Avaya Solution & Interoperability Test Lab

Application Notes for XMedius Solutions Inc. XMediusFAX On-Premises with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring XMedius Solutions Inc. XMediusFAX On-Premises fax server with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

XMediusFAX On-Premises is a software based fax server that sends and receives fax calls over an IP network. In the configuration tested, XMediusFAX interoperates with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to send/receive faxes using SIP trunks and the T.38 fax protocol between XMediusFAX and the Avaya SIP infrastructure.

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

These Application Notes describe the procedures for configuring XMedius Solutions Inc. XMediusFAX On-Premises (XMediusFAX) fax server with Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager) using SIP trunks.

XMediusFAX is a software based fax server that sends and receives fax calls over an IP network. In the configuration tested, XMediusFAX interoperated with Session Manager and Communication Manager to send/receive faxes using SIP trunks and the T.38 protocol between XMediusFAX and the Avaya SIP infrastructure. The compliance testing focused on fax calls to and from the XMediusFAX fax server using various page lengths, resolutions, paper sizes, and fax data speeds.

2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of XMediusFAX with the Avaya SIP infrastructure consisting of Session Manager and Communication Manager. This section also covers the test results.

The interoperability compliance test included feature and serviceability test. The feature test cases were performed manually. Fax calls to and from XMediusFAX were made. The faxes were sent and received using the XMediusFAX web interface and an analog fax machine at the PSTN. Testing included sending faxes locally and over Direct SIP and PRI trunks.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to XMediusFAX and rebooting the XMediusFAX server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The general test approach was to make intra-site and inter-site fax calls to and from the XMediusFAX fax server. The compliance tested configuration contained two sites. One site served as the main enterprise site and the other served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using SIP trunks and ISDN-PRI trunks between the sites. Faxes were sent with various page lengths, resolutions, paper sizes, and at various fax data speeds. Serviceability testing included verifying proper operation/recovery from network outages, unavailable resources, and Communication Manager and XMediusFAX restarts. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included the TN2302 MedPro circuit pack and the

TN2602 MedPro circuit pack in the Avaya G650 Media Gateway; and the integrated VoIP engine of the Avaya G450 Media Gateway.

The test focused on fax transmission using the T.38 standard. However, a subset of the test cases were also executed using the G.711 pass-through fax mode.

2.2. Test Results

XMediusFAX successfully passed compliance testing with the following observations noted:

- In an Inter-site environment where the two sites communicate using direct SIP trunk, shuffling needs to be disabled for outbound fax (faxes initiated by XMediusFAX). This is only required when T.38 standard is involved and not required for G.711 pass-through mode.
- An Adaptation was created in Session Manager and applied to the XMediusFAX SIP entity to override the destination domain as explained in **Section 6.4**.

2.3. Support

For technical support on XMediusFAX, contact XMedius Solutions Inc. at:

- Web: support.xmediusfax.com
- Phone +1-866-615-3066 (NA)
  +33(0)1 57 61 30 30 (EMEA)
  0011-800-132-00000 (Australia)
- Email: support.software@xmedius.com

3. Reference Configuration

Figures 1A and 1B illustrate the reference configurations used during testing.

The local fax testing configuration is as shown in **Figure 1A** where a Session Manager and Communication Manager with a G450 Media Gateway are involved. XMediusFAX communicates to the Avaya SIP infrastructure (Communication Manager and Session Manager) via a SIP trunk. The media resources required by the trunk are provided by the DSPs on G450 Media Gateway. A laptop running the Windows Fax Console application is connected to the G450 Media Gateway via an analog port. This entire setup is referred to as Site A.

The fax over direct SIP testing configuration is as shown in **Figure 1A**, where Site A is connected to Remote Site 1 via Direct SIP. In this context, Direct SIP means that the two intra sites are connected directly without a Session Manager in between them. The Remote Site 1 has a laptop running the Windows Fax Console application connected via an analog port.

The fax over ISDN/PRI testing configuration is as shown in **Figure 1A**, where Site A is connected to Remote Site 2 via ISDN/PRI. The Remote Site 2 has a laptop running the Windows Fax Console application connected via an analog port.

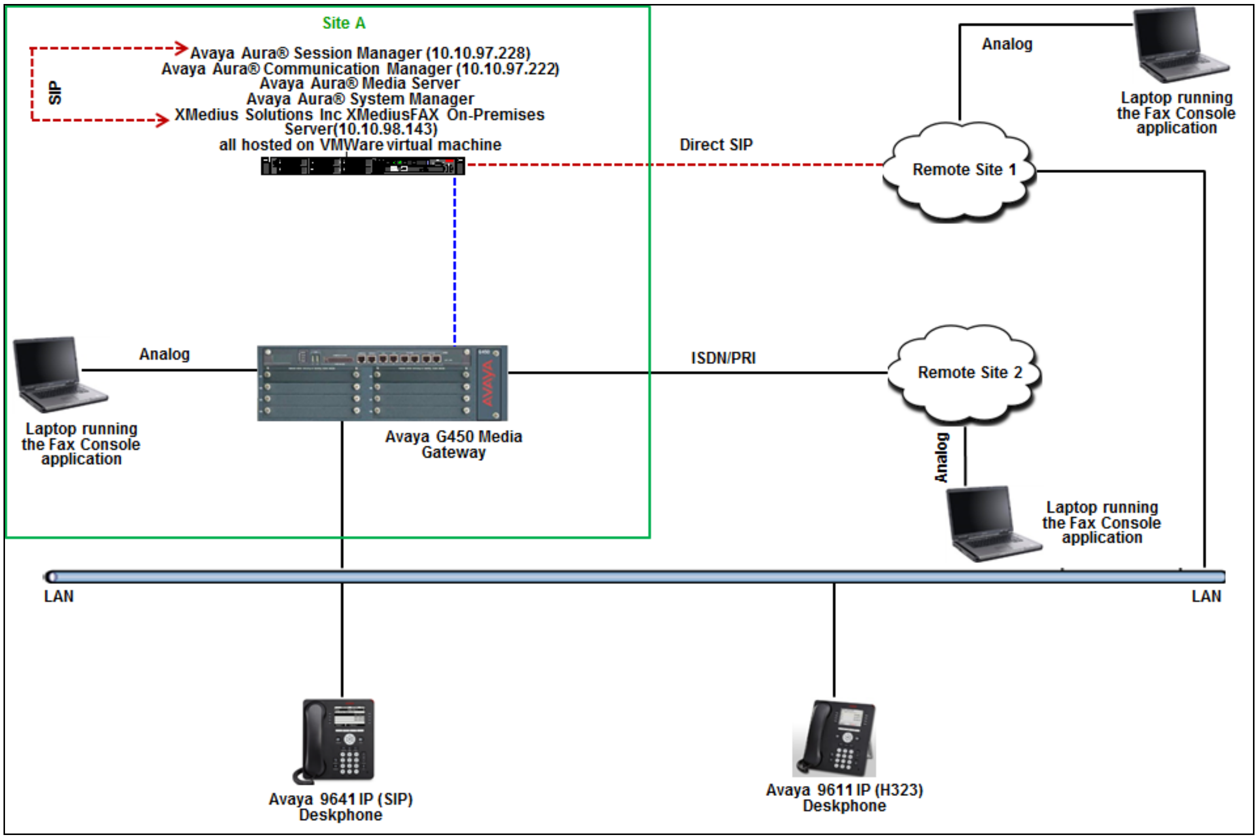

Site A
SIP
Avaya Aura® Session Manager (10.10.97.228)
Avaya Aura® Communication Manager (10.10.97.222)
Avaya Aura® Media Server
Avaya Aura® System Manager
XMedius Solutions Inc XMediusFAX On-Premises Server(10.10.98.143)
all hosted on VMWare virtual machine
Analog
Laptop running the Fax Console application
Direct SIP
Remote Site 1
Analog
Laptop running the Fax Console application
Avaya G450 Media Gateway
ISDN/PRI
Remote Site 2
Analog
Laptop running the Fax Console application
LAN
LAN
Avaya 9641 IP (SIP) Deskphone
Avaya 9611 IP (H323) Deskphone

Figure 1A: Test Configuration with SIP Interface to XMediusFAX On-Premises with ISDN/PRI and Direct SIP connectivity to Remote Sites

The local fax testing configuration is as shown in **Figure 1B**, where a Session Manager and Communication Manager with a G650 Media Gateway are involved. XMediusFAX at this site communicates to the Avaya SIP infrastructure (Communication Manager and Session Manager) via a SIP trunk. The media resources required by the trunk are provided by the IP Media Processor (MedPro) circuit pack. Two versions of the IP MedPro circuit pack were tested in this configuration: TN2302AP and TN2602AP. A laptop running the Windows Fax Console application is connected to the G650 Media Gateway via an analog port.

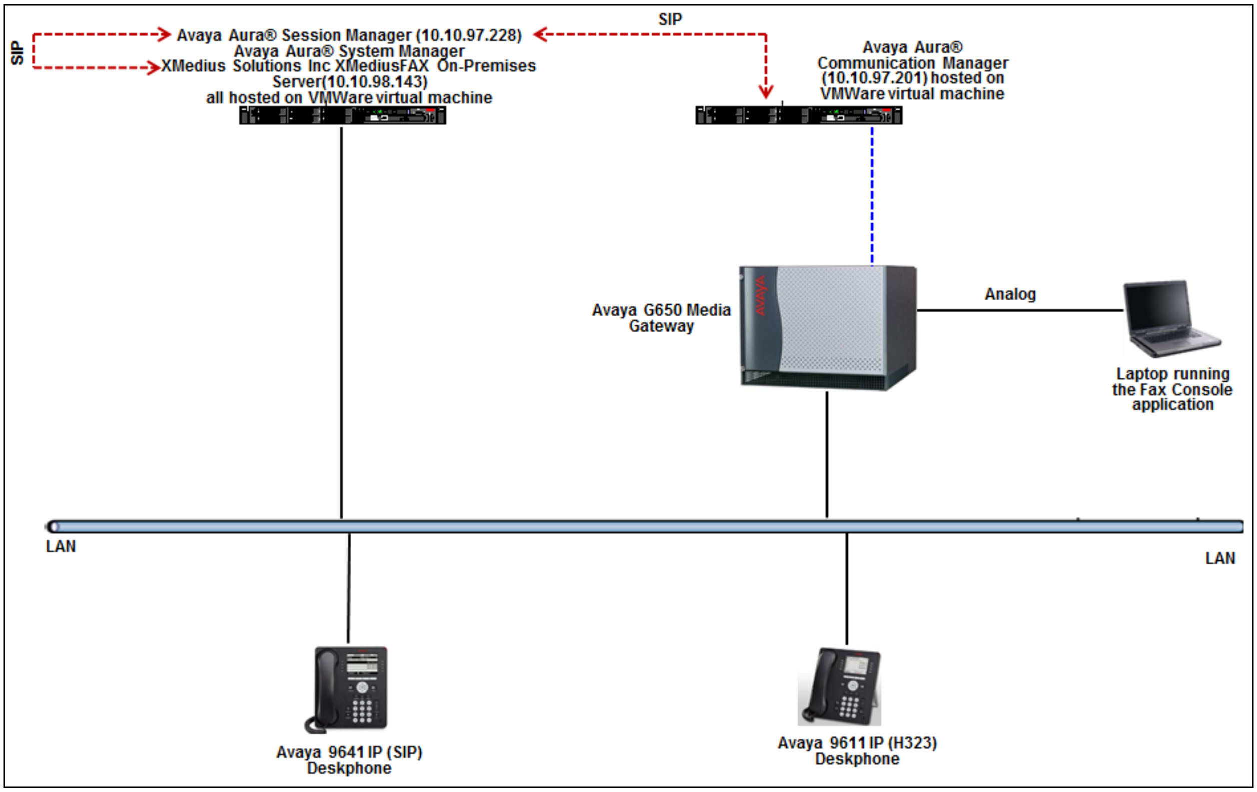

SIP
SIP
Avaya Aura® Session Manager (10.10.97.228)
Avaya Aura® System Manager
XMedius Solutions Inc XMediusFAX On-Premises Server(10.10.98.143)
all hosted on VMWare virtual machine
Avaya Aura® Communication Manager (10.10.97.201) hosted on VMWare virtual machine
Avaya G650 Media Gateway
Analog
Laptop running the Fax Console application
LAN
LAN
Avaya 9641 IP (SIP) Deskphone
Avaya 9611 IP (H323) Deskphone

Figure 1B: Test Configuration with SIP Interface to XMediusFAX On-Premises

Although the IP endpoints are not involved in the faxing operations, they are present at both sites to verify that VoIP telephone calls are not affected by the FoIP faxing operations and vice versa.

Outbound fax calls originating from XMediusFAX are sent to Session Manager first, and then from Session Manager to Communication Manager via SIP trunks. Based on the dialed digits, Communication Manager will either direct the calls to the local fax destination, or to the other sites via an ISDN-PRI or SIP trunk. Inbound fax calls terminating to XMediusFAX sent from the local fax machine or from the remote site are received by Communication Manager. The calls are then directed to Session Manager for onward routing to XMediusFAX via SIP trunks.

4. Equipment and Software Validated

The following equipment and software were used for the reference configuration:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.0.1.1.0-FP1SP1
Avaya Aura® Session Manager running on virtualized environment	7.0.1.1.701114
Avaya Aura® System Manager running on virtualized environment	7.0.1.2 (SP2)
Avaya Aura® Media Server running on virtualized environment	7.7.0.359
Avaya G450 Media Gateway • DCP MM MM712AP	FW 37.19.0/1 HW10 FW014
Avaya G650 Media Gateway: • TN2302AP • TN2602AP	 HW20 FW117 HW02 FW066
Avaya 96x1 Series IP Deskphones: • 9641GS (SIP) • 9611G (H323)	 7.0.1.1.5 6.6229
XMedius Solutions Inc. XMediusFAX On-Premises running on Windows 2008 R2 x64 Standard SP1	R8.0.0.334 + Hotfix XMFaxDriver 8.0.0.387

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration to support the network shown in **Figures 1A** and **1B**.

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

5.1. License

Use the **display system-parameters customer-options** command to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  10
           Maximum Concurrently Registered IP Stations: 2400  6
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  34
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

5.2. IP Network Region

Use the **display ip-network-region** command to view the network region settings. The values shown below are the values used during compliance testing.

- **Authoritative Domain**: ***bvwdev.com***. This field was configured to match the domain name configured on Session Manager. The domain will appear in the “From” header of SIP messages originating from this IP region.
- **Name**: Any descriptive name may be used (optional).
- **Intra-region IP-IP Direct Audio**: ***yes***
- **Inter-region IP-IP Direct Audio**: ***yes***
  By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the **Signaling Group** form.
- **Codec Set**: ***1***. The codec set contains the list of codecs available for calls within this IP network region.

```
display ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: bvwdev.com
    Name: Region1               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: 8001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.3. Codecs

IP codec set 1 was used during compliance testing. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing.

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

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.711A           n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: none
 2:
 3:
 4:
 5:
```

On **Page 2**, set the **FAX Mode** field to ***t.38-standard*** and the **ECM** field is set to ***y*** by default. The **Modem Mode** field should be set to ***off***.

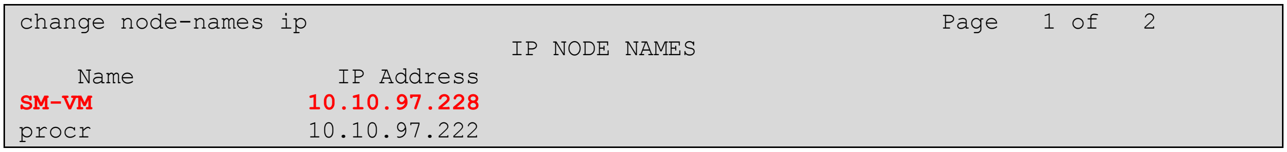
Retain the **FAX Redundancy** at its default value of ***0***.

A subset of the test cases were also executed with the **FAX Mode** field set to ***off*** for pass-through mode (not shown).

```
display 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

                                                                     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. Node Names

Use the **change node-names ip** command to create a node name for the IP address of Session Manager. Enter a descriptive name in the **Name** column and the IP address assigned to Session Manager in the **IP address** column.

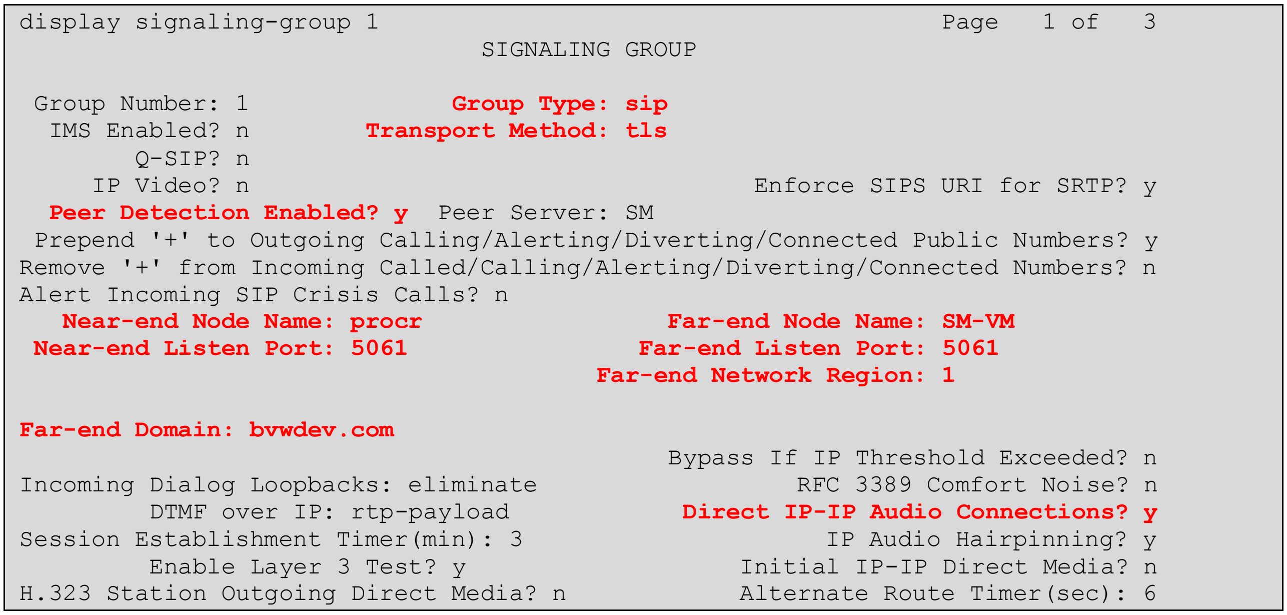


```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name                 IP Address
SM-VM                   10.10.97.228
procr                   10.10.97.222
```

5.5. Signaling Group

Signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. Signaling group 1 was configured using the parameters highlighted below.

- **Group Type**: ***sip***
- **Transport Method**: ***tls***
- **Peer Detection Enabled**: ***y***
- **Near-end Node Name**: ***procr*** this node name maps to the IP address of Communication Manager processor interface.
- **Near-end Listen Port**: ***5061***
- **Far-end Node Name**: ***SM-VM*** this node name maps to the IP address of Session Manager.
- **Far-end Listen Port**: ***5061***
- **Far-end Network Region**: ***1*** this defines the IP network region which contains Session Manager.
- **Far-end Domain**: ***bvwdev.com*** this domain is sent in the "To" header of SIP messages of calls using this signaling group.
- **Direct IP-IP Audio Connections**: ***y*** this field must be set to ***y*** to enable media shuffling on the SIP trunk.

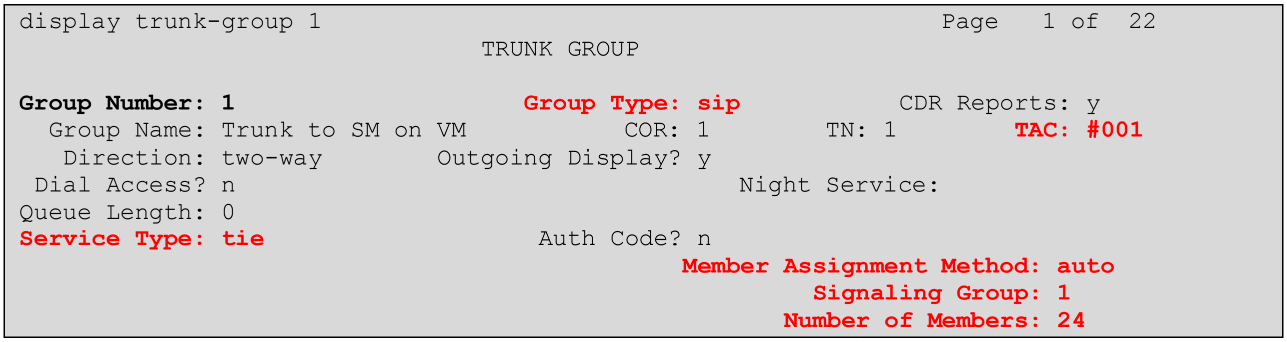


```
display signaling-group 1                                       Page   1 of   3
                                SIGNALING GROUP

 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: SM-VM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: bvwdev.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? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.6. Trunk Group

Trunk group 1 was used for the SIP trunk group between Communication Manager and Session Manager. Trunk group 1 was configured using the parameters highlighted below.

- **Group Type:** ***sip***
- **TAC:** ***#001*** Enter a valid value consistent with the Communication Manager dial plan.
- **Service Type:** ***tie***
- **Member Assignment Method:** ***auto***
- **Signaling Group**: ***1***. This field is set to the signaling group shown in **Section 5.5**.
- **Number of Members:** ***24***. This field represents the number of trunk group members in the SIP trunk group.



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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Trunk to SM on VM           COR: 1        TN: 1        TAC: #001
   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: 1
                                                     Number of Members: 24
```

On **Page 3**:

- The **Numbering Format** field was set to ***private***. This field specifies the format of the calling party number sent to the far-end.
- The default values may be retained for the other fields.

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



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

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y

 DSN Term? n                     SIP ANAT Supported? n
```

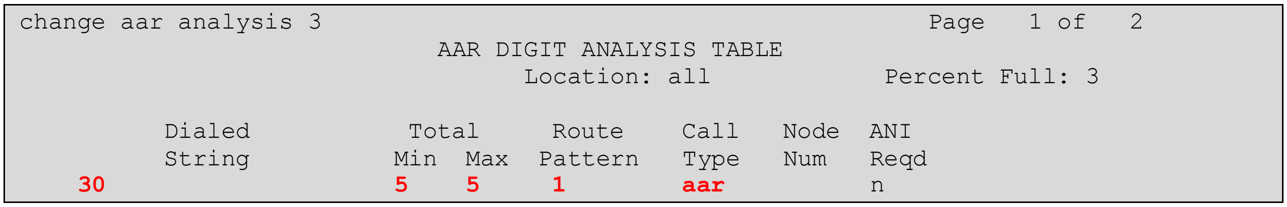
5.7. Private Numbering

Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a ***5***-digit extension beginning with ***56*** and routed across trunk group ***1*** will be sent as a ***5***-digit calling number. The calling party number is sent to the far-end in the SIP "From" header.

```
display private-numbering 0                                     Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private          Total
Len Code           Grp(s)     Prefix           Len
 4  33             6                           4     Total Administered: 6
 5  50             1                           5        Maximum Entries: 540
 5  52             1                           5
 5  53             1                           5
 5  54             1                           5
 5  56             1                           5
```

5.8. Automatic Alternate Routing

Automatic Alternate Routing (AAR) was used to route calls either to Session Manager or to Communication Manager at the other site. Use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table. The example below shows numbers that begin with ***30*** and are ***5*** digits long use route pattern ***1*** (to Session Manager). This routing sends calls from Communication Manager to XMediusFAX via Session Manager. Similarly other entries can be configured.

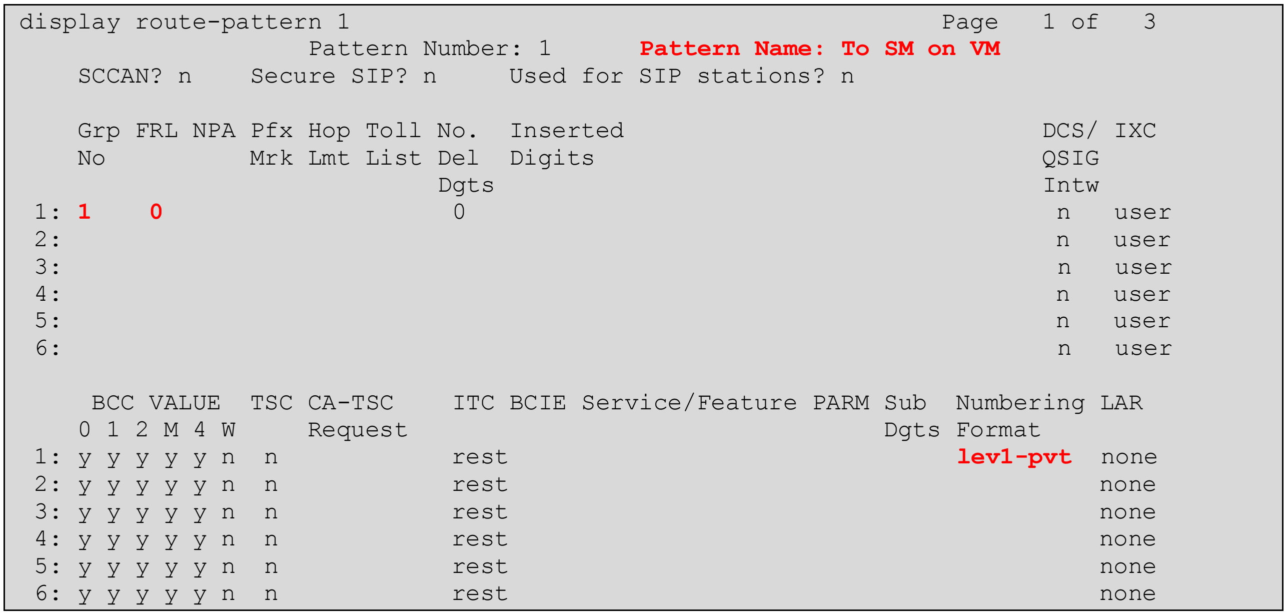


```
change aar analysis 3                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 3

          Dialed           Total      Route     Call    Node   ANI
          String          Min  Max   Pattern    Type    Num    Reqd
    30                    5    5     1          aar            n
```

5.9. Route Pattern

Route pattern 1 was used for calls destined for XMediusFAX through Session Manager. Route pattern 1 was configured using the parameters highlighted below. Similarly other route patterns can be configured.

- **Pattern Name**: Any descriptive name.
- **Grp No**: ***1*** this field is set to the trunk group number defined in **Section 5.6**.
- **FRL**: ***0*** this field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.
- **Numbering Format**: ***lev1-pvt***



```
display route-pattern 1                                         Page   1 of   3
                    Pattern Number: 1       Pattern Name: To SM on VM
    SCCAN? n     Secure SIP? n     Used for SIP stations? n

    Grp  FRL NPA Pfx Hop Toll No.  Inserted                             DCS/  IXC
    No           Mrk Lmt List Del  Digits                               QSIG
                              Dgts                                      Intw
 1: 1    0                     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 Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev1-pvt  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
```

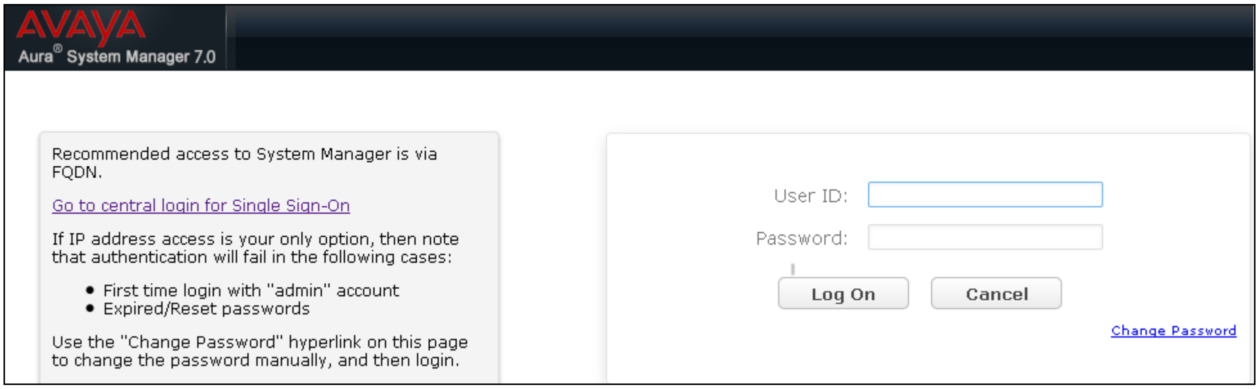
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface.

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

6.1. Login

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.

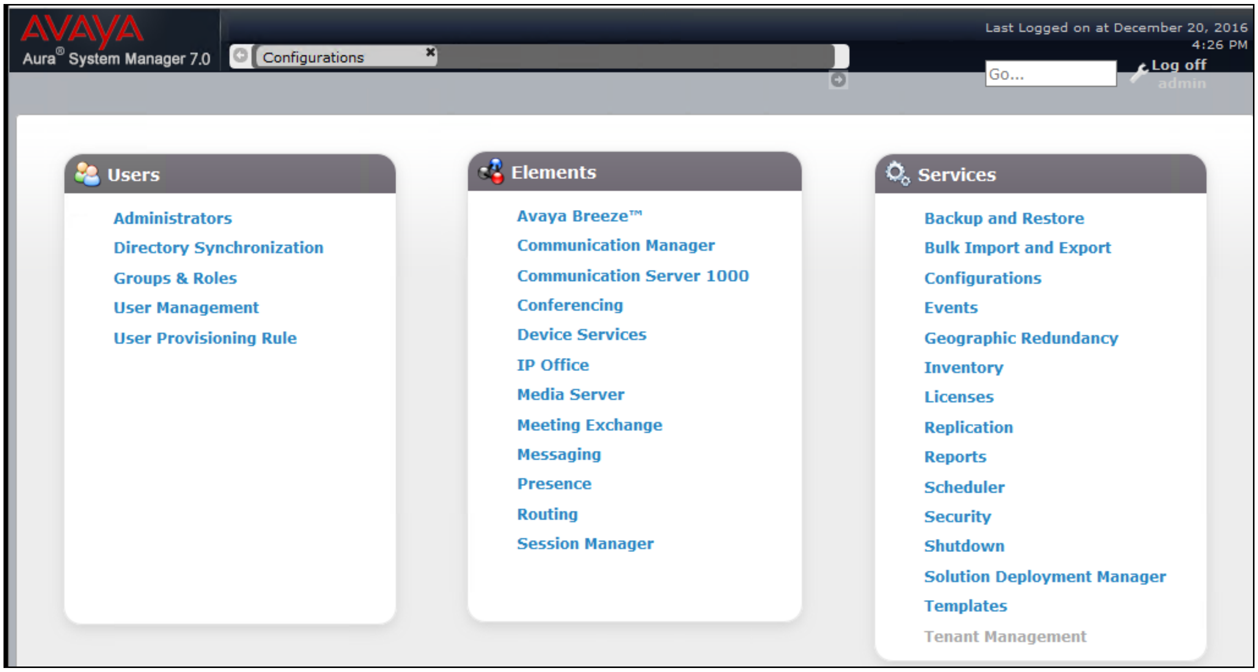
Go to central login for Single Sign-On

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, and then login.

The System Manager dashboard is shown as below.



6.2. Add SIP Domain

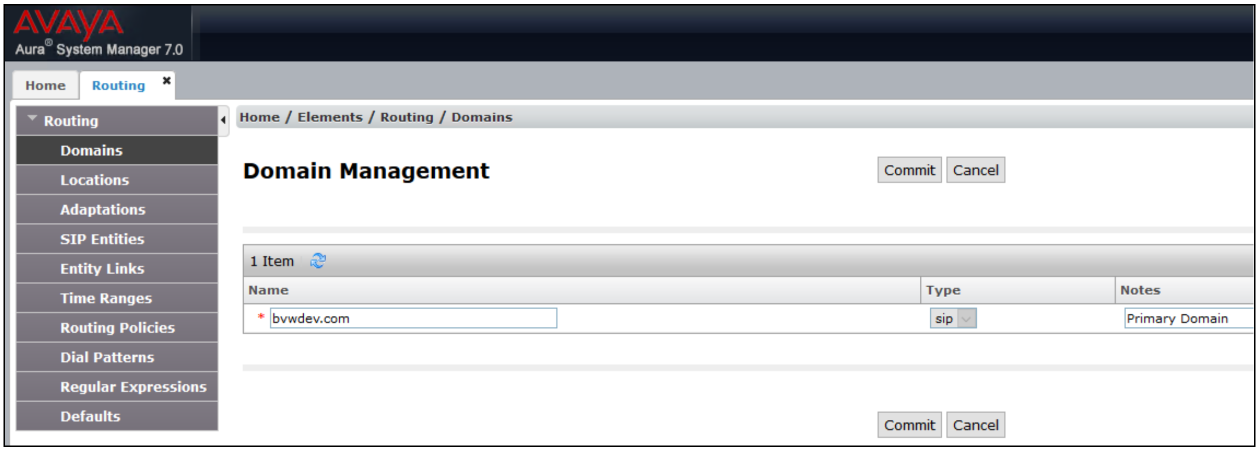
The **Routing** menu contains all the configuration tasks listed at the beginning of this section.

During compliance testing, one SIP domain was configured.

Navigate to **Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with

- **Name**: ***bvwdev.com*** (as set in **Section 5.2**).
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.



Domain Management

1 Item

Name	Type	Notes
* bvwdev.com	sip	Primary Domain

6.3. Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one location was configured at each site for compliance testing.

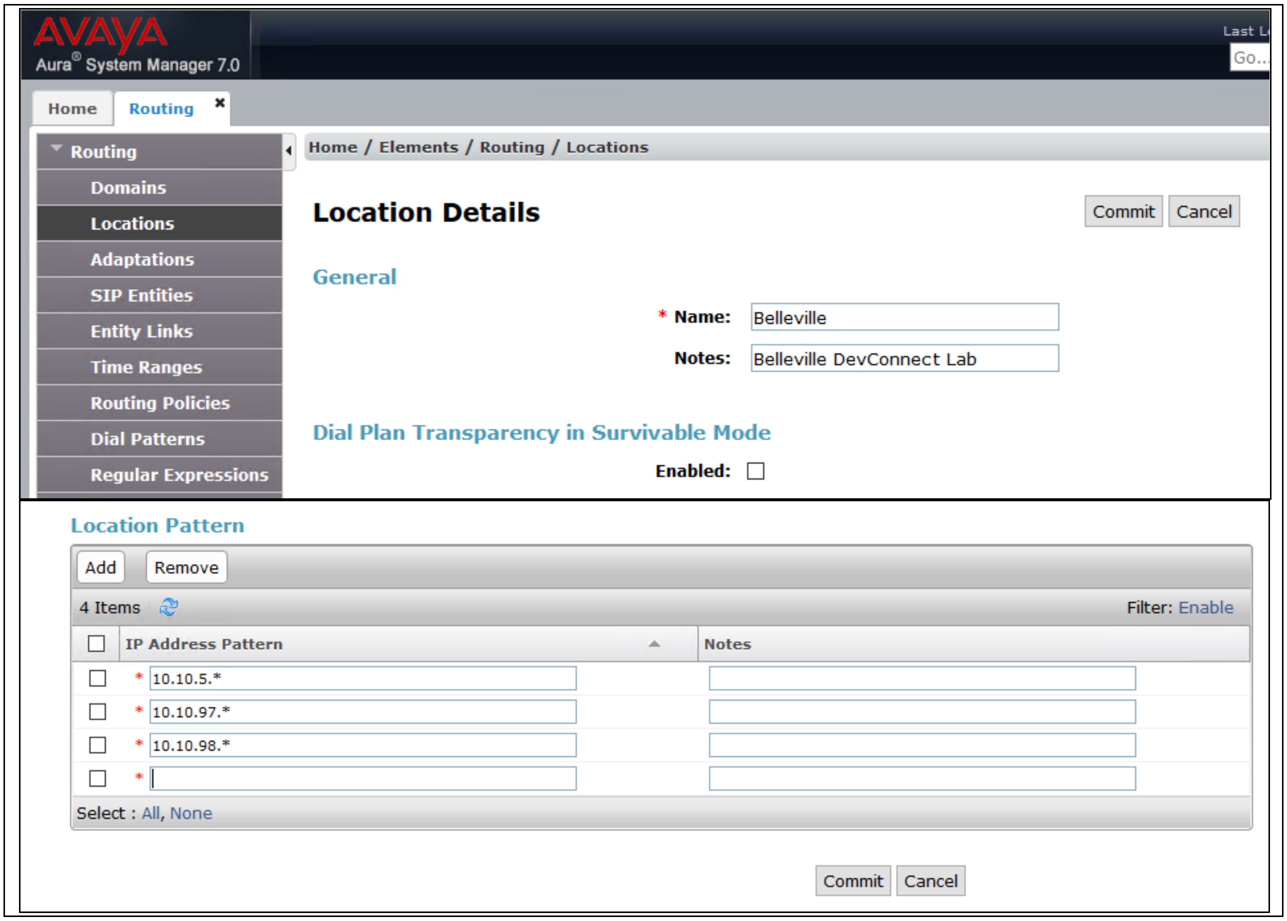
Navigate to **Routing→Locations** and click the **New** button (not shown) to add the location.

Under **General**:

- **Name**: a descriptive name
- **Notes**: optional descriptive text

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of all devices involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

Click **Commit** to save the configuration.



Location Details

General

* Name:	Belleville
Notes:	Belleville DevConnect Lab

Dial Plan Transparency in Survivable Mode

Enabled: □

Location Pattern

4 Items — Filter: Enable

□	IP Address Pattern	Notes
□	* 10.10.5.*	
□	* 10.10.97.*	
□	* 10.10.98.*	
□	*	

6.4. Add Adaptation

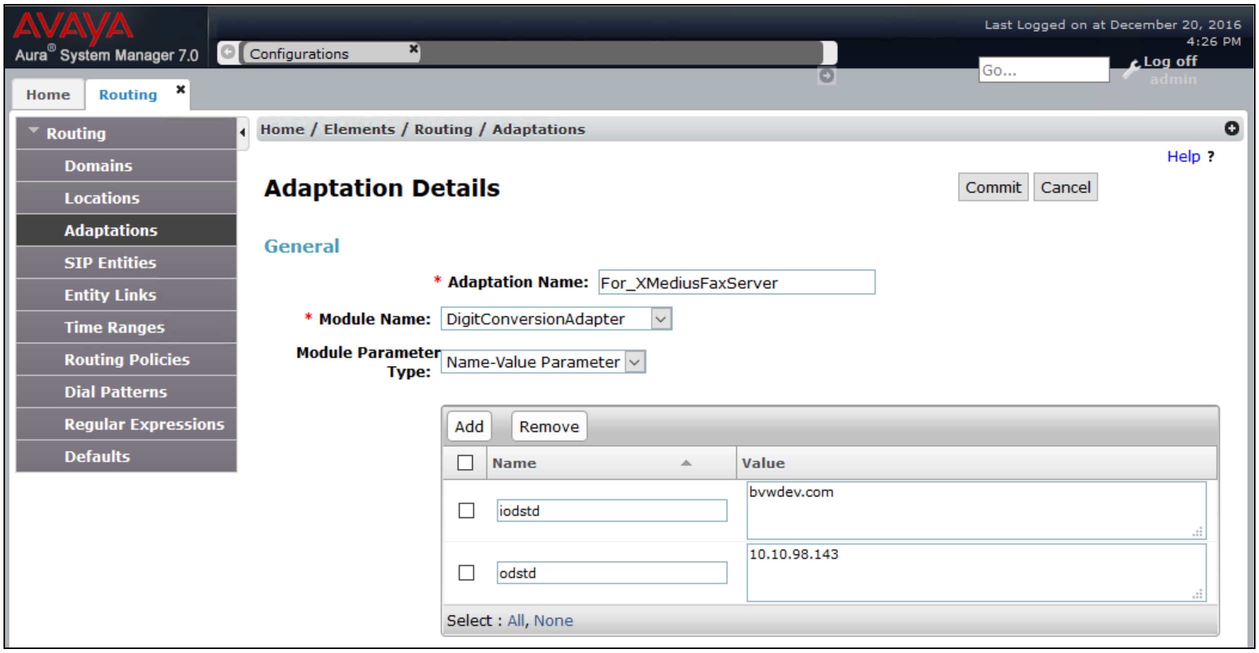
An Adaptation was created and applied to the XMediusFAX SIP entity to override the destination domain as shown below.

- **Adaptation Name:** Any descriptive name. During compliance testing ***For_XMediusFAXServer*** was used.
- **Module Name:** Select ***DigitConversionAdapter*** from the drop down menu.
- **Module Parameter Type:** Select ***Name-Value Parameter*** from the drop down menu.

Click on **Add** to add the following parameters:
The ingressOverrideDestinationDomain (**iodstd**) module parameter replaces the domain in the Request-URI, To Header (if administered), and Notify/message-summary body with ***bvwdev.com*** for ingress only.

The overrideDestinationDomain (**odstd**) module parameter replaces the domain in the Request-URI, To Header (if administered), Refer-To header, and Notify/message-summary body with the IP address of XMediusFAX ***10.10.98.143*** for egress only.

Retain default value for all other fields.



Adaptation Details

General

* Adaptation Name: For_XMediusFaxServer

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

□	Name	Value
□	iodstd	bvwdev.com
□	odstd	10.10.98.143

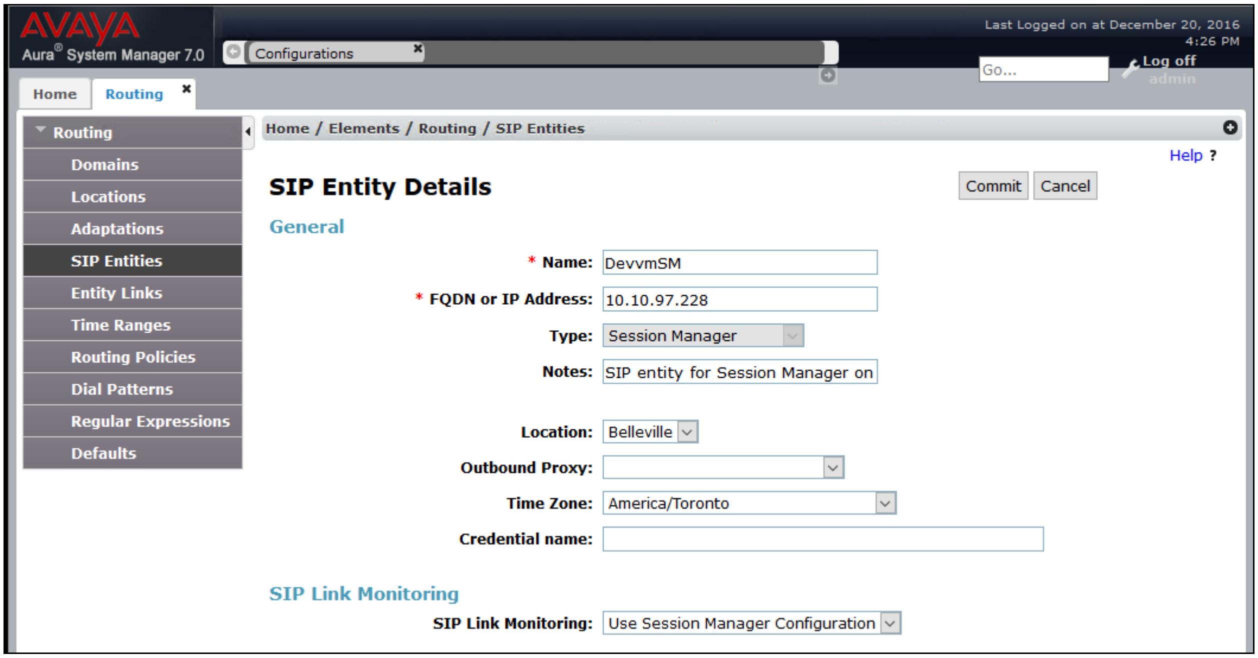
6.5. Add SIP Entities

A SIP entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP entity was added for the Session Manager, Communication Manager, and XMediusFAX.

Navigate to **Routing→SIP Entities**, and click the **New** button (not shown) to add a SIP entity. The configuration details for the SIP entity defined for Session Manager are as follows:

Under **General**:

- **Name**: A descriptive name.
- **FQDN or IP Address**: ***10.10.97.228***. This is the IP address assigned to the signaling interface of the Session Manager.
- **Type**: Select ***Session Manager***.
- **Notes**: Optional.
- **Location**: Select ***Belleville*** as configured in **Section 6.3**



SIP Entity Details

General

* Name: DevvmSM

* FQDN or IP Address: 10.10.97.228

Type: Session Manager

Notes: SIP entity for Session Manager on

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

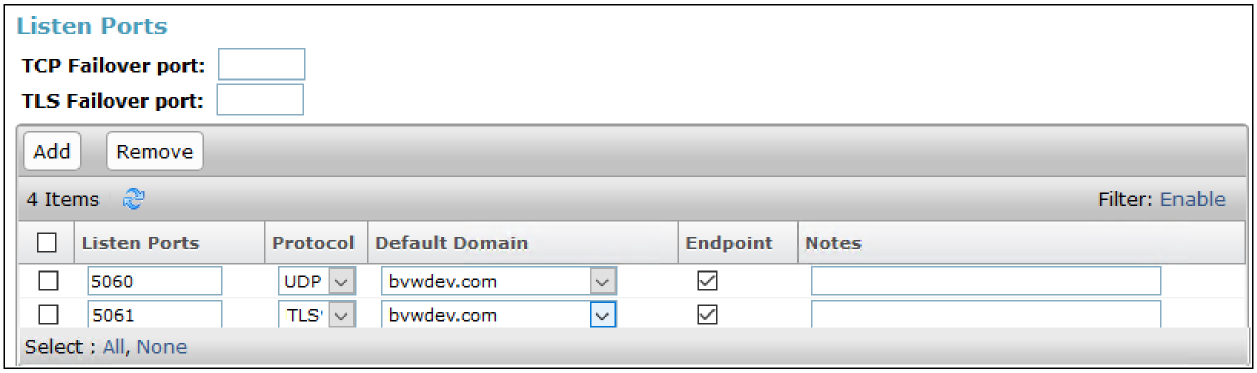
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Under **Listen Ports**, click **Add**, then edit the fields in the resulting new row as shown below:

- **Port**: ***5061***. This is the port number on which the system listens for SIP requests.
- **Protocol**: ***TLS***. The TLS transport protocol was used between Session Manager and Communication Manager as configured in **Section 5.5**.
- **Default Domain**: Select the SIP Domain created in **Section 6.2**.
- Repeat the three bullets above, but select ***5060*** for **Port** and ***UDP*** for **Protocol**. The UDP protocol was used between Session Manager and XMediusFAX.



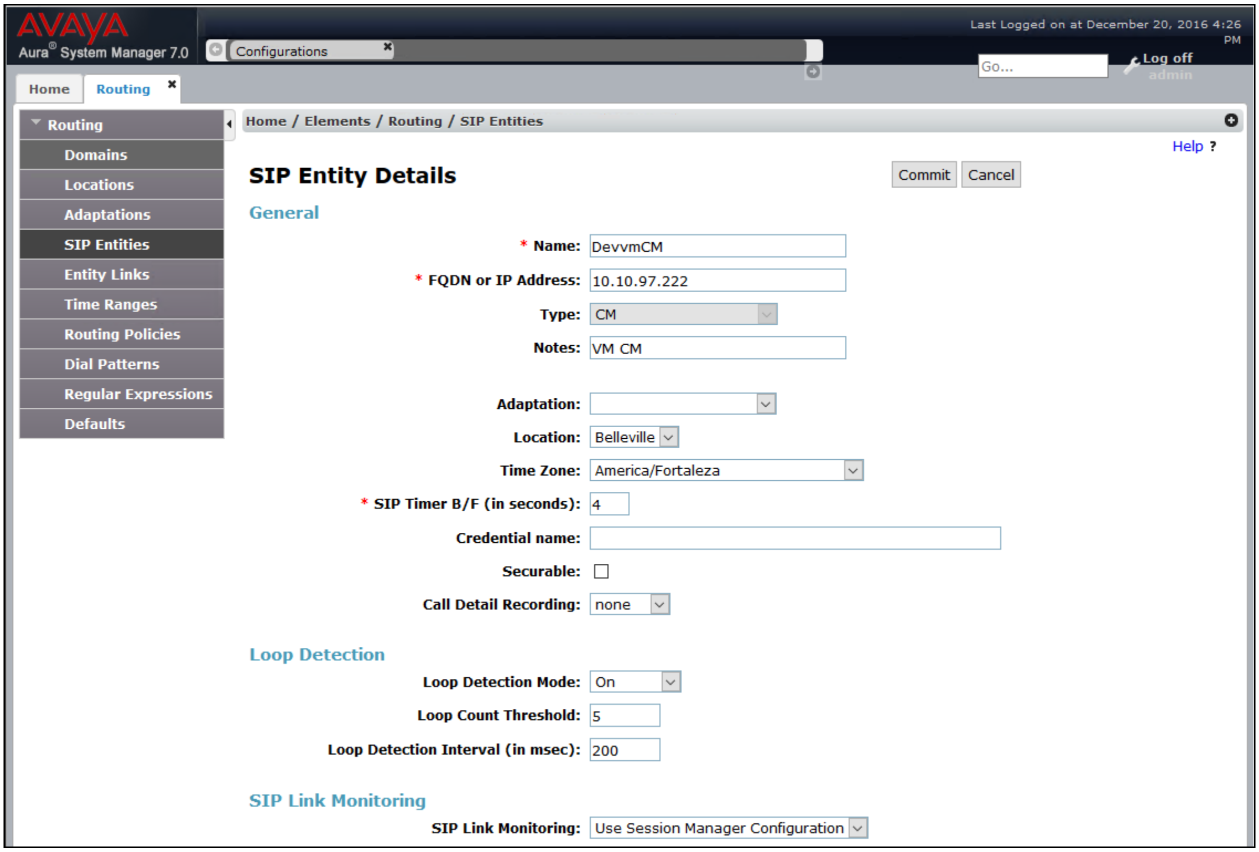
TCP Failover port:

TLS Failover port:

□	Listen Ports	Protocol	Default Domain	Endpoint	Notes
□	5060	UDP	bvwdev.com	☑	
□	5061	TLS	bvwdev.com	☑	

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

The screen below shows the SIP entity configuration details for Communication Manager. Note the ***CM*** selection for **Type**.



SIP Entity Details

General

* Name:	DevvmCM
* FQDN or IP Address:	10.10.97.222
Type:	CM
Notes:	VM CM
Adaptation:	
Location:	Belleville
Time Zone:	America/Fortaleza
* SIP Timer B/F (in seconds):	4
Credential name:	
Securable:	□
Call Detail Recording:	none

Loop Detection

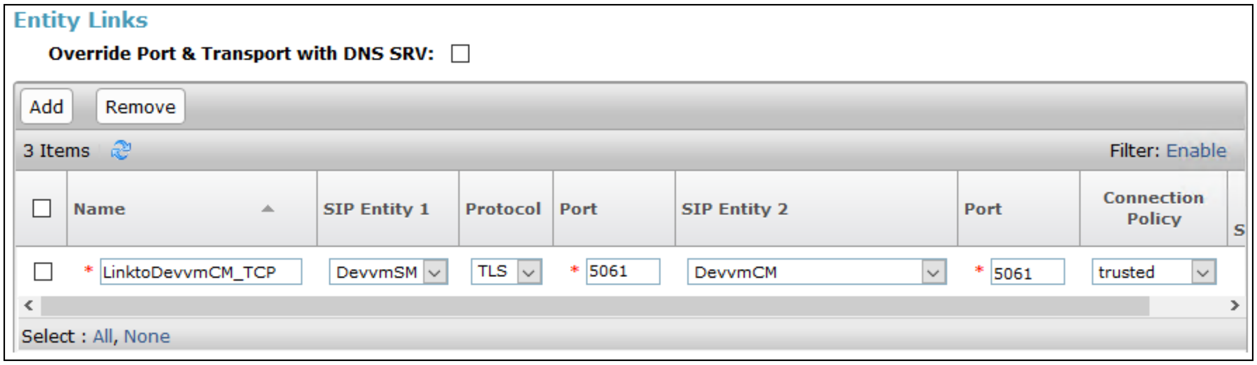
Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name**: A descriptive name
- **SIP Entity 1**: Select the Session Manager SIP entity as created in **Section 6.5**.
- **Protocol**: Select ***TLS*** as the transport protocol as configured in **Section 5.5**.
- **Port**: *5061*. This is the port number to which the other system sends SIP requests as configured in **Section 5.5**.
- **SIP Entity 2**: Select the Communication Manager SIP entity as created in **Section 6.5**.
- **Port**: *5061*. This is the port number on which the other system receives SIP requests.
- **Connection Policy**: Select ***trusted***.



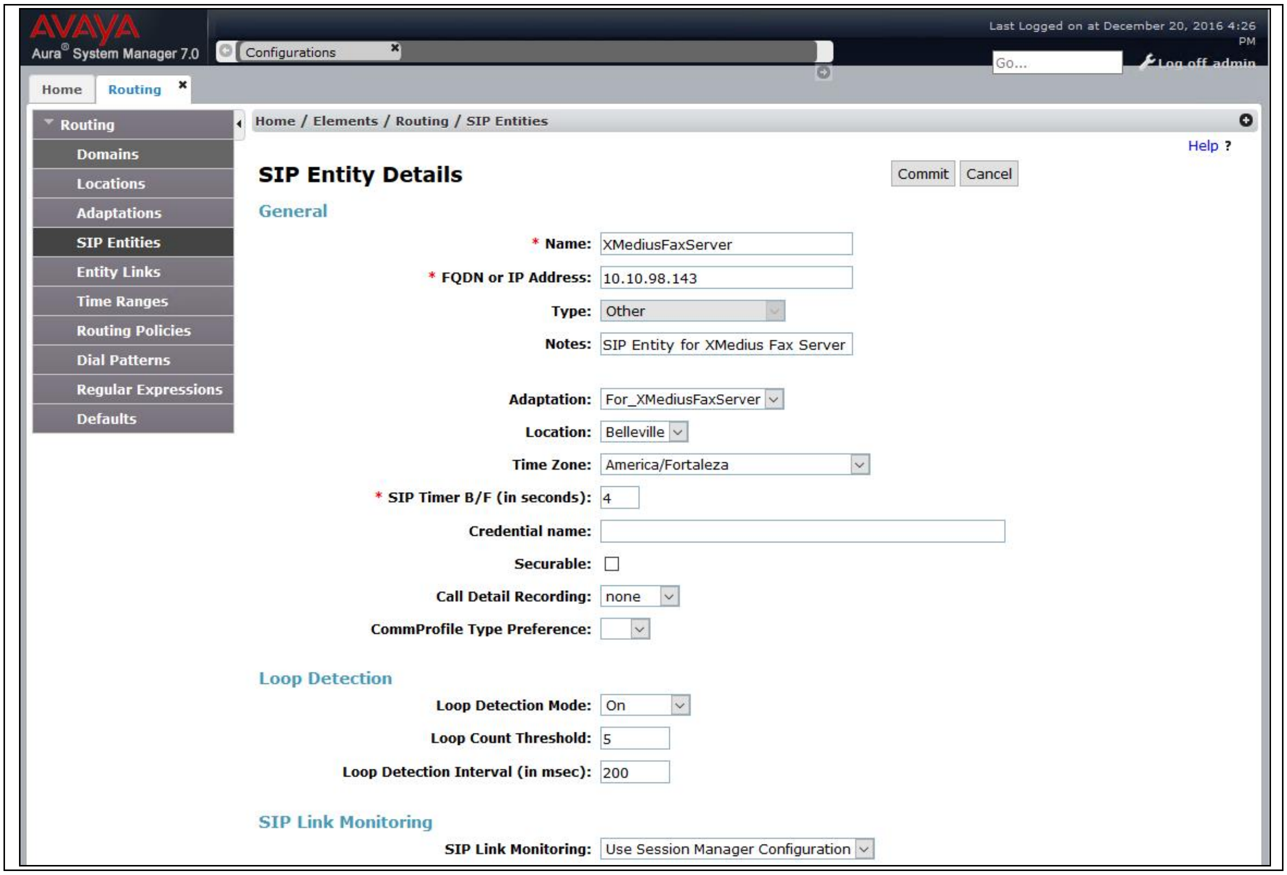
Entity Links

Override Port & Transport with DNS SRV: □

3 Items

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	* LinktoDevvmCM_TCP	DevvmSM	TLS	* 5061	DevvmCM	* 5061	trusted

The screen below shows the SIP entity configuration details for XMediusFAX. Note the ***Other*** selection for **Type**, and the **Adaptation** created in **Section 6.4** is selected.



SIP Entity Details

General

* Name:	XMediusFaxServer
* FQDN or IP Address:	10.10.98.143
Type:	Other
Notes:	SIP Entity for XMedius Fax Server
Adaptation:	For_XMediusFaxServer
Location:	Belleville
Time Zone:	America/Fortaleza
* SIP Timer B/F (in seconds):	4
Credential name:	
Securable:	□
Call Detail Recording:	none
CommProfile Type Preference:	

Loop Detection

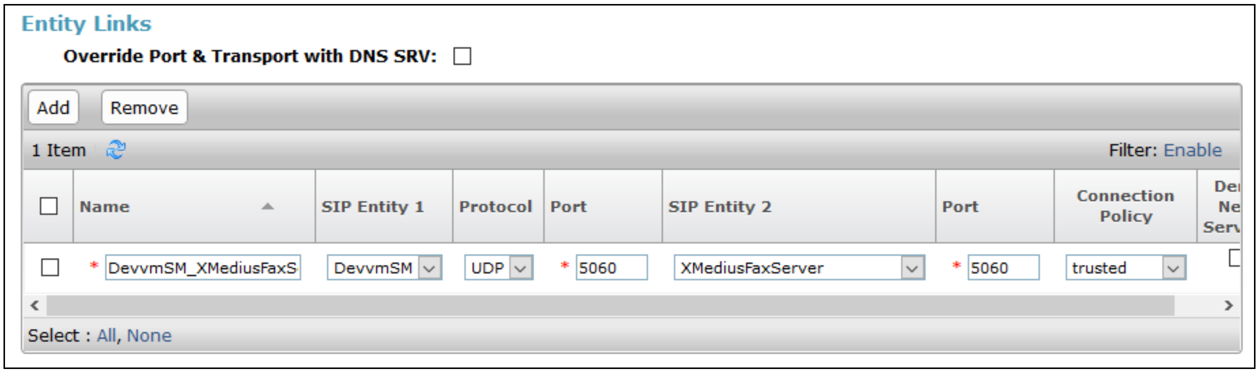
Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name**: A descriptive name.
- **SIP Entity 1**: Select the Session Manager SIP entity as created in **Section 6.5**.
- **Protocol**: Select ***UDP*** as the transport protocol.
- **Port**: *5060*. This is the port number to which the other system sends SIP requests.
- **SIP Entity 2**: Select the XMediusFAX SIP entity as created in **Section 6.5**.
- **Port**: *5060*. This is the port number on which the other system receives SIP requests.
- **Connection Policy**: Select ***trusted***.



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	De Ne Serv
□	* DevvmSM_XMediusFaxS	DevvmSM	UDP	* 5060	XMediusFaxServer	* 5060	trusted	□

6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP entities connected to the Session Manager. Two routing policies were added – one for routing calls to Communication Manager, and the other for routing calls to XMediusFAX.

Navigate to **Routing→Routing Policies**, and click the **New** button (not shown) to add a new Routing Policy.

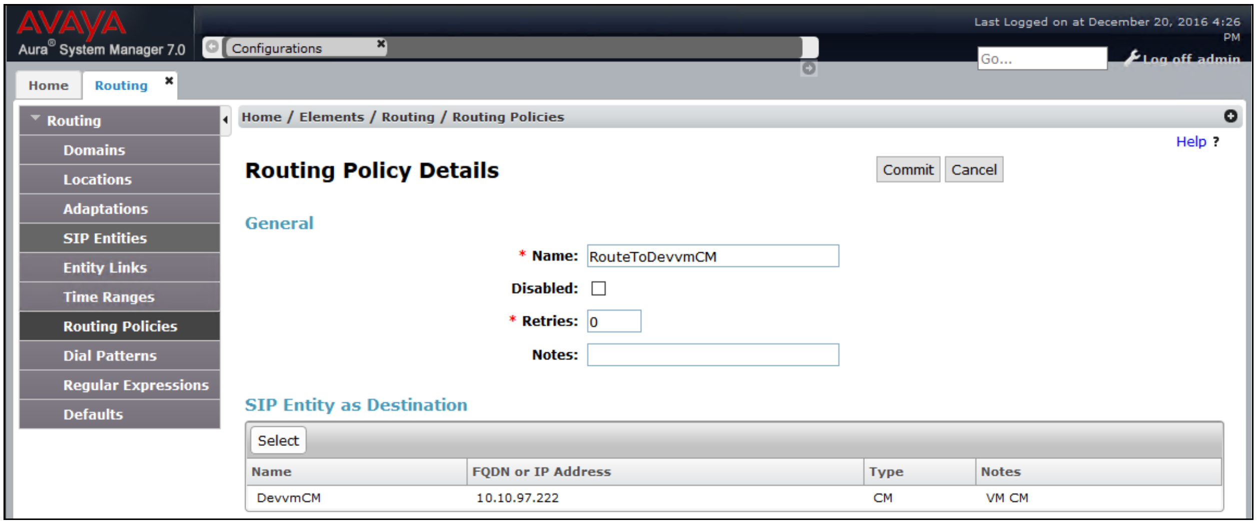
Under **General**:

- **Name**: A descriptive name.
- **Notes**: Optional descriptive text.

Under **SIP Entity as Destination**:
Click **Select** to select the appropriate SIP entity to which the routing policy applies (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

The screens below show the configuration details for the two Routing Policies used during compliance testing, one for Communication Manager and the other for XMediusFAX.



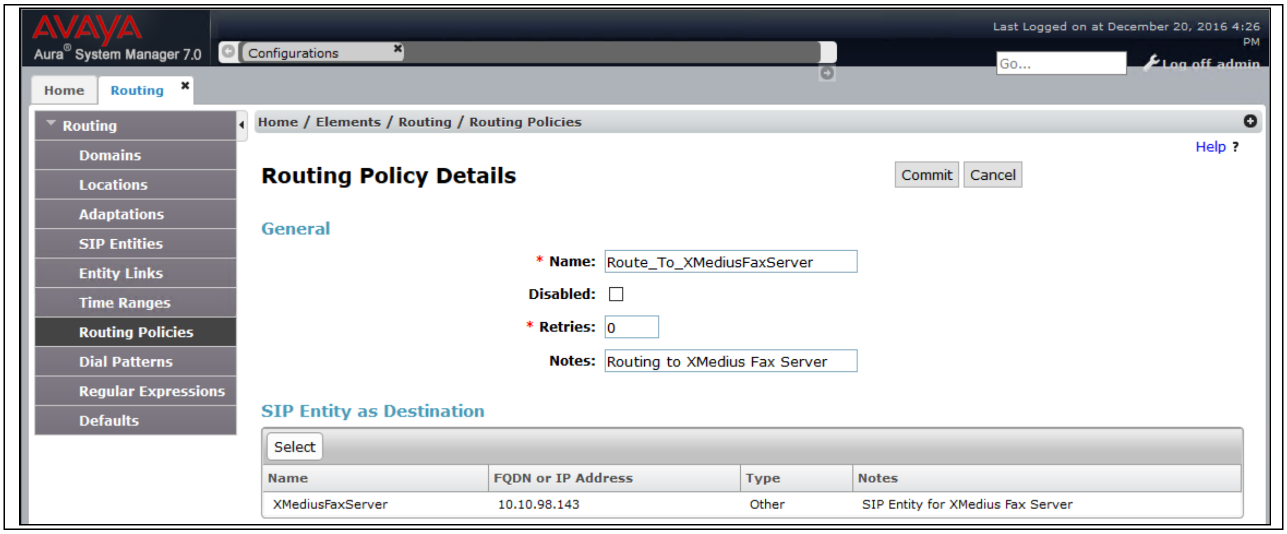
Routing Policy Details

General

* Name:	RouteToDevvmCM
Disabled:	□
* Retries:	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
DevvmCM	10.10.97.222	CM	VM CM



Routing Policy Details

General

* Name:	Route_To_XMediusFaxServer
Disabled:	□
* Retries:	0
Notes:	Routing to XMedius Fax Server

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
XMediusFaxServer	10.10.98.143	Other	SIP Entity for XMedius Fax Server

6.7. Add Dial Patterns

Dial patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP entities. During compliance testing three dial patterns were created. One for routing calls to G450 Gateway, one for G650 Gateway and the other for XMediusFAX.

Navigate to **Routing→Dial Patterns**, click the **New** button (not shown) to add a new dial pattern.

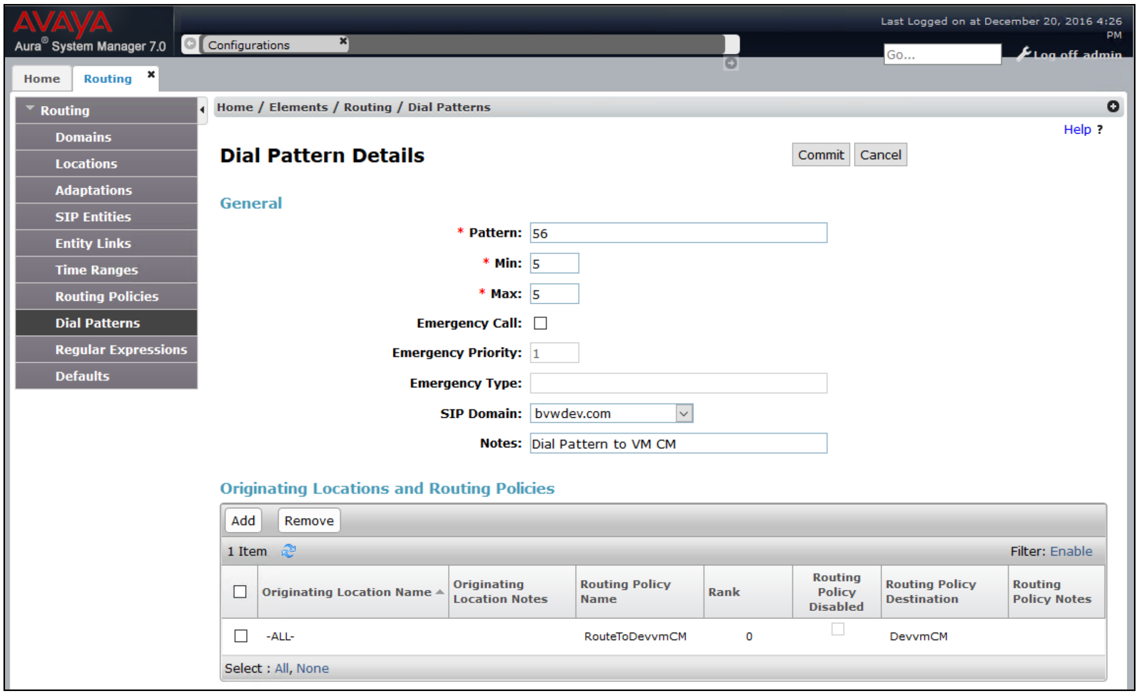
Under **General**:

- **Pattern**: Dialed number or prefix
- **Min**: Minimum length of dialed number
- **Max**: Maximum length of dialed number
- **SIP Domain**: select the SIP domain created in **Section 6.2** (or select **–ALL–** to be less restrictive)
- **Notes**: Optional descriptive text

Under **Originating Locations and Routing Policies**:
Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

The screens below shows the configuration details for the dial pattern defined for routing calls to Communication Manager with G450 Gateway. Similarly other patterns can be added for other entities.



Dial Pattern Details

General

* Pattern:	56
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev.com
Notes:	Dial Pattern to VM CM

Originating Locations and Routing Policies

1 Item

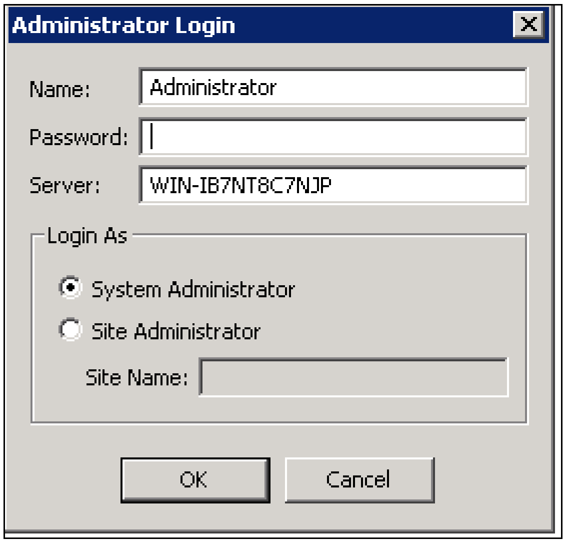
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		RouteToDevvmCM	0	□	DevvmCM	

7. Configure XMedius Solutions Inc XMediusFAX On-Premises

This section describes the configuration of XMediusFAX. It assumes that the application and all required software components have been installed and properly licensed. The number of channels supported by XMediusFAX is controlled via an XMediusFAX server license file. For instructions on sending and receiving faxes, consult the XMediusFAX Administrator Guide and User Guide as mentioned in **Section 10**.

7.1. Launch the Application

On the XMediusFAX server, launch the XMediusFAX application from the Windows Start Menu. Navigate to **Start → All Programs → XMediusFAX → XMediusFAX**. A login screen appears. Log in with proper credentials and click the **OK** button.



Name: Administrator

Password:

Server: WIN-IB7NT8C7NJP

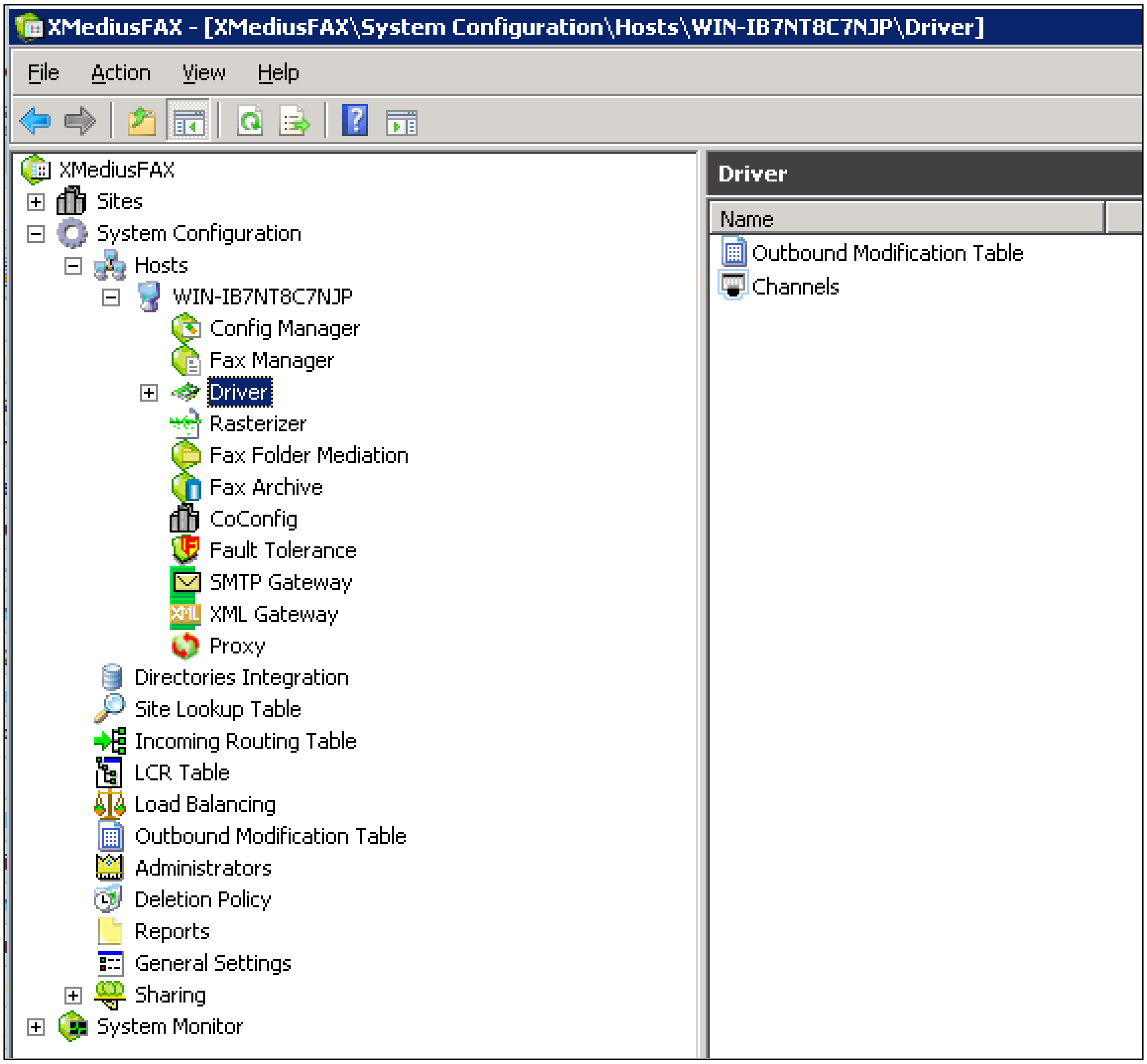
● System Administrator

○ Site Administrator

Site Name:

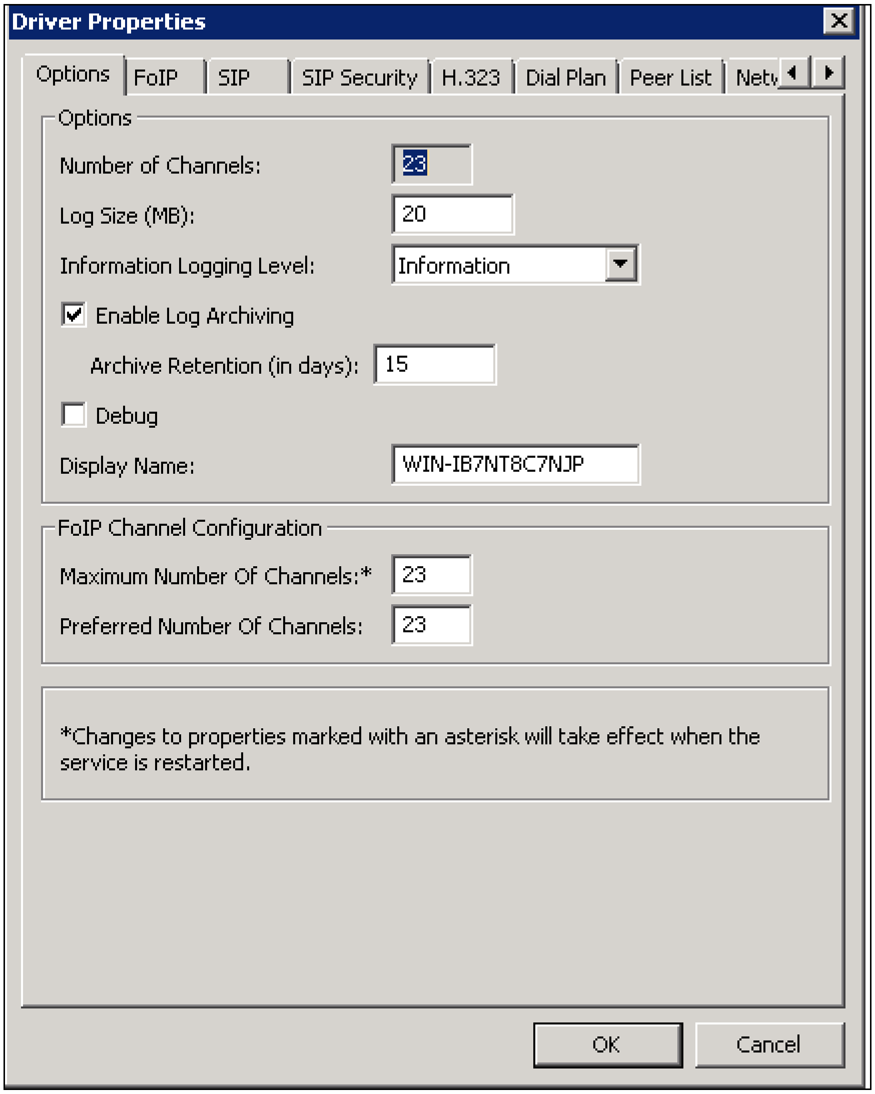
7.2. Configure Driver Properties

On the main screen, navigate to **XMediusFAX** → **System Configuration** → **Hosts** → **WIN-IB7NT8C7NJP** → **Driver** in the left hand tree menu, where **WIN-IB7NT8C7NJP** is the server computer name. Select **Properties** (not shown) by right-clicking on **Driver**.



7.2.1. General Options

On the **Driver Properties** screen, select the **Options** tab, set the **Maximum Number Of Channels** and **Preferred Number Of Channels** fields under **FoIP Channel Configuration** to the number of simultaneous faxes to be processed. Retain default values for all other fields.



Options

Number of Channels: 23

Log Size (MB): 20

Information Logging Level: Information

☑ Enable Log Archiving

Archive Retention (in days): 15

☐ Debug

Display Name: WIN-IB7NT8C7NJP

FoIP Channel Configuration

Maximum Number Of Channels:* 23

Preferred Number Of Channels: 23

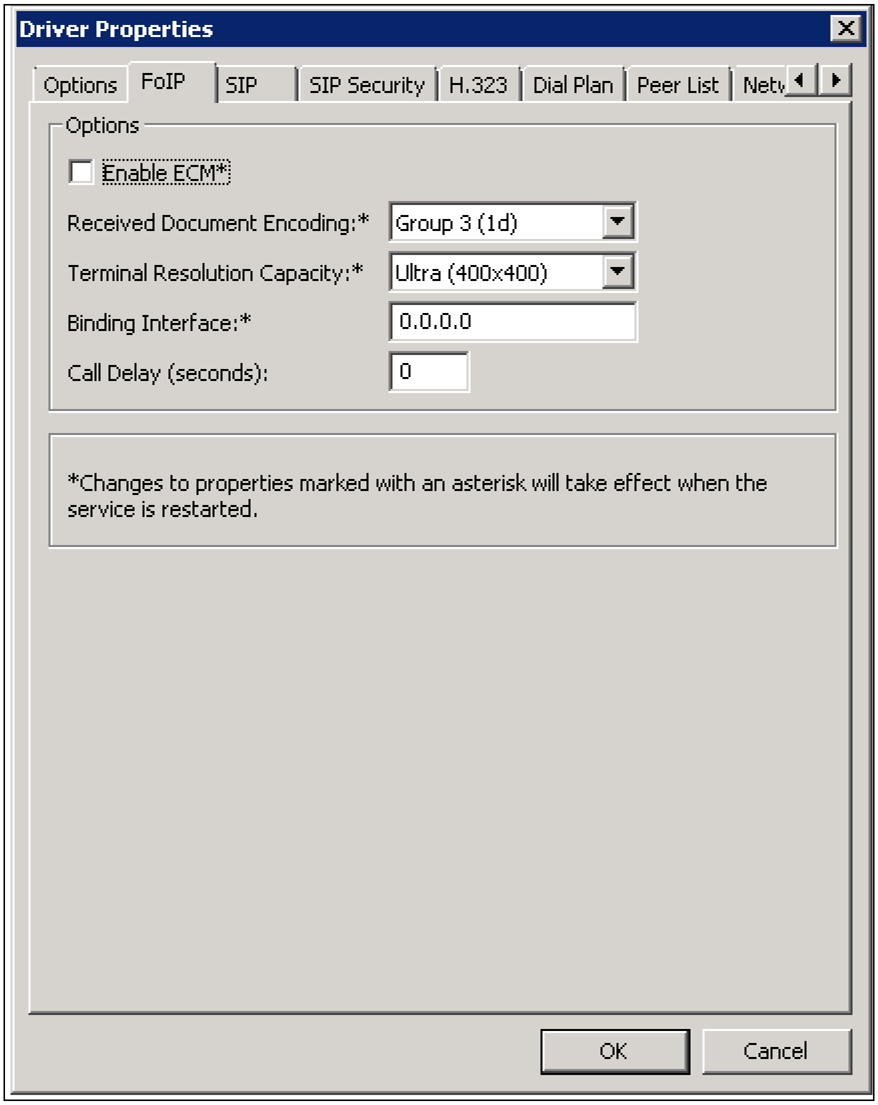
*Changes to properties marked with an asterisk will take effect when the service is restarted.

7.2.2. FoIP Parameters

On the **Driver Properties** screen, select the **FoIP** tab and configure the fields as follows:

- **Received Document Encoding** – Set this field to the highest encoding allowed. For the compliance test, this value was set to ***Group 3 (1d)***.
- **Terminal Resolution Capacity** – Set this field to the highest resolution allowed for incoming calls. For the compliance test, this value was set to ***Ultra (400x400)***.
- The **Enable ECM** box needs to be checked if error correction mode is desired.

Retain default values for all other fields.



Options

□ Enable ECM*

Received Document Encoding:* Group 3 (1d)

Terminal Resolution Capacity:* Ultra (400x400)

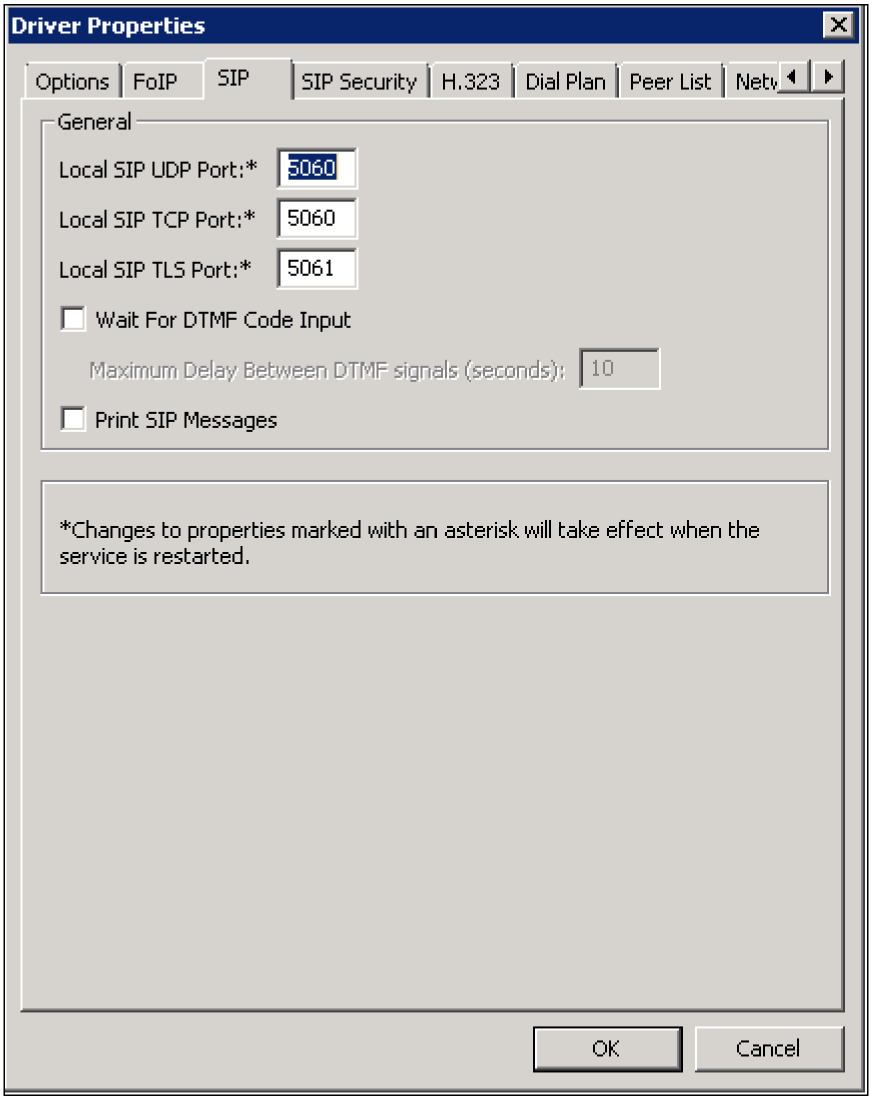
Binding Interface:* 0.0.0.0

Call Delay (seconds): 0

*Changes to properties marked with an asterisk will take effect when the service is restarted.

7.2.3. SIP Parameters

On the **Driver Properties** screen, select the **SIP** tab. Configure the **Local SIP UDP Port** field to match the UDP **Port** field of the fax server SIP entity link entry configured in **Section 6.5**. During compliance testing, UDP was used as the transport layer protocol by XMediusFAX.



Local SIP UDP Port:* 5060

Local SIP TCP Port:* 5060

Local SIP TLS Port:* 5061

□ Wait For DTMF Code Input

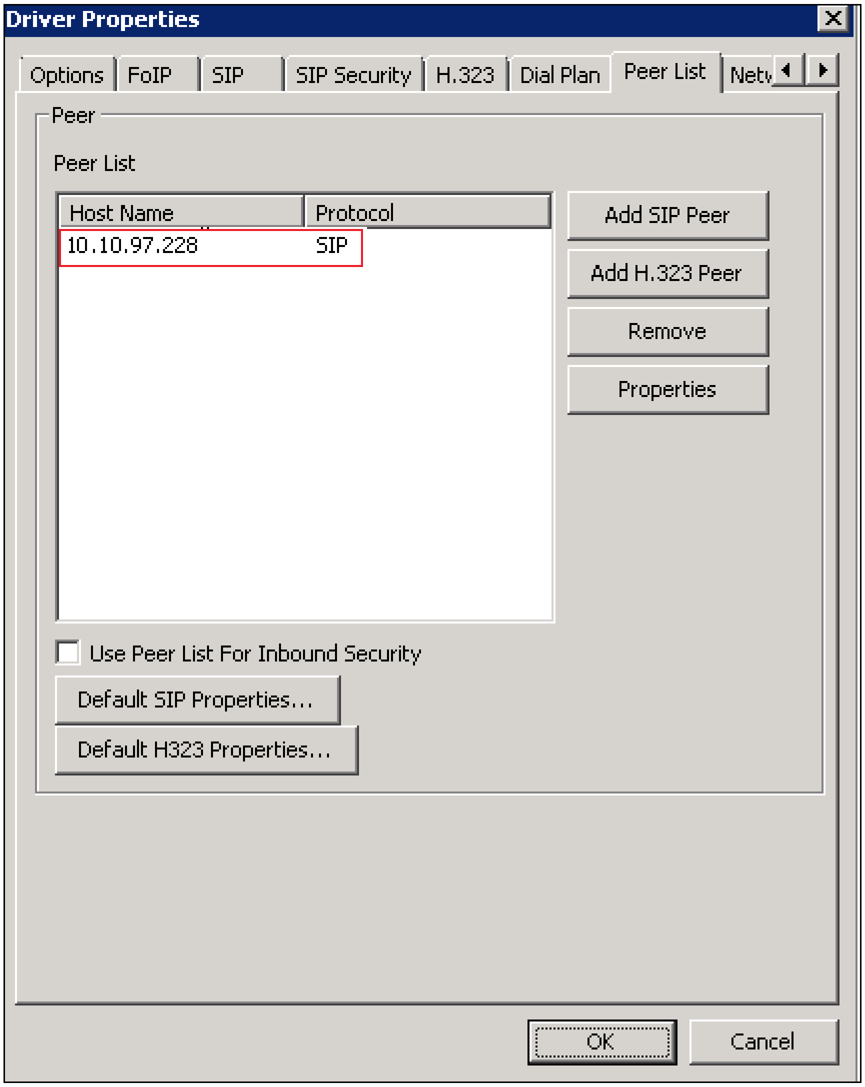
Maximum Delay Between DTMF signals (seconds): 10

□ Print SIP Messages

*Changes to properties marked with an asterisk will take effect when the service is restarted.

7.2.4. Peer List

On the **Driver Properties** screen, select the **Peer List** tab. To add a new SIP peer, select the **Add SIP Peer** button and enter the values shown in **Section 7.2.5**. To view an existing peer, highlight the peer in the list and click **Properties**. The example below shows the peer list after the Session Manager interface ***10.10.97.228*** has been added to the list.



Driver Properties

Options | FoIP | SIP | SIP Security | H.323 | Dial Plan | Peer List | Netw

Peer

Peer List

Host Name	Protocol
10.10.97.228	SIP

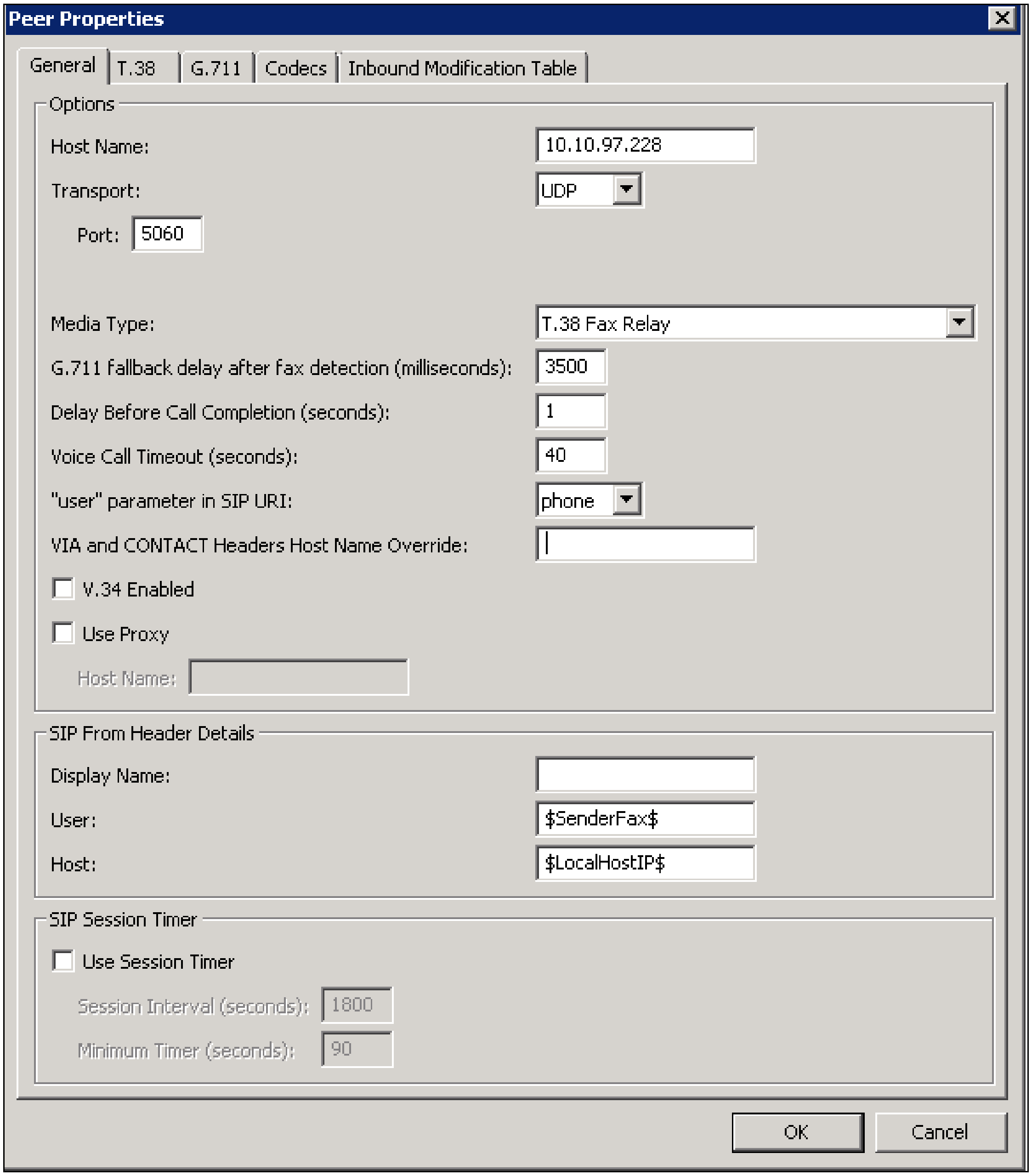
□ Use Peer List For Inbound Security

7.2.5. Peer Properties for Session Manager

On the **Peer Properties** screen, configure as follows:

- **Host Name** – Set this field to the IP address of Session Manager.
- **Transport -** Set this field to ***UDP***. During compliance testing, UDP was used as the transport layer protocol by XMediusFAX as configured in **Section 6.5**.
- **Port** - Set this field to ***5060*** as configured in **Section 6.5**.
- **Media Type** – Set this field to ***T.38 Fax Relay*** for the T.38 fax mode, or ***G.711 Passthrough*** for the pass-through fax mode.

Retain default values for all other fields.



Options

Host Name: 10.10.97.228

Transport: UDP

Port: 5060

Media Type: T.38 Fax Relay

G.711 fallback delay after fax detection (milliseconds): 3500

Delay Before Call Completion (seconds): 1

Voice Call Timeout (seconds): 40

"user" parameter in SIP URI: phone

VIA and CONTACT Headers Host Name Override:

□ V.34 Enabled

□ Use Proxy

Host Name:

SIP From Header Details

Display Name:

User: $SenderFax$

Host: $LocalHostIP$

SIP Session Timer

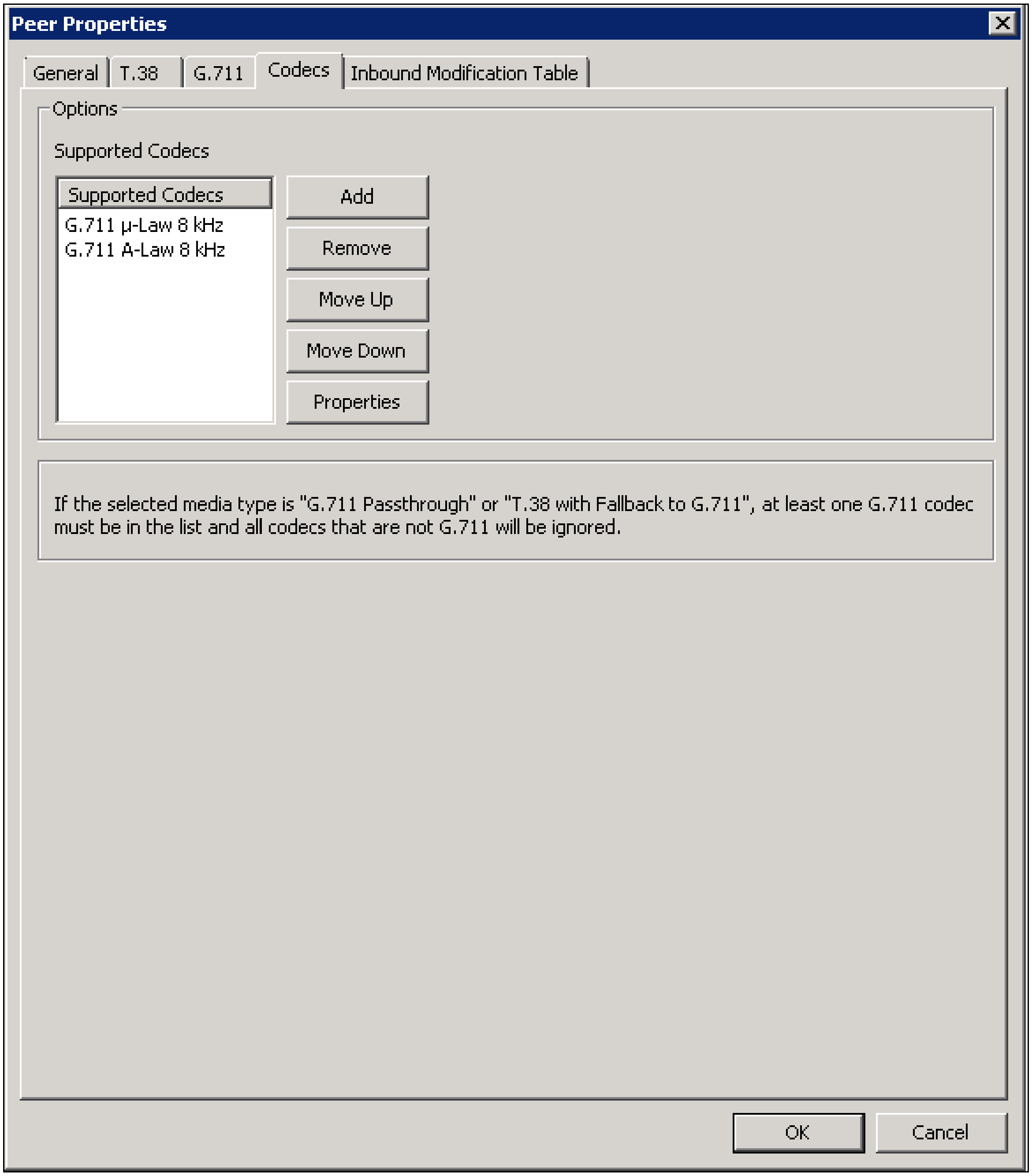
□ Use Session Timer

Session Interval (seconds): 1800

Minimum Timer (seconds): 90

7.2.6. Codec

On the **Peer Properties** screen, select the **Codec** tab. To add a codec for the SIP peer, select the **Add** button and select the values from the drop-down menu. To view an existing codec, highlight the codec in the list and click **Properties**. The example below shows the default codec list supported by the newly added SIP peer

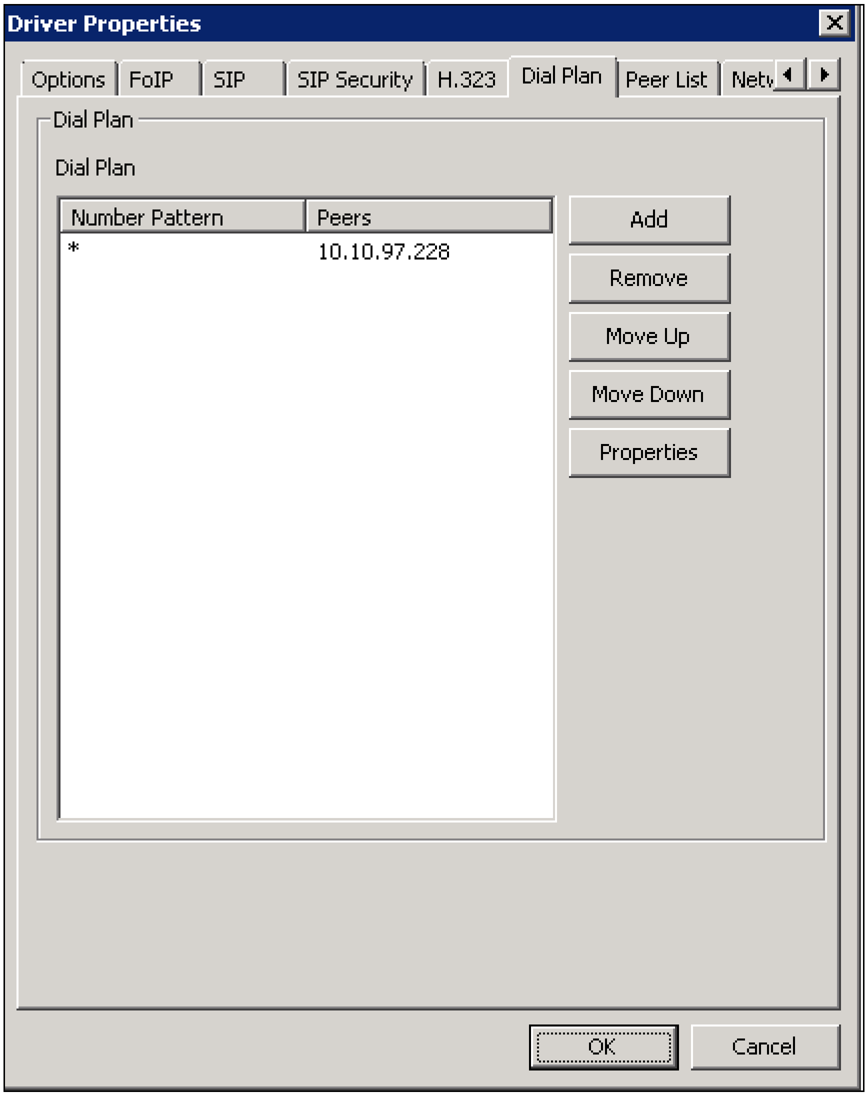


G.711 µ-Law 8 kHz
G.711 A-Law 8 kHz

If the selected media type is "G.711 Passthrough" or "T.38 with Fallback to G.711", at least one G.711 codec must be in the list and all codecs that are not G.711 will be ignored.

7.2.7. Dial Plan

On the **Driver Properties** screen, select the **Dial Plan** tab. To add a new entry to the dial plan, select the **Add** button and enter the values shown in **Section 7.2.8**. To view an existing entry, highlight the entry in the list and click **Properties** to get the **Number Pattern Properties** screen. The example below shows the dial plan after the entry for ***** (any value) has been added to the list.

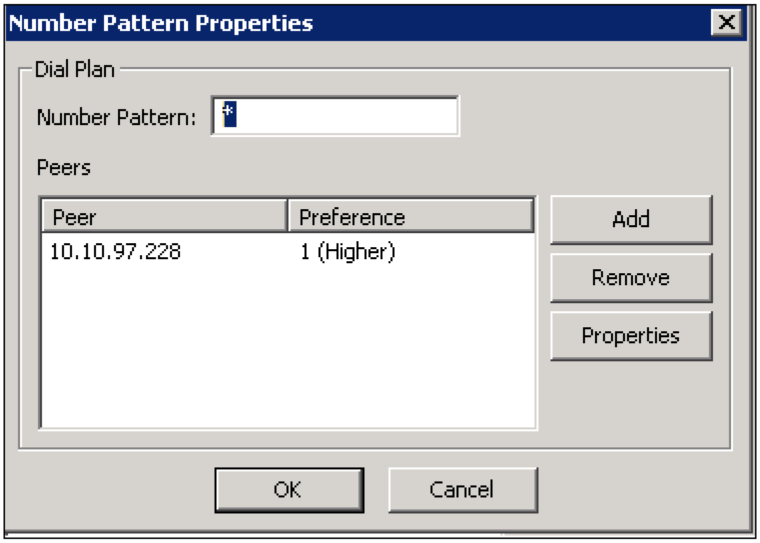


Number Pattern	Peers
*	10.10.97.228

7.2.8. Number Pattern Properties

On the **Number Pattern Properties** screen, configure as follows:

- **Number Pattern** – Set this field to the pattern to match. In this example, the value of ***** indicates any dialed number is acceptable.
- **Peers** – Click the **Add** button. In the **Peer Properties** window that appears (not shown), enter the **Peer** IP address as configured in **Section 7.2.5** and **Preference** value of ***1*** and click **OK**. In this example, only one peer is configured.



Number Pattern: *

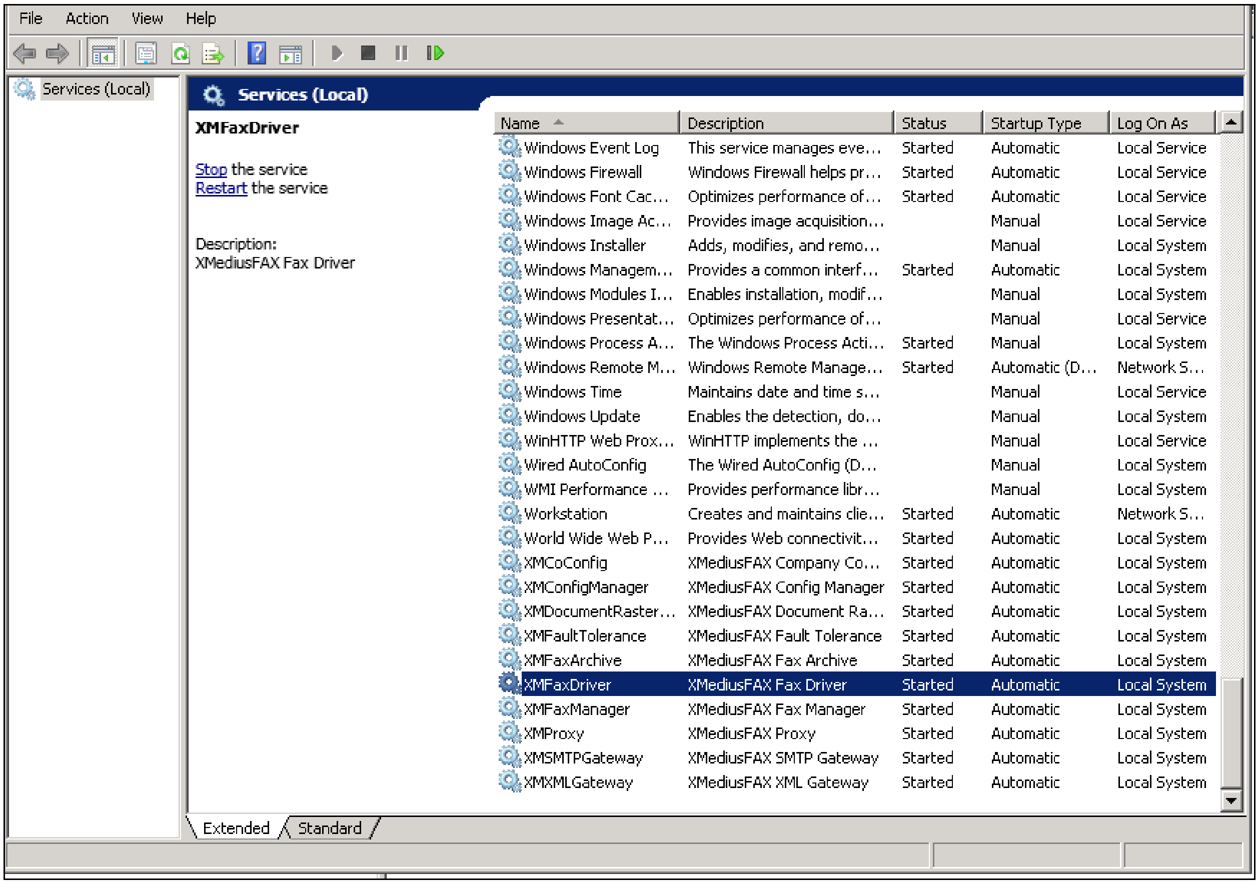
Peers

Peer	Preference
10.10.97.228	1 (Higher)

Lastly, click **OK** on the **Driver Properties** screen shown in **Section 7.2.7**, to accept the Driver Configuration.

7.2.9. Restart XMFaxDriver Service

Once all the driver properties have been configured, go to **Start → Control Panel → Administrative Tools → Services** to stop and start the **XMFaxDriver** service to make the changes take effect.



XMFaxDriver

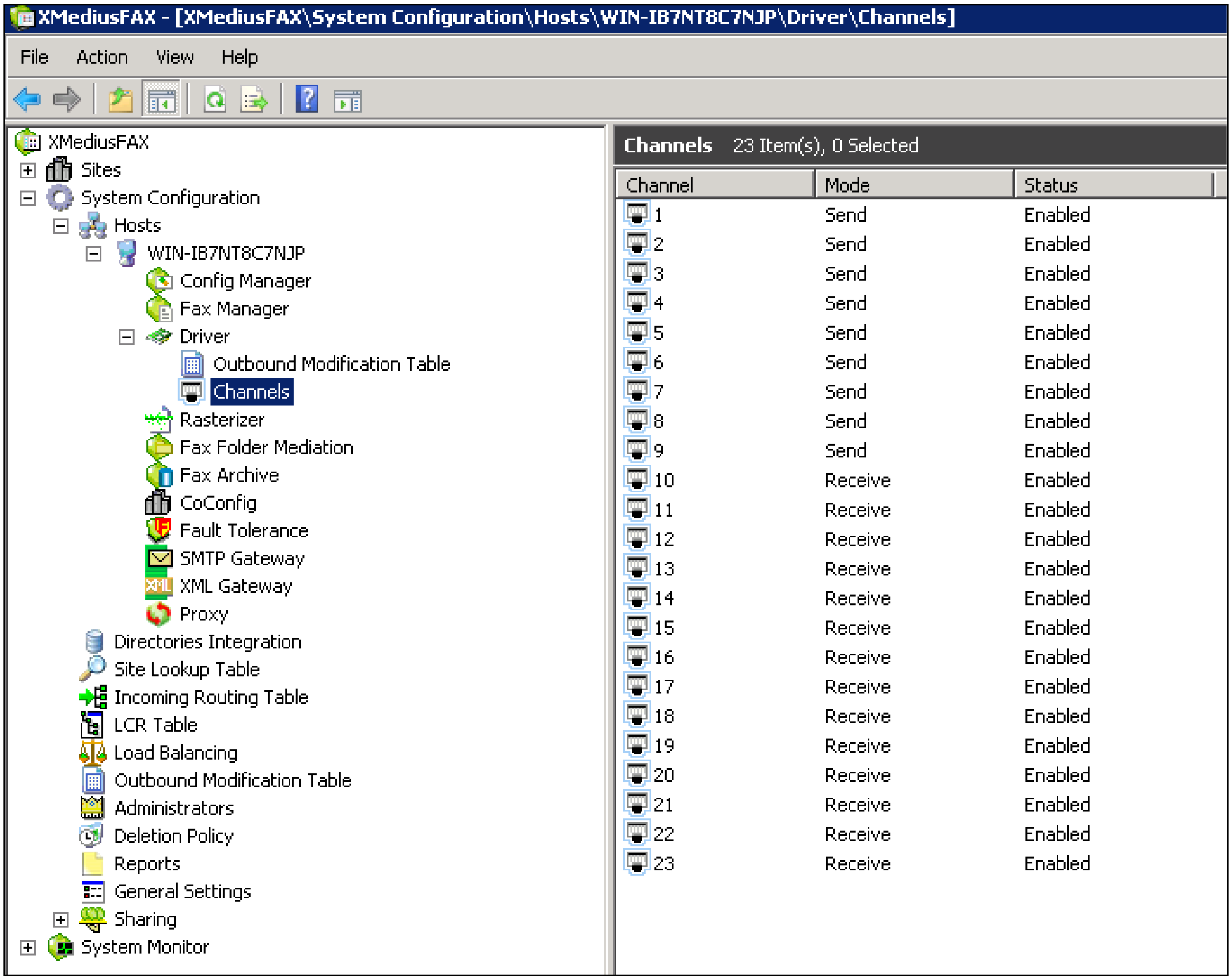
Stop the service
Restart the service

Description:
XMediusFAX Fax Driver

Name	Description	Status	Startup Type	Log On As
Windows Event Log	This service manages eve...	Started	Automatic	Local Service
Windows Firewall	Windows Firewall helps pr...	Started	Automatic	Local Service
Windows Font Cac...	Optimizes performance of...	Started	Automatic	Local Service
Windows Image Ac...	Provides image acquisition...		Manual	Local Service
Windows Installer	Adds, modifies, and remo...		Manual	Local System
Windows Managem...	Provides a common interf...	Started	Automatic	Local System
Windows Modules I...	Enables installation, modif...		Manual	Local System
Windows Presentat...	Optimizes performance of...		Manual	Local Service
Windows Process A...	The Windows Process Acti...	Started	Manual	Local System
Windows Remote M...	Windows Remote Manage...	Started	Automatic (D...	Network S...
Windows Time	Maintains date and time s...		Manual	Local Service
Windows Update	Enables the detection, do...		Manual	Local System
WinHTTP Web Prox...	WinHTTP implements the ...		Manual	Local Service
Wired AutoConfig	The Wired AutoConfig (D...		Manual	Local System
WMI Performance ...	Provides performance libr...		Manual	Local System
Workstation	Creates and maintains clie...	Started	Automatic	Network S...
World Wide Web P...	Provides Web connectivit...	Started	Automatic	Local System
XMCoConfig	XMediusFAX Company Co...	Started	Automatic	Local System
XMConfigManager	XMediusFAX Config Manager	Started	Automatic	Local System
XMDocumentRaster...	XMediusFAX Document Ra...	Started	Automatic	Local System
XMFaultTolerance	XMediusFAX Fault Tolerance	Started	Automatic	Local System
XMFaxArchive	XMediusFAX Fax Archive	Started	Automatic	Local System
XMFaxDriver	XMediusFAX Fax Driver	Started	Automatic	Local System
XMFaxManager	XMediusFAX Fax Manager	Started	Automatic	Local System
XMProxy	XMediusFAX Proxy	Started	Automatic	Local System
XMSMTPGateway	XMediusFAX SMTP Gateway	Started	Automatic	Local System
XMXMLGateway	XMediusFAX XML Gateway	Started	Automatic	Local System

7.3. Configure Channels

On the main screen, navigate to **XMediusFAX → System Configuration → Hosts → WIN-IB7NT8C7NJP → Driver → Channels** in the left hand tree menu. Set the **Mode** to ***Send***, ***Receive*** or ***Both*** (not shown) by right-clicking on each of the channels in the right pane. During compliance testing, 9 channels were set to ***Send*** and 14 channels were set to ***Receive***.



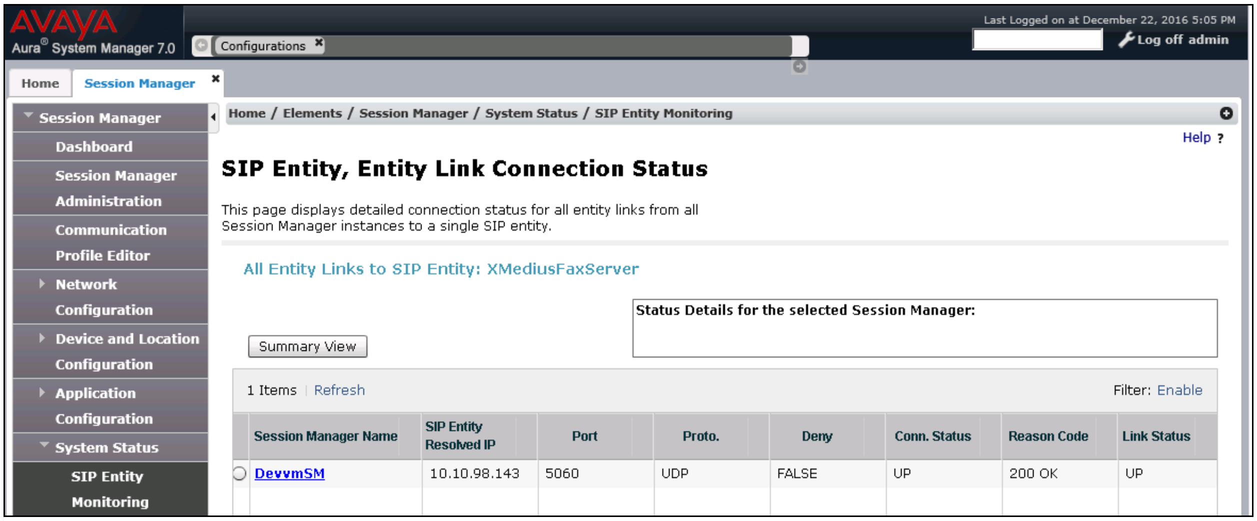
Channels 23 Item(s), 0 Selected

Channel	Mode	Status
1	Send	Enabled
2	Send	Enabled
3	Send	Enabled
4	Send	Enabled
5	Send	Enabled
6	Send	Enabled
7	Send	Enabled
8	Send	Enabled
9	Send	Enabled
10	Receive	Enabled
11	Receive	Enabled
12	Receive	Enabled
13	Receive	Enabled
14	Receive	Enabled
15	Receive	Enabled
16	Receive	Enabled
17	Receive	Enabled
18	Receive	Enabled
19	Receive	Enabled
20	Receive	Enabled
21	Receive	Enabled
22	Receive	Enabled
23	Receive	Enabled

8. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager→System Status→SIP Entity Monitoring**, and click on the appropriate SIP entity to verify that the entity links to Communication Manager and XMediusFAX are up. Screen below shows the XMediusFAX entity link that was configured in **Section 6.5**.


AVAYA
Aura® System Manager 7.0
Configurations
Last Logged on at December 22, 2016 5:05 PM
Log off admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Home / Elements / Session Manager / System Status / SIP Entity Monitoring
Help ?
Summary View
Filter: Enable

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: XMediusFaxServer

Status Details for the selected Session Manager:

1 Items | Refresh

	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	DevvmSM	10.10.98.143	5060	UDP	FALSE	UP	200 OK	UP

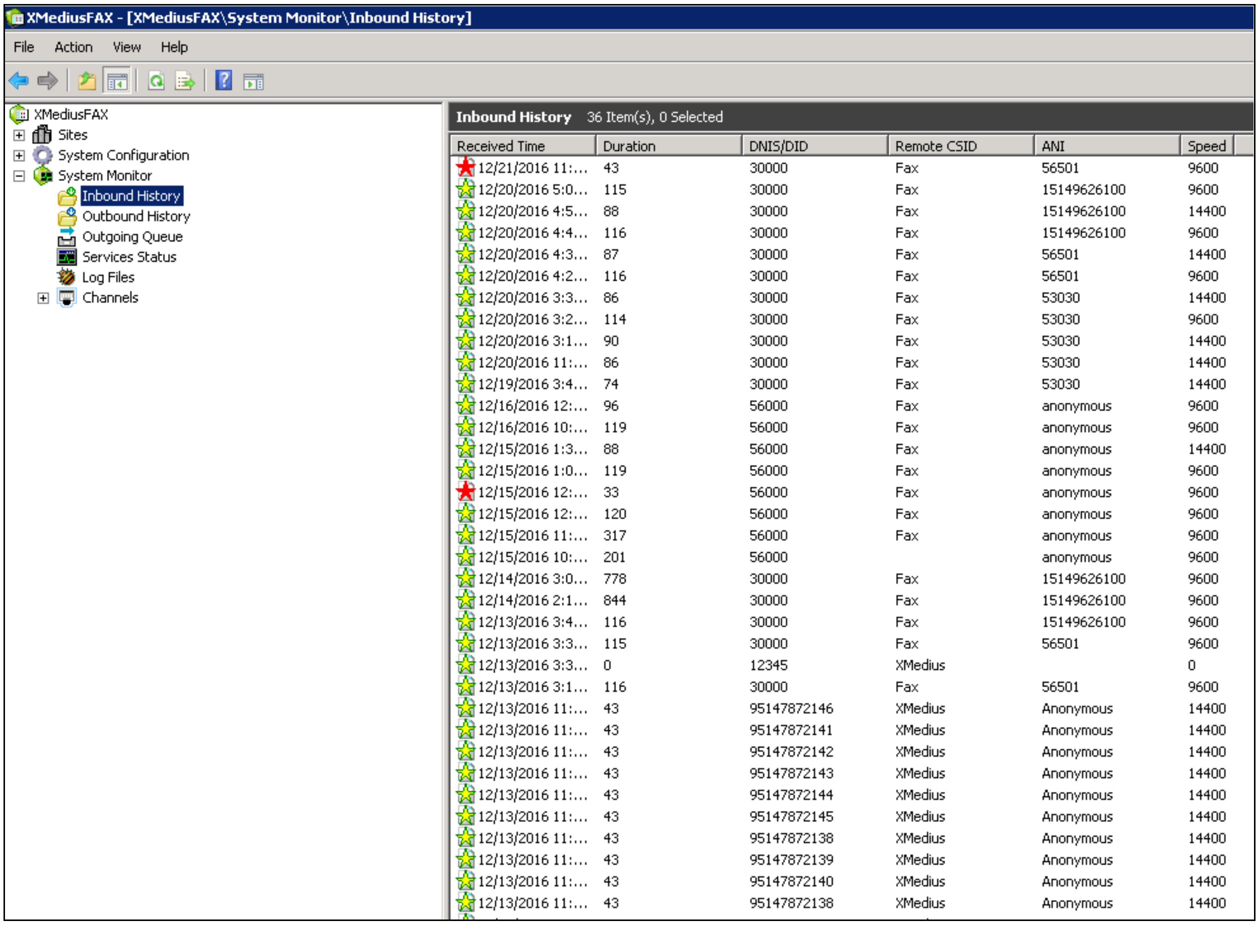
- From the Communication Manager SAT, use the **status signaling-group *x*** command to verify that the SIP signaling group is in-service (where ***x*** is the signaling group number associated with the trunk between Communication Manager and Session Manager as configured in **Section 5.5**).

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

- From the Communication Manager SAT, use the **status trunk *y*** command to verify that the SIP trunk group is in-service (where ***y*** is the trunk group number for the trunk between Communication Manager and Session Manager as configured in **Section 5.6**).

```
status trunk 1                                                      Page   1

                             TRUNK GROUP STATUS

Member    Port      Service State        Mtce Connected Ports
                                         Busy

0001/001 T00001    in-service/idle      no
0001/002 T00002    in-service/idle      no
```

- Verify that fax calls can be placed to/from XMediusFAX at each site. Example below shows the Inbound History of faxes received.



Inbound History 36 Item(s), 0 Selected

Received Time	Duration	DNIS/DID	Remote CSID	ANI	Speed
12/21/2016 11:...	43	30000	Fax	56501	9600
12/20/2016 5:0...	115	30000	Fax	15149626100	9600
12/20/2016 4:5...	88	30000	Fax	15149626100	14400
12/20/2016 4:4...	116	30000	Fax	15149626100	9600
12/20/2016 4:3...	87	30000	Fax	56501	14400
12/20/2016 4:2...	116	30000	Fax	56501	9600
12/20/2016 3:3...	86	30000	Fax	53030	14400
12/20/2016 3:2...	114	30000	Fax	53030	9600
12/20/2016 3:1...	90	30000	Fax	53030	14400
12/20/2016 11:...	86	30000	Fax	53030	14400
12/19/2016 3:4...	74	30000	Fax	53030	14400
12/16/2016 12:...	96	56000	Fax	anonymous	9600
12/16/2016 10:...	119	56000	Fax	anonymous	9600
12/15/2016 1:3...	88	56000	Fax	anonymous	14400
12/15/2016 1:0...	119	56000	Fax	anonymous	9600
12/15/2016 12:...	33	56000	Fax	anonymous	9600
12/15/2016 12:...	120	56000	Fax	anonymous	9600
12/15/2016 11:...	317	56000	Fax	anonymous	9600
12/15/2016 10:...	201	56000		anonymous	9600
12/14/2016 3:0...	778	30000	Fax	15149626100	9600
12/14/2016 2:1...	844	30000	Fax	15149626100	9600
12/13/2016 3:4...	116	30000	Fax	15149626100	9600
12/13/2016 3:3...	115	30000	Fax	56501	9600
12/13/2016 3:3...	0	12345	XMedius		0
12/13/2016 3:1...	116	30000	Fax	56501	9600
12/13/2016 11:...	43	95147872146	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872141	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872142	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872143	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872144	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872145	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872138	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872139	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872140	XMedius	Anonymous	14400
12/13/2016 11:...	43	95147872138	XMedius	Anonymous	14400

9. Conclusion

These Application Notes describe the procedures required to configure XMedius Solutions Inc. XMediusFAX On-Premises to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support the network shown in **Figure 1A** and **1B**. XMedius Solutions Inc. XMediusFAX On-Premises passed compliance testing with the observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2 May 2016.
2. *Deploying Avaya Aura® System Manager*, Release 7.0.1, Issue 2 August 2016.
3. *Administering Avaya Aura® System Manager for Release 7.0.1*, Release 7.0.1, Issue 3 January 2017.
4. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, 03-300509, Issue 2.1 August 2016.
5. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0.1, 555-245-205, Issue 3 October 2016.

Product documentation for XMediusFAX may be obtained from XMedius Solutions Inc.

7. *XMediusFAX Administrator Guide, Version Number 8.0.0.334, March 2016*.
8. *XMediusFAX Installation Guide, Version Number 8.0.0.334, March 2016*.
9. *XMediusFAX User Guide, Version Number 8.0.0.334, March 2016*.

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.