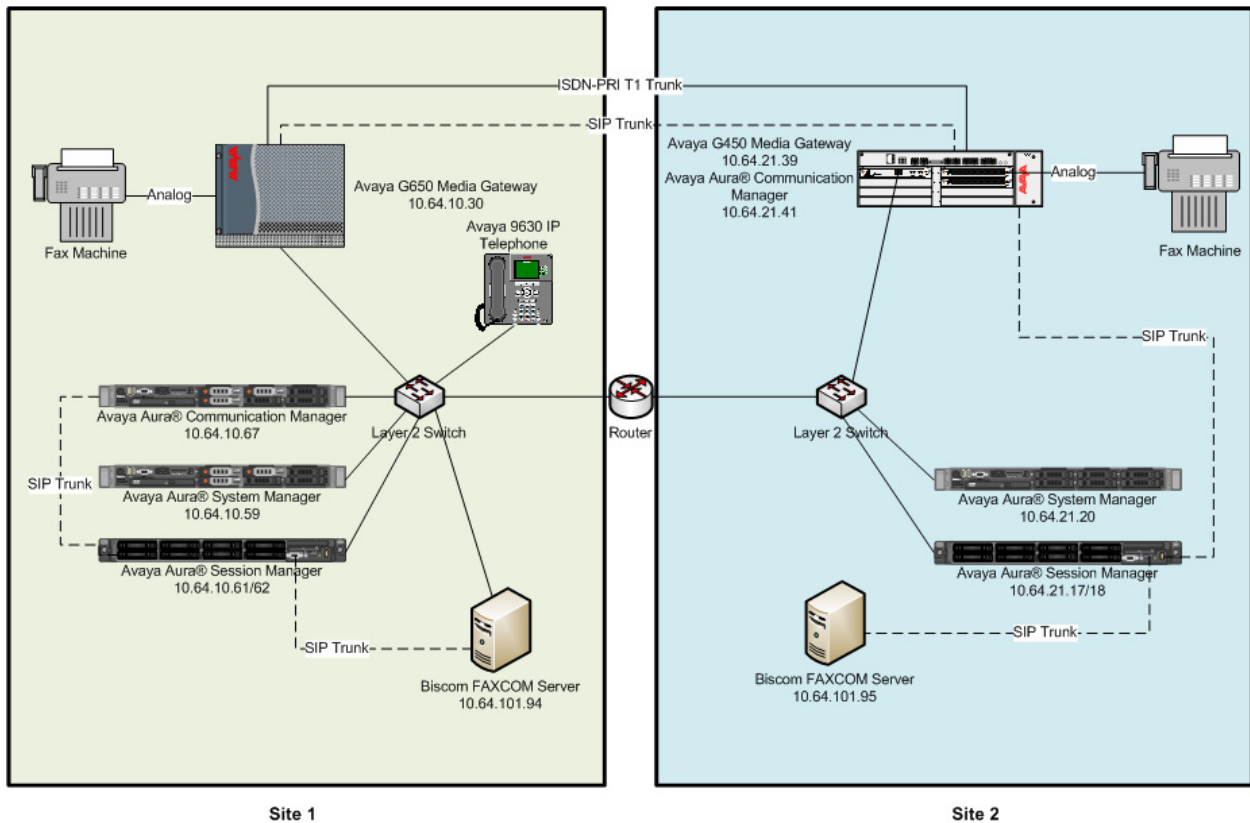


Figure: Reference Configuration

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 running on Avaya S8300D Server	R016x.03.0.124.0
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Aura® System Manager	6.3.2.4.1399
Avaya G450 Media Gateway	33.13.0
Biscom FAXCOM Server	6.5.5.0
Dialogic Brooktrout SR140	Brooktrout SDK 6.6.1

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
  Global Call Classification? y
  Hospitality (Basic)? 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 and **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:
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
```

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? y
                                Maximum Call Rate for Direct-IP Multimedia: 2048:Kbits
                                Maximum Call Rate for Priority Direct-IP Multimedia: 2048:Kbits

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

```

5.4. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm** and **10.64.10.62** entry was added.

```

change node-names ip                                     Page 1 of 2

                                IP NODE NAMES

Name          IP Address
default       0.0.0.0
msgsrvr       10.64.10.67
procr         10.64.10.67
procr6        ::
sm          10.64.10.62

```

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., **sm**
- Set **Far-end Network region** to the configured region in **Section 5.2**, i.e., **1**
- Enter a **Far-end Domain**, e.g., **avaya.com**
- Set **Direct IP-IP Audio Connections** to **n**

```
add 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? n                                    Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: Others

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

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate            Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                       RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3              Direct IP-IP Audio Connections? n
Enable Layer 3 Test? y                          IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n         Initial IP-IP 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**
- Enter a **Group Name**, e.g., **SM**
- Enter a valid **TAC**, e.g., ***001**
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.5**, i.e., **1**
- Enter a desired number in **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: SM                                     COR: 1                  TN: 1          TAC: *001
  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: 25

```

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
                                                UII 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 patterns.

Configure this route pattern as follows:

- Type a name in **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
      1: 1    0                               Dgts      Intw
      2:                                     n        user
                                               n        user

```

5.8. Administer Private Numbering

Use the **change private-numbering 1** 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**

Note: For compliance testing, 10-digit extensions beginning with 552 routed over trunk groups 1 resulted in a 10-digit calling party number.

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

Ext  Ext      Trk      Private      Total
Len  Code      Grp(s)    Prefix      Len
10  552        1
Total Administered: 1
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, extensions starting with 552 were used for routing calls to FAXCOM.

- Set **Dialed String** to starting digits of extensions that will be used, e.g., 29
- Set **Min** and **Max** to 10 for 10 digit extensions
- Set **Route Pattern** to pattern configured in **Section 5.7**, i.e., 1
- Set **Call Type** to **aar**

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

```
change aar analysis 552
AAR DIGIT ANALYSIS TABLE
Location: all
Percent Full: 1

Dialed      Total      Route      Call      Node      ANI
String      Min  Max  Pattern  Type      Num      Reqd
552         10  10    1       aar          n
588         5   5     10      aar          n
60          4   4     30      aar          n
602         4   4     10      aar          n
605         4   4     30      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 document [1] and/or [2] in reference section of this document.

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 by entering <https://<ip-address>/SMGR> URL in a web browser, where <ip-address> is the IP address of System Manager.



Avaya Aura® System Manager 6.3

[Home](#) / [Log On](#)

Log On

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually

User ID:
Password:

[Change Password](#)

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.

Log in using appropriate credentials.



Users	Elements	Services
Administrators Manage Administrative Users	Communication Manager Manage Communication Manager 5.2 and higher elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Server 1000 Manage Communication Server 1000 elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user resources and provision users	IP Office Manage IP Office elements	Events Manage alarms, view and harvest logs
	Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	Geographic Redundancy Manage Geographic Redundancy
	Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	Inventory Manage, discover, and navigate to elements
	Presence Presence	Licenses View and configure licenses
	Routing Session Manager Routing Administration	Replication Track data replication nodes, repair replication nodes
	Session Manager Session Manager Administration, Status, Maintenance and Performance Management	Scheduler Schedule, track, cancel, update and delete jobs
		Security Manage Security Certificates
		Shutdown Shutdown System Manager Gracefully
		Software Management Upgrade and Patch Management for Communication Manager devices and IP Office
		Templates Manage Templates for Communication Manager, Messaging System and IP Office elements

6.1. Add SIP Domain

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

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

Click **Commit** to save changes.

Routing * Home

- ▼ Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing / Domains

Domain Management Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Notes
* avaya.com	sip	

Commit Cancel

6.2. Add Location

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

Under **General**:

- Type in a descriptive **Name**

Under **Location Pattern** click on **New** (not shown):

- Type in an **IP Address Pattern**, e.g., 10.64.101.*

Click **Commit** to save changes. Screen shot shown on next page.

Location Details

Commit Cancel

General

* Name:

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

* Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth:

Alarm Threshold

Overall Alarm Threshold: %

Multimedia Alarm Threshold: %

* Latency before Overall Alarm Trigger: Minutes

* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

Add Remove

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.10.*	<input type="text"/>
<input type="checkbox"/>	* 10.64.101.*	<input type="text"/>

Select : All, None

6.3. Add SIP Entity – Communication Manager

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

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of Communication Manager in **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 been already configured.

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:

6.4. Add Entity Link – Communication Manager

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

- Type in a descriptive name in **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.

Entity Links

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM	* SM_Public	TLS	* 5061	* Communication Manager	* 5061	Trusted	

6.5. Add SIP Entity – FAXCOM

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

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of FAXCOM in **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 been already configured.

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:

6.6. Add Entity Link – FAXCOM

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

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

Click **Commit** to save changes.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* biscom	* asm-tr1	UDP	* 5060	* biscom-1	* 5060	trusted

6.7. Add Time Ranges

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

- Type in a descriptive name in **Name** field

Click **Commit** to save changes.

Time Ranges [Commit](#) [Cancel](#)

1 Item | [Refresh](#) Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* TimeRange	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	* 00:00	* 23:59	

6.8. Add Routing Policy – Communication Manager

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

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
 - Select Communication Manager SIP entity added in **Section 6.3**
- Under **Time of Day**, click on **Add** (not shown):
 - Select time range added in previous step

Click **Commit** to save changes.

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cm-tr1	10.64.10.67	CM	

Time of Day

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	<input type="text" value="0"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select : All, None

Dial Patterns

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Regular Expressions

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

6.9. Add Routing Policy – FAXCOM

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

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
 - Select biscom-1 entity added in **Section 6.5**
- Under **Time of Day**, click on **Add** (not shown):
 - Select time range added in previous step

Click **Commit** to save changes.

Routing Policy Details

[Commit](#) [Cancel](#)

General

* **Name:**

Disabled:

* **Retries:**

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
biscom-1	10.64.101.94	SIP Trunk	

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

Select : All, None

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
- Set **Domain** to domain configured on **Section 6.1**

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, dialed number of 25xxx were used to route calls to Communication Manager. Thus, pattern, min and max values were all set to 5.

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain: ▼

Notes:

Originating Locations and Routing Policies

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	cm-tr1	0	<input type="checkbox"/>	cm-tr1	

Select : All, None

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 **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, dialed number of 552xxxxxxx were used to route calls to FAXCOM. Thus, pattern, min and max values were all set to 10.

Dial Pattern Details

[Commit](#) [Cancel](#)

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

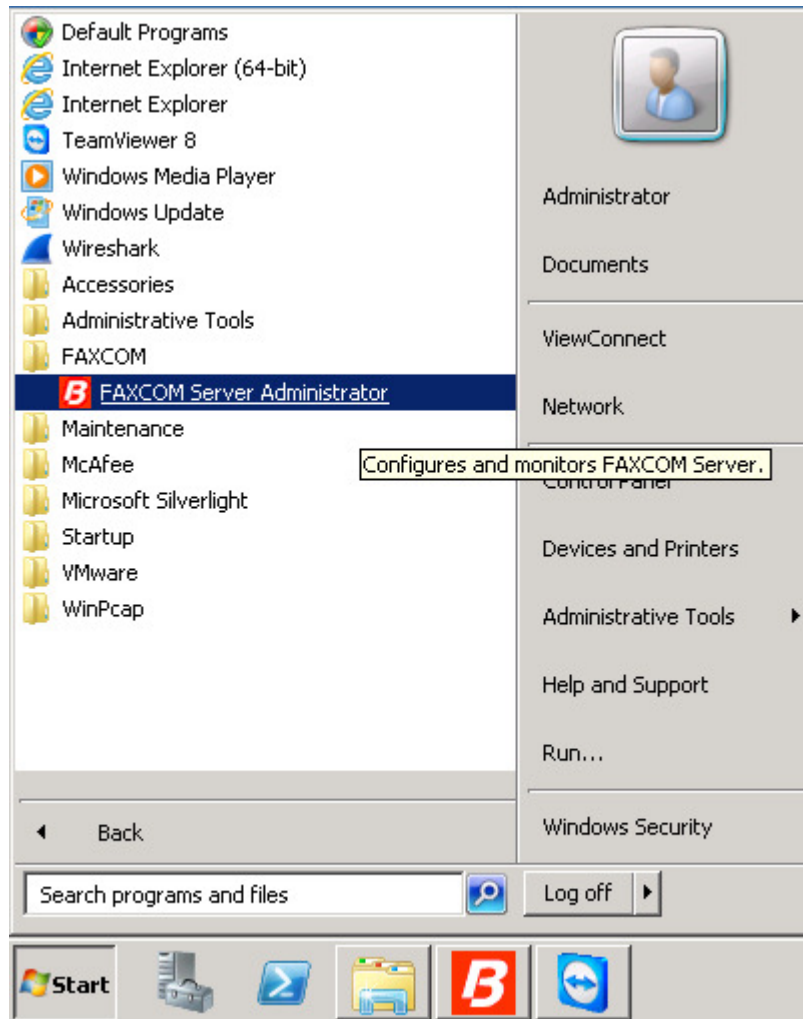
1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name ^	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		faxcom		<input type="checkbox"/>	biscom-2	

Select : All, None

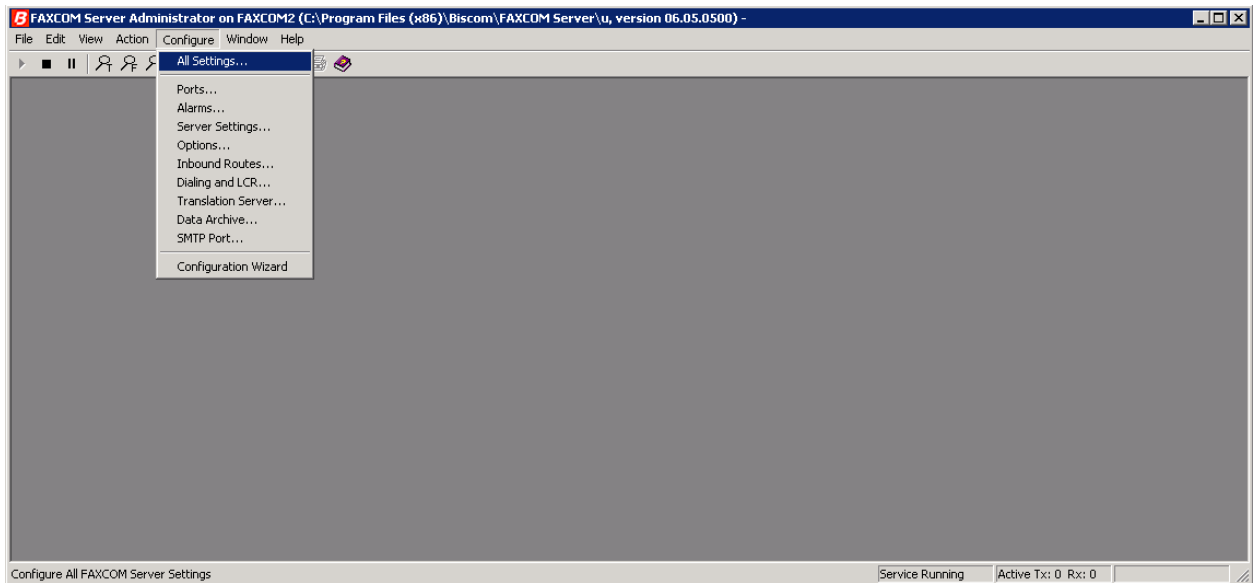
7. Configure FAXCOM

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



From the menu choices at the top, click **Configure**. From the drop down menu select **All Settings**.

Note: Alternatively, wrench icon from the icon bar below the menu choices can also be clicked to bring up the **Configure All Settings** window.



On the **Configure All Settings** window, click the **SR140 Settings** tab. This configures the Dialogic SR140 fax over IP software license, which is the actual direct interface to the Avaya. In the **SR140 Settings** tab, configure the following:

- 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 **IP Preference** field, select **IPV4 Only**
- In the **Local IP Address** field, type the IP address of the fax server
- In the **Gateway IP Address** field, type the IP address of Session Manager; then click the **Add** button

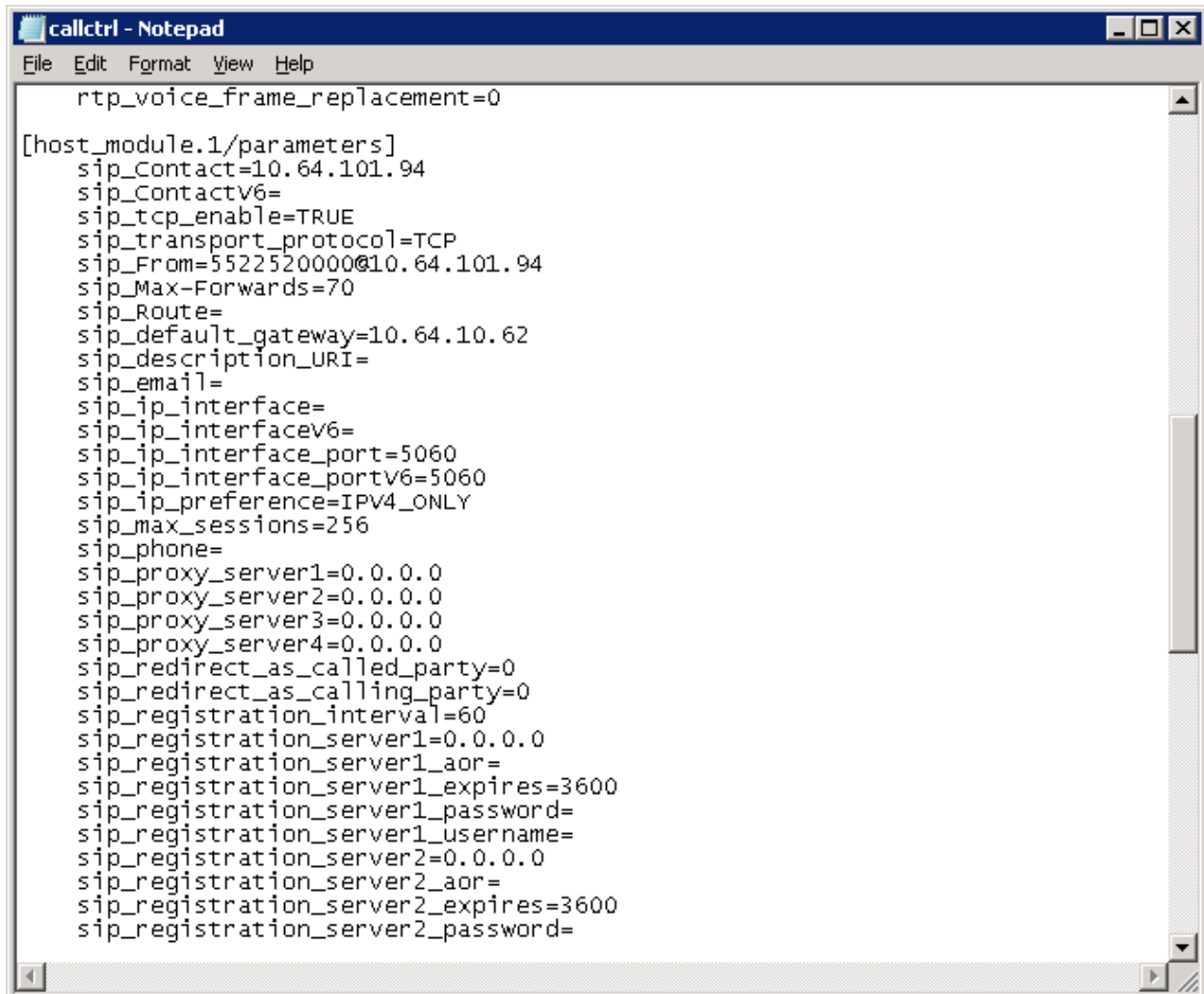
Once all these values are configured, click **Done**, and you will be prompted to restart the FAXCOM service in order for the values to take effect. Restart the service when ready.

The screenshot shows the 'Configure All Settings' window with the 'SR140 Settings' tab selected. The window has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with the following tabs: Dialing, Local Exchanges, Internal Numbers, LCR Routes, LCR Rules, Translation Server, Data Archive, Alarm Events, Alarm Notifications, Fax Ports, Host Ports, Server Settings, SR140 Settings (selected), Options, and Inbound Routes. The SR140 Settings tab contains the following fields and controls:

- Licensed channels: 48
- License Manager: License Manager (button)
- Debug logging: (checked)
- V.34 Mode: (unchecked)
- Round Robin: (unchecked)
- T.38 Version: 0 (dropdown menu)
- Mode: T.38, T.38 + G.711, G.711
- Call Control: H.323, SIP
- Call Control Variant: Avaya (dropdown menu)
- IP Preference: IPV4 Only (dropdown menu)
- Local IP Address: 10.64.101.95 (text field)
- H.323 Gatekeeper IP Address: 0.0.0.0 (text field)
- Gateway IP Address: 10.64.10.62 (text field)
- Buttons: Add, Remove, Move Up, Move Down
- Buttons: Done, Help

In Windows Explorer, navigate to the **C:\Program Files (x86)\Biscom\FAXCOM Server\U\FAPI\TR1034\Cfg** directory. (Note: on 64-bit systems, the high level directory will likely be “\Program Files (x86).”) Open the **callctrl.cfg** file with a text editing program. In the **[host_module.1/parameters]** section, set the “sip_From” value to a valid header that the Avaya will recognize, which is usually a phone number @ the name or IP address of the FAXCOM server.

Example value: sip_From=5522520000@10.64.101.94

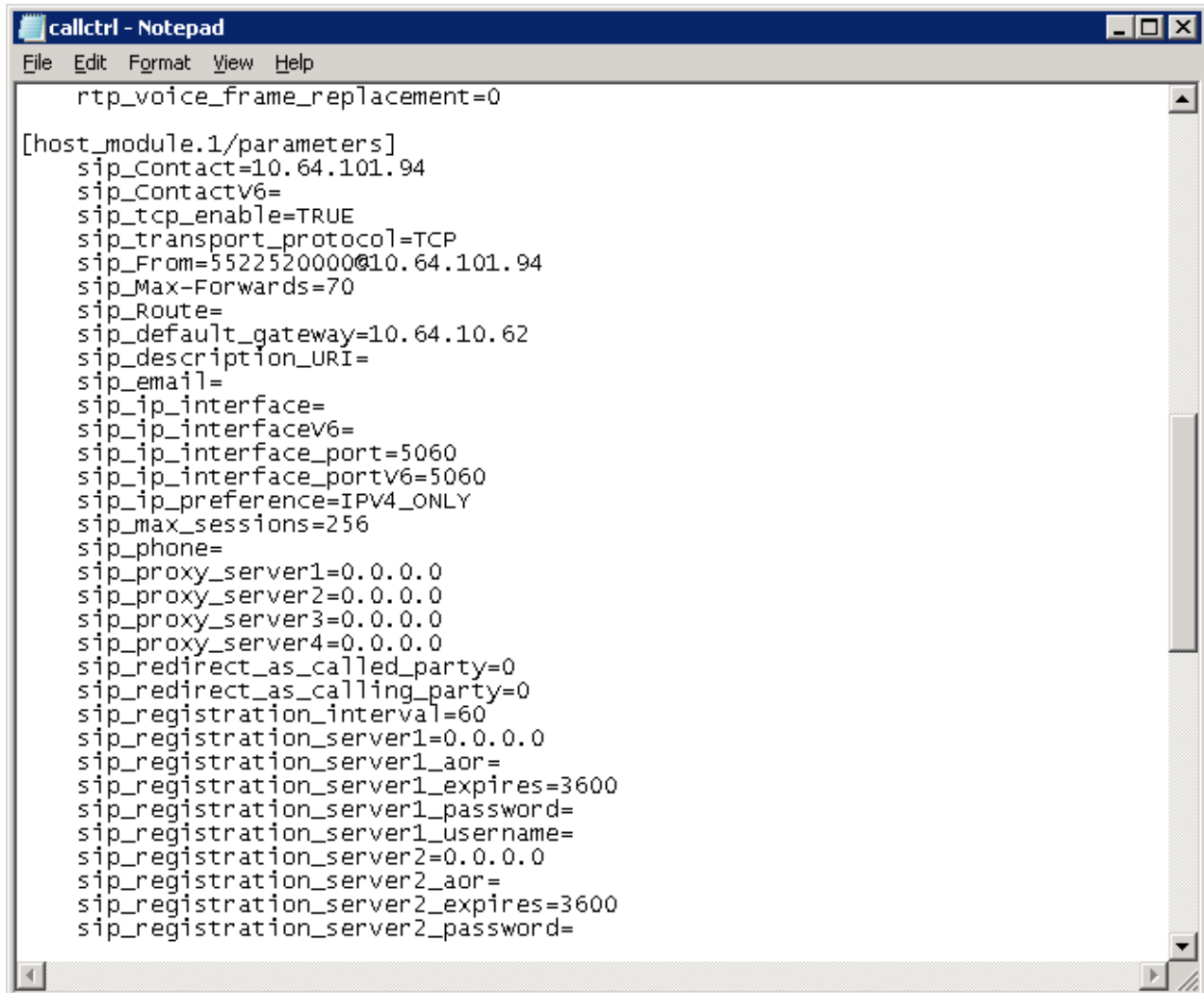


```
callctrl - Notepad
File Edit Format View Help
rtp_voice_frame_replacement=0

[host_module.1/parameters]
sip_contact=10.64.101.94
sip_contactv6=
sip_tcp_enable=TRUE
sip_transport_protocol=TCP
sip_from=5522520000@10.64.101.94
sip_max_forwards=70
sip_route=
sip_default_gateway=10.64.10.62
sip_description_URI=
sip_email=
sip_ip_interface=
sip_ip_interfacev6=
sip_ip_interface_port=5060
sip_ip_interface_portv6=5060
sip_ip_preference=IPV4_ONLY
sip_max_sessions=256
sip_phone=
sip_proxy_server1=0.0.0.0
sip_proxy_server2=0.0.0.0
sip_proxy_server3=0.0.0.0
sip_proxy_server4=0.0.0.0
sip_redirect_as_called_party=0
sip_redirect_as_calling_party=0
sip_registration_interval=60
sip_registration_server1=0.0.0.0
sip_registration_server1_aor=
sip_registration_server1_expires=3600
sip_registration_server1_password=
sip_registration_server1_username=
sip_registration_server2=0.0.0.0
sip_registration_server2_aor=
sip_registration_server2_expires=3600
sip_registration_server2_password=
```

This step is necessary only if SIP over TCP is being configured between the FAXCOM server and Session Manager. In the same file mentioned above under `[host_module.1/parameters]` section, add the following two lines:

```
sip_tcp_enable=TRUE  
sip_transport_protocol=TCP
```



```
callctrl - Notepad  
File Edit Format View Help  
rtp_voice_frame_replacement=0  
[host_module.1/parameters]  
sip_contact=10.64.101.94  
sip_contactv6=  
sip_tcp_enable=TRUE  
sip_transport_protocol=TCP  
sip_from=5522520000@10.64.101.94  
sip_max_forwards=70  
sip_route=  
sip_default_gateway=10.64.10.62  
sip_description_uri=  
sip_email=  
sip_ip_interface=  
sip_ip_interfacev6=  
sip_ip_interface_port=5060  
sip_ip_interface_portv6=5060  
sip_ip_preference=IPV4_ONLY  
sip_max_sessions=256  
sip_phone=  
sip_proxy_server1=0.0.0.0  
sip_proxy_server2=0.0.0.0  
sip_proxy_server3=0.0.0.0  
sip_proxy_server4=0.0.0.0  
sip_redirect_as_called_party=0  
sip_redirect_as_calling_party=0  
sip_registration_interval=60  
sip_registration_server1=0.0.0.0  
sip_registration_server1_aor=  
sip_registration_server1_expires=3600  
sip_registration_server1_password=  
sip_registration_server1_username=  
sip_registration_server2=0.0.0.0  
sip_registration_server2_aor=  
sip_registration_server2_expires=3600  
sip_registration_server2_password=
```

Once edits are made to the callctrl.cfg file, save the file, and make the file read-only. The read-only step is critical. If the file is not made read-only, then the values will be overwritten.

- After the callctrl.cfg file has been saved and made read-only, restart the FAXCOM service once more.

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 Biscom-1 SIP entity that was configured in this document (not shown).

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

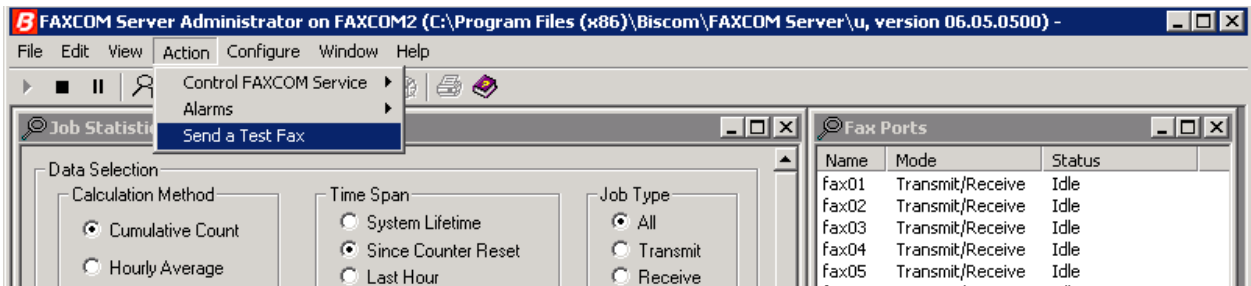
1 Items Refresh		Filter: Enable							
Session Manager	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status		
<input type="radio"/> asm-tr1	10.64.101.9	5060	TCP	FALSE	UP	200 OK	UP		

8.2. FAXCOM

From the Biscom FAXCOM Server Administrator program, bring up the “Fax Ports” window either by icon with the magnifying glass and the letter F, or by clicking **View** from the menu choices on top and selecting **Fax Ports**. This brings up a window showing all the licensed fax ports and each port’s status. All ports should be in **idle** state.

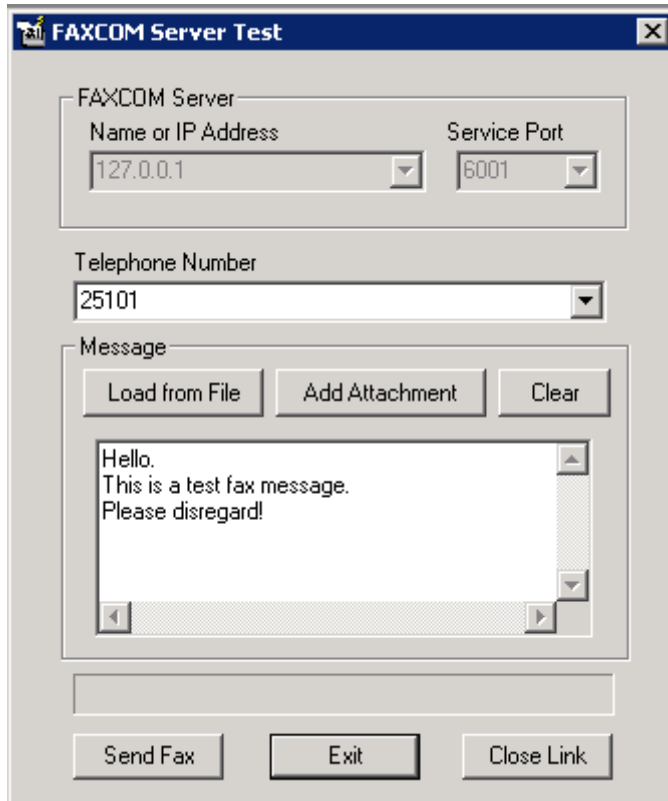
Name	Mode	Status
Fax01	Transmit/Receive	Idle
Fax02	Transmit/Receive	Idle
Fax03	Transmit/Receive	Idle
Fax04	Transmit/Receive	Idle
Fax05	Transmit/Receive	Idle
Fax06	Transmit/Receive	Idle
Fax07	Transmit/Receive	Idle
Fax08	Transmit/Receive	Idle
Fax09	Transmit/Receive	Idle
Fax10	Transmit/Receive	Idle
Fax11	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, you can send a test fax using the **FAXCOM Server Administrator**. Click the **Action menu** choice; click **Send a Test Fax**.



On the **FAXCOM Server Test Window**:

- The **FAXCOM Server: Name or IP Address** field defaults to 127.0.0.1, leave it unchanged. In the **FAXCOM Server: Service Port** field, type **6001** if it doesn't display that value already.
- In the **Telephone Number** field, type the phone number of a fax device (e.g., if sending to an external number, dial the necessary prefix).
- In the **Message** box, type in a sample text, if desired. Click the **Send Fax** button. This will send a one-page test fax to Communication Manager. If successful, an OK report will be displayed.



Below is an example of a successful test fax:



9. Conclusion

Biscom FAXCOM passed compliance testing. These Application Notes describe the procedures required to configure Biscom FAXCOM to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support the network shown 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 6.3, Issue 2, June 2013
- [2] Administering Avaya Aura® Communication Manager, Release 6.3, Document 03-300509, Issue 8, May 2013

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

- [1] FAXCOM Server Administrator's Guide, July 2013 Revised Edition, © Biscom, Inc., 1995-2013

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.