Application Notes for Configuring XMedius XM Fax Software with Avaya Aura® Communication Manager and Avaya Aura® Session Manager via SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the XMedius Fax Software version 9.0 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Session Manager 8.0 via SIP trunk.

XMedius XM Fax is fax software that sends and receives fax calls over an IP network. In the tested configuration, the XMedius XM Fax interoperated with Avaya Aura® Session Manager to send/receive faxes using SIP trunk facilities.

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 XM Fax (XM Fax) Software version 9.0 with Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager) using SIP trunks.

XMedius XM Fax is host-based Fax over IP that uses the web interface to send and receive fax calls over an IP network. In the tested configuration, XM Fax interoperated with Avaya Aura® Session Manager to send/receive faxes using a SIP trunk interface.

2. General Test Approach and Test Results

This section describes the compliance test approach used to verify interoperability of XM Fax with Session Manager. By using a SIP trunk that was established between the Communication Manager and XM Fax via Session Manager, faxes were sent and received between these two systems.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the XMedius XM Fax does not utilize TLS and secure media encryption features as requested by XMedius.

2.1. Interoperability Compliance Testing

The compliance test tested interoperability between XM Fax and Session Manager by making intra-site fax calls between XM Fax software client and an analog fax machine that was connected to a Communication Manager via Session Manager using SIP trunks. For inter-site fax, calls were made between XM Fax and an analog fax machine that was connected on a remote site. The remote site connection used SIP trunk through Avaya Session Border Controller that connects to SIP service provider (PSTN). Specifically, the following fax operations were tested in the setup for the compliance test:

- Fax from/to XM Fax software client to/from fax machine at a local site
- Fax from/to XM Fax software client to/from fax machine at a remote site (PSTN)

Both T.38 standard and G.711 pass-through were tested. Faxes were sent with various page lengths and resolutions.

Serviceability testing included verifying proper operation/recovery from failed cables, unavailable resources, and restarts of XM Fax services.

Fax calls were also tested with the integrated VoIP engine of the Avaya G450 Media Gateway and the Avaya MM760 Media Module installed in the Avaya G450 Media Gateway.

2.2. Test Results

XM Fax successfully passed all compliance testing with the following observations:

- The Fax transmission rate depends on the Media Gateway or the card being used. In a G450 Media gateway, the negotiation is seen at V.29 (9600 bits).
- XM Fax does not recognize SIP domain in the host part of request header for incoming fax call, it rejects the call with 404 Not Found. To overcome this issue, use an adaptation in Session Manager to replace the SIP domain with IP address of the XM Fax server. Refer **Section 6.4** for more detail.

Note1: Fax calls consume DSP (Digital Signal Processing) resources for processing fax data on the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G450 Media Gateway. To increase the capacity to support simultaneous fax calls, additional Avaya MM760 Media Module or Modules need to be installed in the Avaya G450 Media Gateway. Customers should work with their Avaya sales representatives to ensure that their fax solutions have adequate licenses and DSP resources to match the intended Fax capacity/usage.

Note2: The SIP trunk group on Communication Manager for connecting to Session Manager at each site, as well as the SIP trunk group for connecting the two sites, must be configured with adequate number of trunk group members to support the number of simultaneous fax calls intended.

2.3. Support

North American Technical support for XM Fax Software can be obtained by contacting XMedius at.

- North America: +1 514-787-2100
- EMEA: +33 (0) 1 70 92 13 10
- Email: info@xmedius.com
- Website: https://support.xmediusfax.com/hc/en-us

3. Reference Configuration

The test configuration was designed to emulate a local site and a remote site. **Figure 1** illustrates the configuration used in these Application Notes. In the sample configuration, Communication Manager, G450 Media Gateway, Avaya Aura® Session Manager, System Manager, XM Fax and an analog fax machine are considered to be a local site. The XM Fax software client communicates to the Communication Manager via the Session Manager using SIP UDP. In turn, Communication Manager used a SIP Trunk to communicate with Session Manager. An analog fax port is configured on the Communication Manager to which a fax machine is connected. The equipment involved in the remote site is beyond the scope of this document and is shown here for reference only. The local and remote sites communicate via SIP trunks that are configured between the Communication Manager, Session Manager and the PBXs available at the remote site.

- Bi-directional faxed between XM Fax software client and the local fax endpoint 1 that connected to an analog port in the G450 Media Gateway.
- Bi-directional faxes between XM Fax software client and PSTN fax endpoint 2 via SIP trunk.

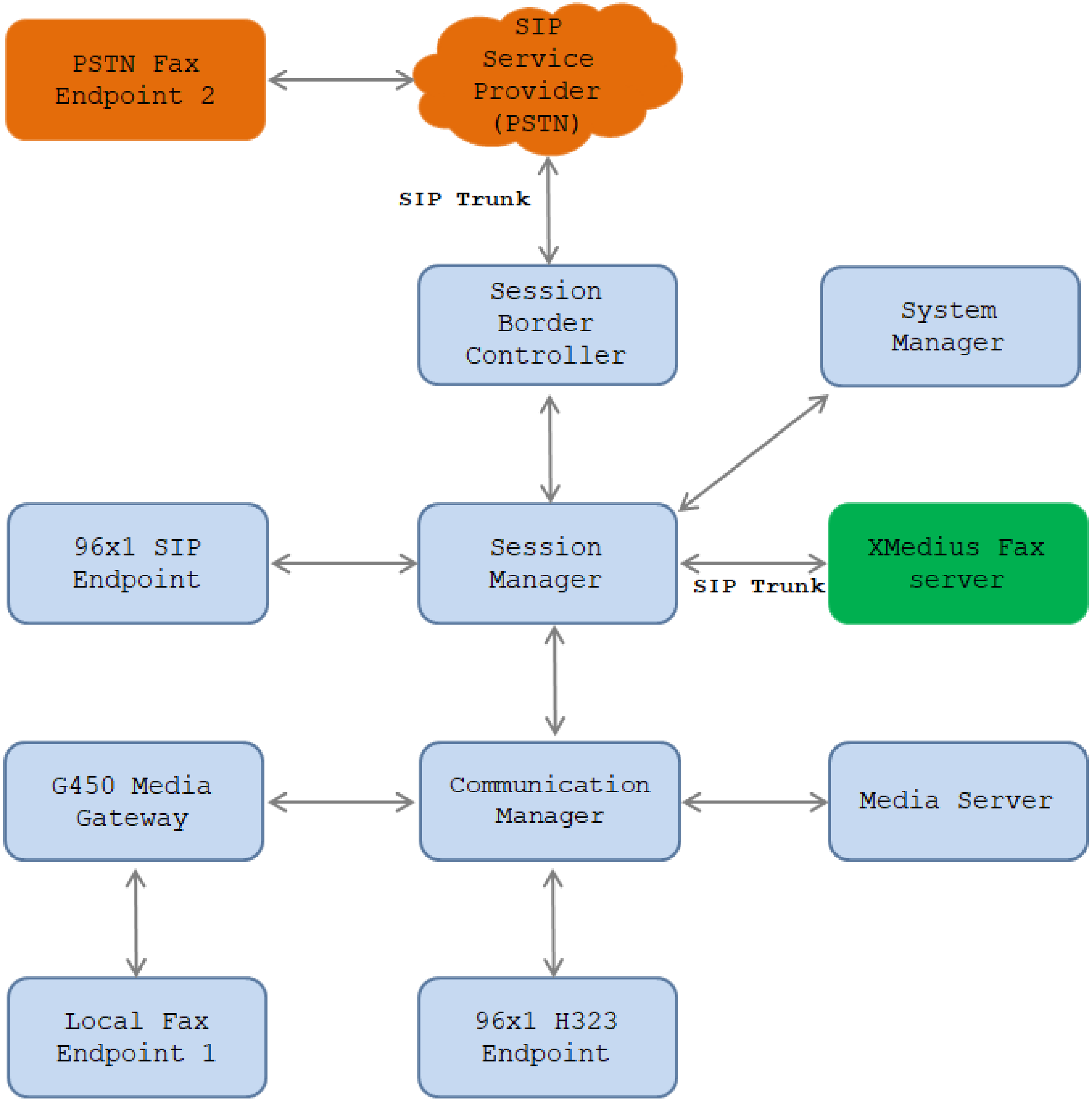


Figure 1: XMedius XM Fax interoperating with Session Manager via SIP Trunk

4. Equipment and Software Validated

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

Equipment	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	8.1.1.0 R018x.01.0.890.0 Patch 25763
Avaya Aura® System Manager running on Virtualized Environment	8.1.1.0 Build 8.1.0.0.733078
Avaya Aura® Session Manager running on Virtualized Environment	8.1.1.0 Build 8.1.1.0.811021
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.150
Avaya G.450 Media Gateway	41.16.0
Avaya 96x1 IP Deskphones	6.8 7.1.7 (SIP)
XMedius XM Fax Software running on Microsoft Windows 10	9.0.0.562

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with Session Manager and XM Fax. It focuses on the configuration of the SIP trunks connecting Communication Manager to the Avaya SIP infrastructure with the following assumptions:

- The examples shown in this section refer to the local site.
- The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, the **save translation** command was used to make the changes permanent.

The procedures for configuring Communication Manager include the following areas:

- Verify Communication Manager License
- Administer IP Node Names
- Administer Codecs
- Administer IP Network Region
- Administer Signaling Group
- Administer Trunk Group
- Administer Private Numbering
- Administer Outbound Routing

5.1. Verify Communication Manager License

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

The license file installed on the system controls the maximum permitted. If there is 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: 12000 20
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 2
                   Maximum Video Capable IP Softphones: 18000 6
                       Maximum Administered SIP Trunks: 12000 58
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```

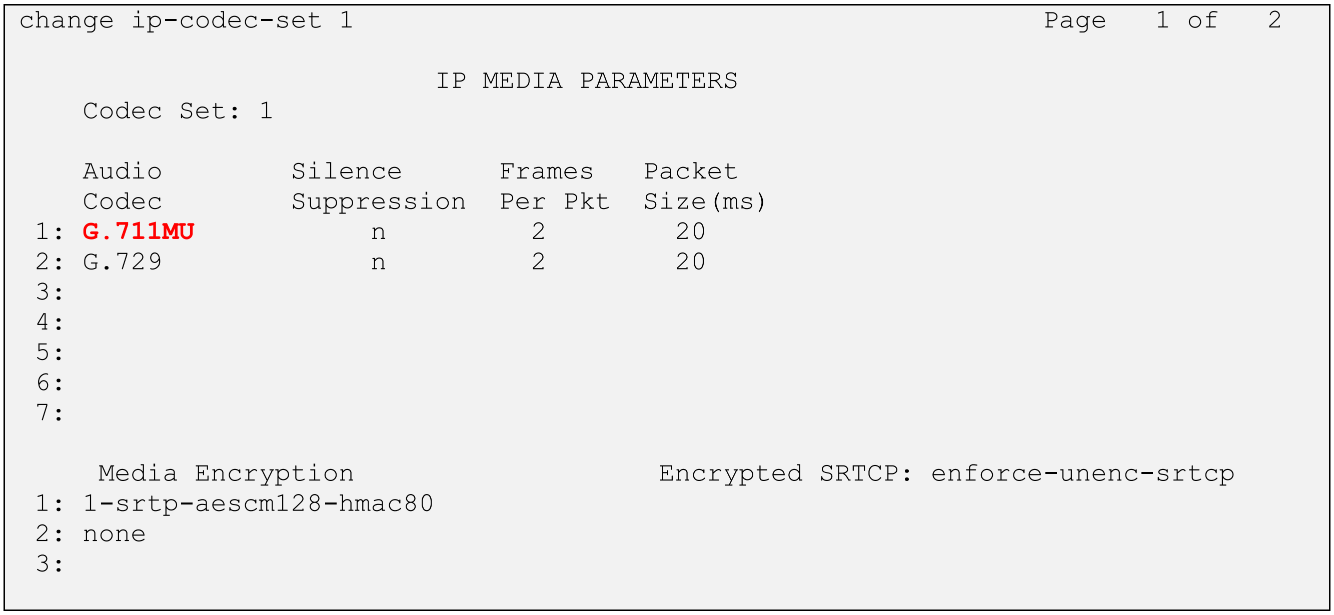
5.2. Administer IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager **(procr**) and for Session Manager (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section 5.5**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
AMS1                10.33.1.30
default             0.0.0.0
interopASM          10.33.1.12
procr               10.33.1.6
```

5.3. Administer Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the local and remote sites. For the compliance test, codec G.711MU and G.729A was configured using ip-codec-set 1. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.



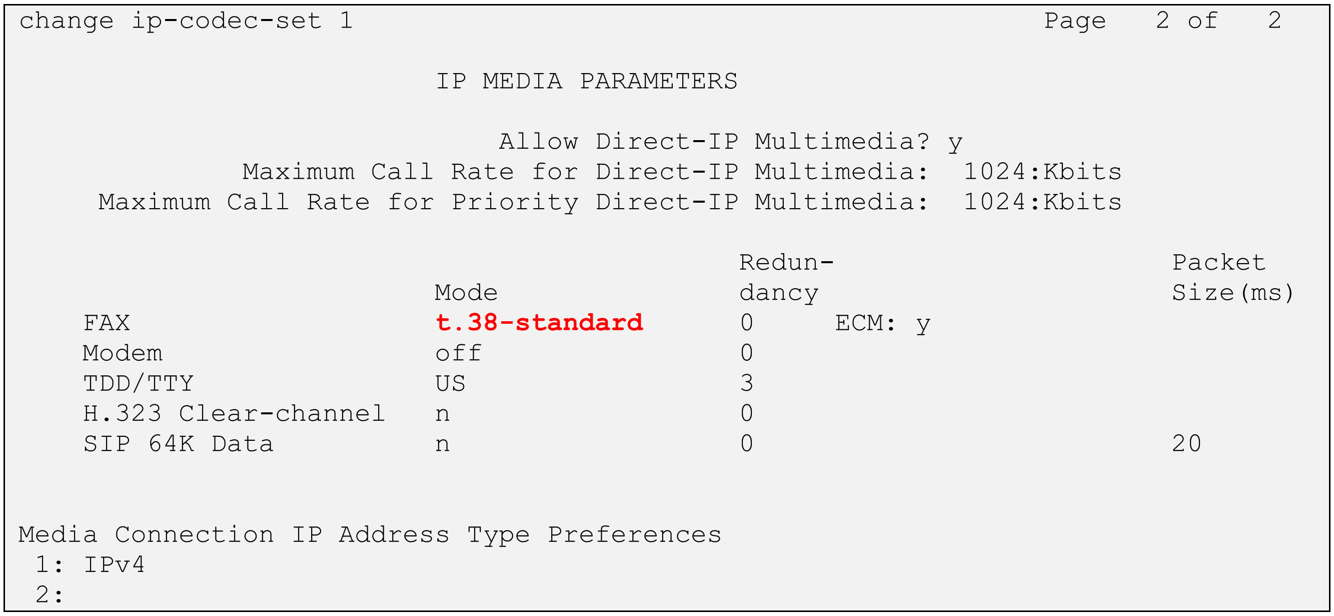
```
change ip-codec-set 1                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729            n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
```

On **Page 2**, set the **FAX** mode to “t.38-standard”. Retain default values for all other fields.



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

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  1024:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  1024:Kbits

                                             Redun-                      Packet
                          Mode               dancy                       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


Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

5.4. Administer IP Network Region

For the compliance test, IP network region 1 was chosen. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the local site. In this configuration, the domain name is **bvwdev.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field. This is optional.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.3**.
- Retain default values for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: bvwdev.com
    Name: Loc-1                   Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

On **Page 4**, define the IP codec set to be used for traffic between various regions. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. In the case of the compliance test, only one IP network region was used, so no inter-region settings were required and therefore only codec set 1 is used.

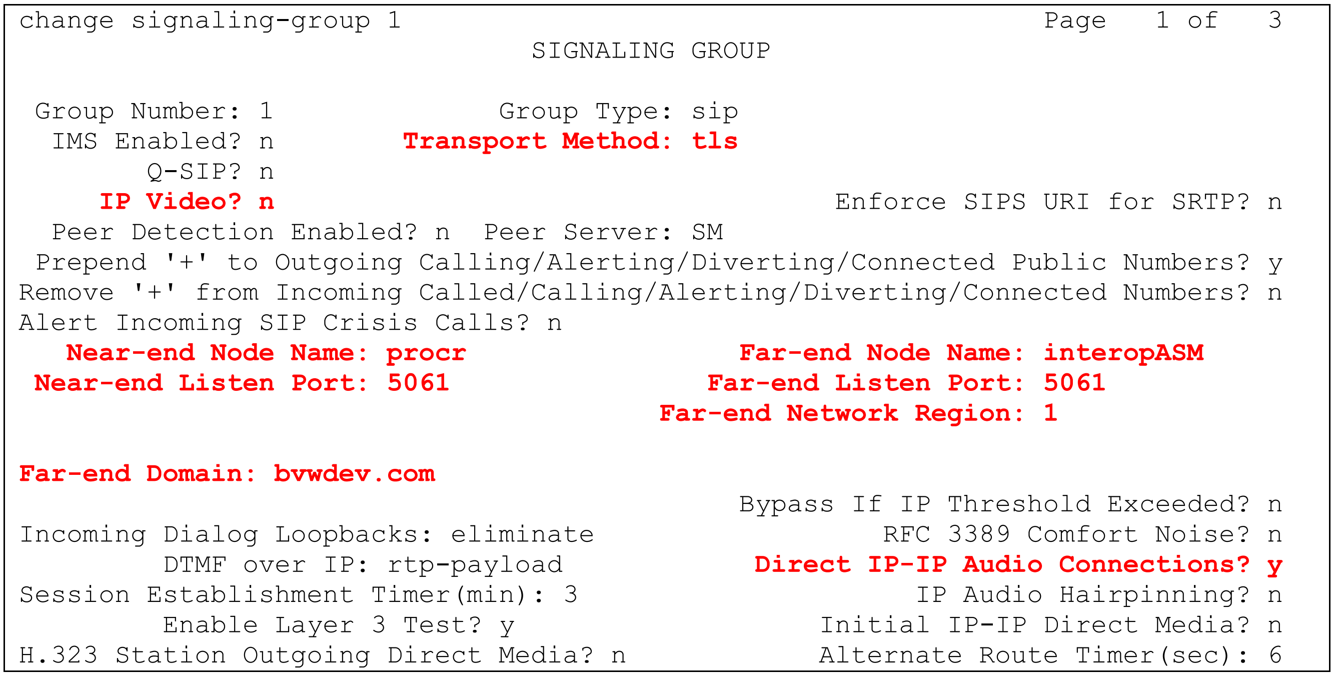
```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                                 all
 2    2     y    NoLimit                      n    t
```

5.5. Administer Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by SIP trunks. This signaling group is used for inbound and outbound calls between the Communication Manager and Session Manager. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- The compliance test was conducted with the **Transport Method** set to "tls". The transport method specified here is used between Communication Manager and Session Manager. Whatever protocol is used here, it must also be used on the Session Manager entity link defined in **Section 6.5**. Compliance testing was also conducted with **Transport Method** set to "tcp" and "udp." .(Note: for TCP and UDP operation, refer to an earlier Application Note: https://www.devconnectprogram.com/fileMedia/download/b2a7ac70-0eab-4a9f-aff0-b706ec465be3)
- Set the **IP Video** to "n" – Note that the IP Video should be set to "n" to disable the video call capability for incoming fax call from Communication Manager to XM FAX to work.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to "procr". This node name maps to the IP address of the Communication Manager as defined in **Section 5.2**.
- Set the **Far-end Node Name** to "InteropASM". This node name maps to the IP address of Session Manager as defined in **Section 5.2**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a default well-known port value. (For TCP the well-known port value is 5060).
- Set the **Far-end Network Region** to the IP network region defined for the local site in **Section 5.4**.
- Set the **Far-end Domain** to the domain of the local site.
- Set **Direct IP-IP Audio Connections** to "**y**". This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to "rtp-payload". This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Retain default values for all other fields.



```
change 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? n
  Peer Detection Enabled? n  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: interopASM
 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? n
         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. Administer Trunk Group

Use the “add trunk-group” command to create a trunk group for the signaling group created in **Section 5.5**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to “sip”.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to “tie”.
- Set **Member Assignment Method** to “auto”.
- Set the **Signaling Group** to the signaling group shown in **Section 5.5**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Retain default values for all other fields.

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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: Private Trunk               COR: 1        TN: 1         TAC: #01
   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: 14
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. The **Numbering Format** was set to “private” and the **Numbering Format** in the route pattern was set to “lev0-pvt” (see **Section 5.8**).

```
add 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? y
                                                Replace Unavailable Numbers? y

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

5.7. Administer Private Numbering

Private numbering defines the calling party number to be sent to the far-end. Use the **change private-numbering** command to create an entry that will be used by the trunk groups defined in **Section 5.6.** In the example shown below, all calls originating from a 4-digit extension beginning with "3" and routed across trunk group 1 are sent with a 4-digit calling number.

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

Ext Ext               Trk         Private           Total
Len Code              Grp(s)      Prefix            Len
 4  3                 1                             4    Total Administered: 5
 4                                                          Maximum Entries: 540
```

5.8. Administer Outbound Routing

In these Application Notes, the Automatic Alternate Routing (AAR) feature is used to route outbound calls via the SIP trunk to the XM Fax server. In the sample configuration, the dial prefix "52" is used as the Dialed String. Local site users will dial "52xx" to reach the XM Fax server. This common configuration is illustrated below with little elaboration. Use the "change dialplan analysis" command to define a dialed string beginning with 52 of length 4 as uniform dialing plan (UDP).

```
change dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 5

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   52             4   udp
```

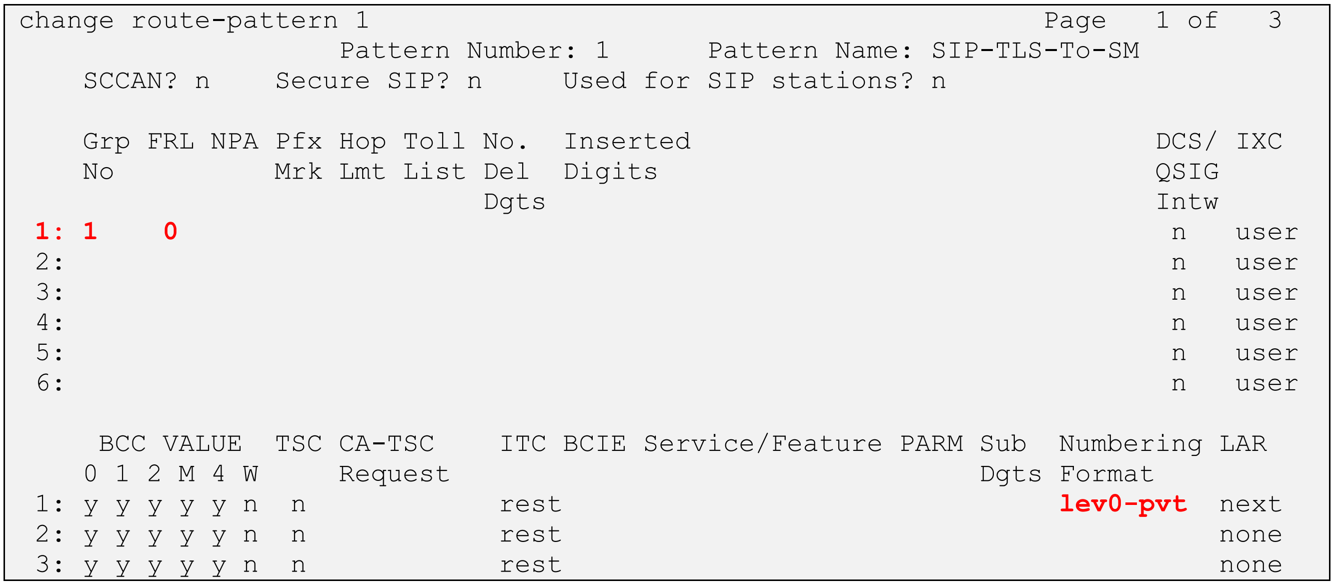
Use the "change uniform-dialplan" command to create a matching pattern that matches with the dial pattern used to reach the XM Fax server. The example below shows entries created for local site. Extension 51xx was used and configured as shown below where "52" is the Matching Pattern with a Length of 4, no digits to be deleted and using the aar feature.

```
change uniform-dialplan 0                                         Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                Percent Full: 0

  Matching                    Insert                Node
  Pattern            Len Del      Digits     Net  Conv Num
 52                   4   0                  aar   n
```

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the “change route-pattern” command to configure the parameters for the local site route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP trunk. For the compliance test, trunk group **1** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: “lev0-pvt”. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in **Section 5.6** for full details.
- Retain default values for all other fields.

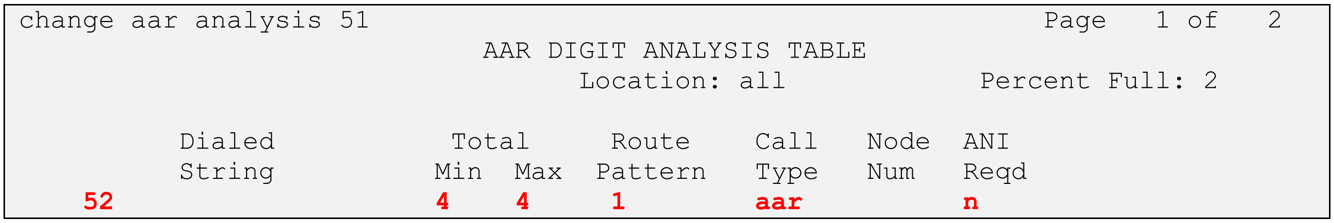


```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
    SCCAN? n     Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                  QSIG
                             Dgts                                         Intw
 1: 1    0                                                                 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                               lev0-pvt  next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
```

Use the “change aar analysis” command to create an entry in the AAR Digit Analysis Table for this purpose. The example below shows entries created for the local site “aar analysis 52”. The highlighted entry specifies that 4 digit dial string 52 was to use route pattern 1 to route calls to the XM Fax server at the local site via Session Manager.



```
change aar analysis 51                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all              Percent Full: 2

          Dialed           Total      Route    Call   Node  ANI
          String         Min  Max   Pattern    Type   Num   Reqd
    52                   4    4      1         aar          n
```

6. Configure Avaya Aura® Session Manager

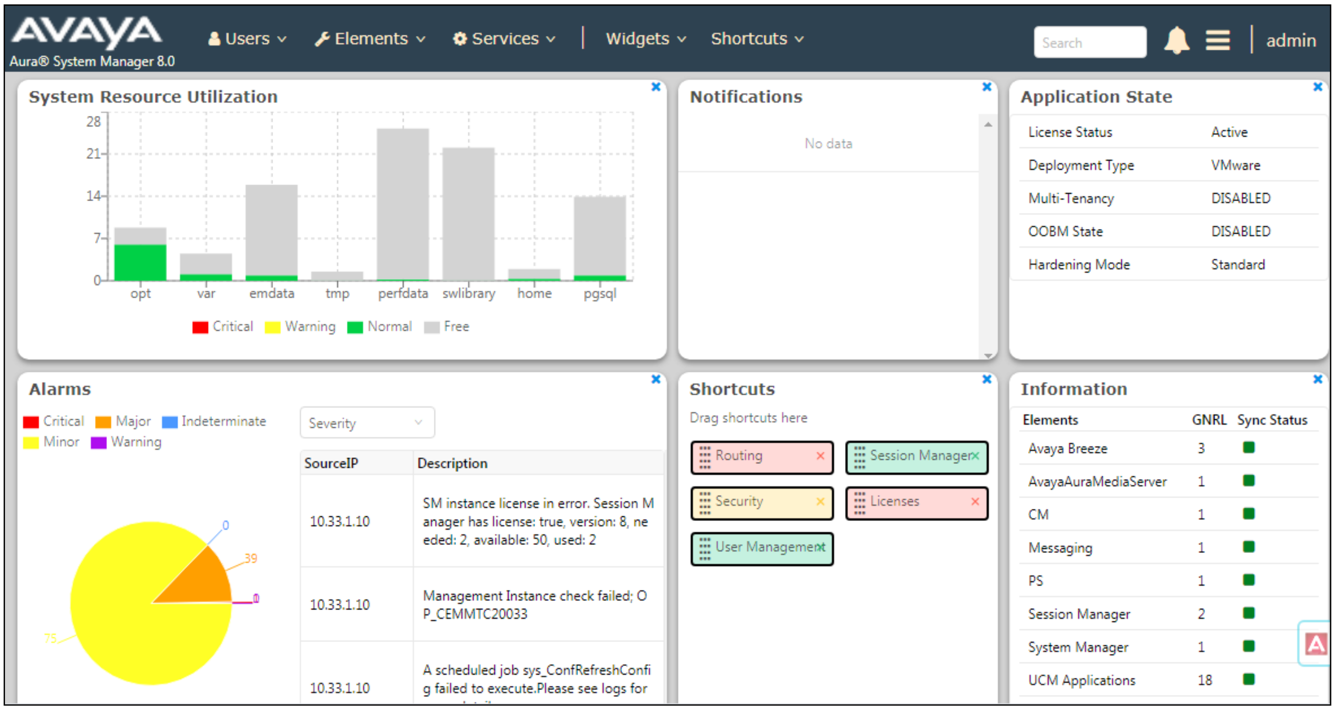
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Location
- Adaptation
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns

For detail configuration details of the Session Manager refer to **Section 10**.

6.1. Logging into the Avaya Aura® System Manager

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Log on** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Application State

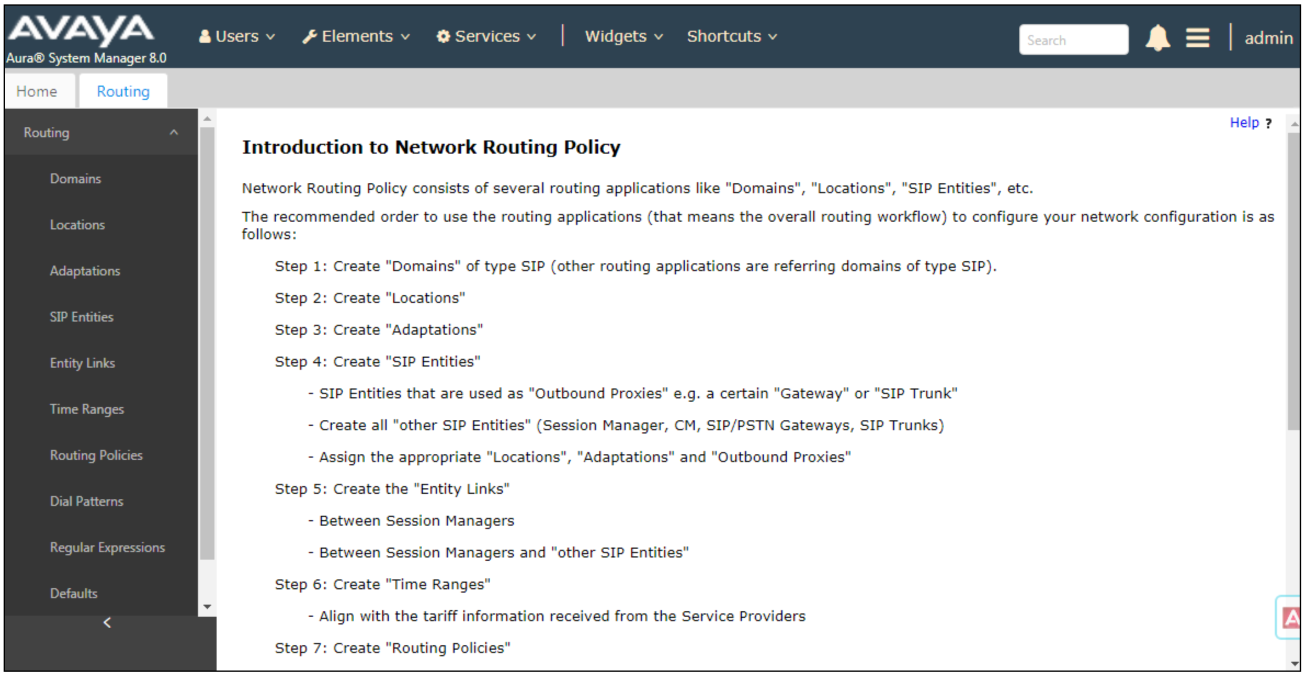
License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

SourceIP	Description
10.33.1.10	SM instance license in error. Session Manager has license: true, version: 8, needed: 2, available: 50, used: 2
10.33.1.10	Management Instance check failed; OP_CEMMTC20033
10.33.1.10	A scheduled job sys_ConfRefreshConfig failed to execute.Please see logs for

Information

Elements	GNRL	Sync Status
Avaya Breeze	3	🟩
AvayaAuraMediaServer	1	🟩
CM	1	🟩
Messaging	1	🟩
PS	1	🟩
Session Manager	2	🟩
System Manager	1	🟩
UCM Applications	18	🟩

Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

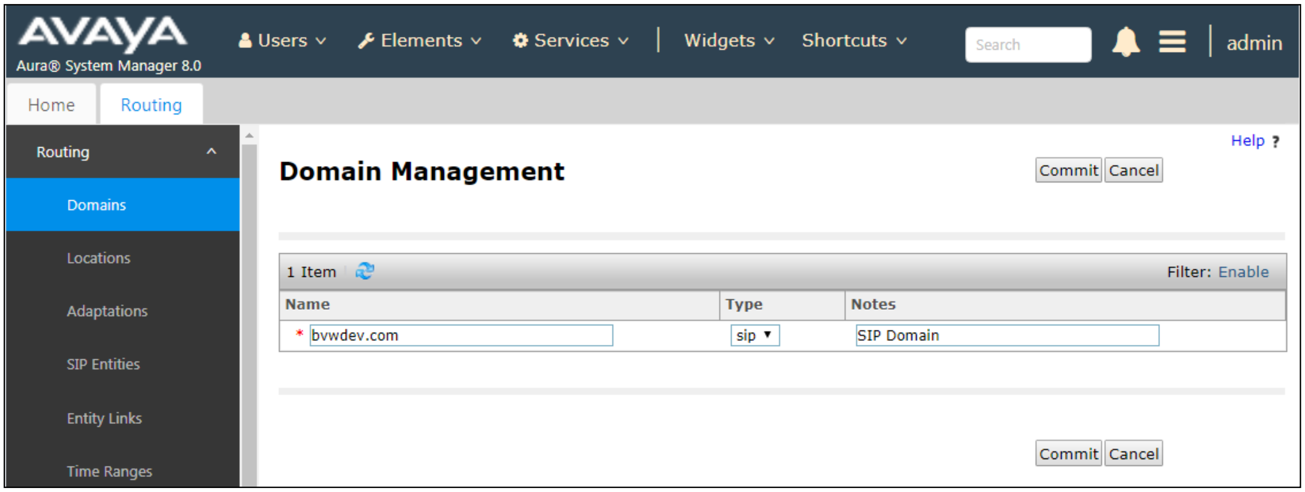
Step 7: Create "Routing Policies"

6.2. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the domain (**bvwdev.com**) as defined in **Section 5.4**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select "sip" from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the added domain.



Domain Management

1 Item

Name	Type	Notes
* bvwdev.com	sip	SIP Domain

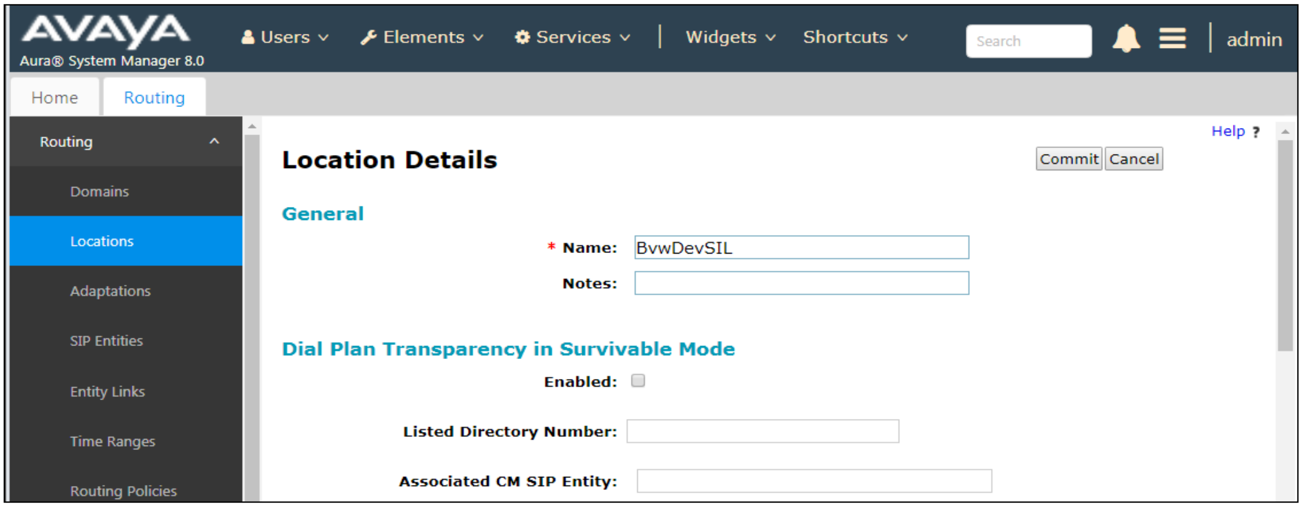
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **BvwDevSIL**, which includes all equipment at the enterprise including Communication Manager, Session Manager and the XM Fax server.

To add a Location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name for the Location.
- **Notes:** Add a brief description (optional).



Location Details

General

* Name: BvwDevSIL

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: □

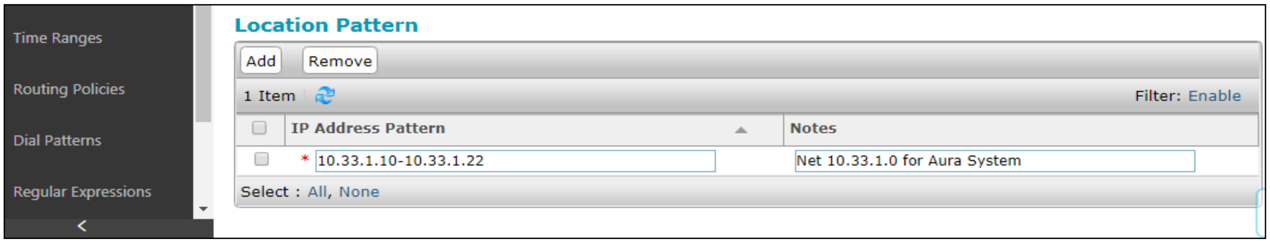
Listed Directory Number:

Associated CM SIP Entity:

Scroll down to the **Location Pattern** section. Click **Add** and enter the following values.

- **IP Address Pattern:** Add all IP address patterns used to identify the location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



Location Pattern

1 Item   Filter: Enable

	IP Address Pattern	Notes
□	* 10.33.1.10-10.33.1.22	Net 10.33.1.0 for Aura System

Select : All, None

6.4. Add Adaptation

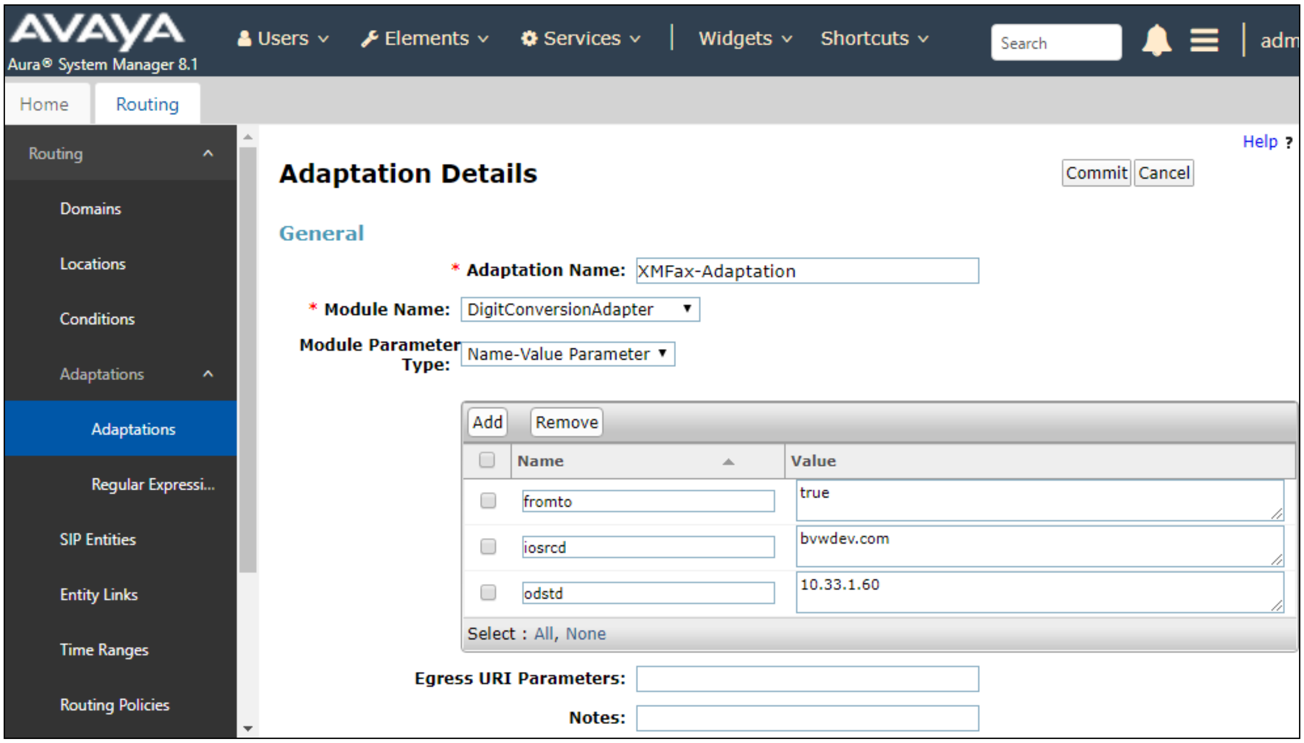
Session Manager can be configured with adaptations that can modify SIP messages before or after routing decisions have been made or perform digit manipulation. The Adaptation **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. For the compliance test, an Adaptation was used.

To create the adaptation that will be applied to the XM Fax SIP Entity, click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., **XMFax-Adaptation)**.
- **Module Name:** Select **DigitConversionAdapter** from the drop-down menu.
- **Module Parameter Type:** Enter **Name-Value Parameter**. This section will expand with an area to enter **Name** and **Value** pairs. Click **Add**, to add there parameters: **fromto** = true, **iosrcd** = bvwdev.com, **odstd** = 10.33.1.60.

This adaptation will change the host part of Request and To header for the incoming fax call to XM Fax from the SIP domain “bvwdev.com” to the IP address of the XM Fax server “10.33.1.60”. Without the change, XM Fax rejects the call with 404 Not found since it does not recognize the sip domain.



Adaptation Details

General

* Adaptation Name: XMFax-Adaptation

* Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

	Name	Value
□	fromto	true
□	iosrcd	bvwdev.com
□	odstd	10.33.1.60

Egress URI Parameters:

Notes:

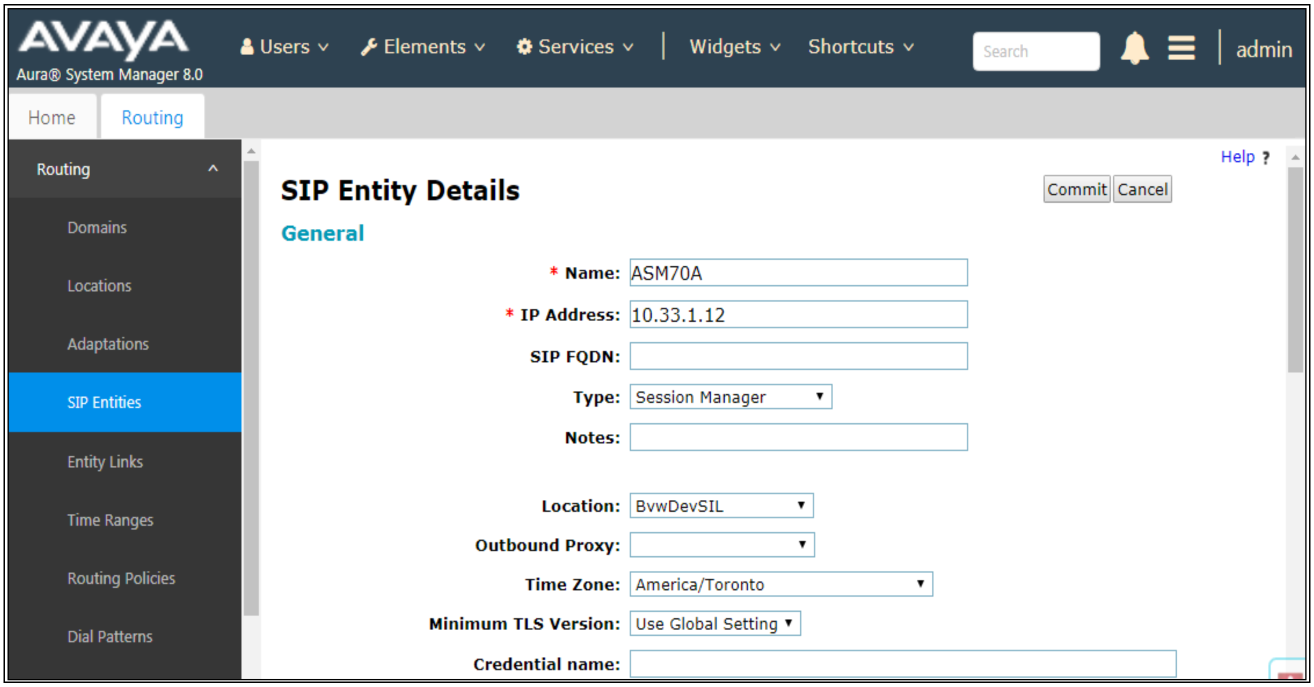
6.5. Add SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the XM FAX PC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the XM Fax server.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name**. During compliance testing no adaptation rule was used.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **BvwDevSIL** created in **Section 6.3**.
- **Time Zone:** Select the time zone where the server is located.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



SIP Entity Details

General

* Name:	ASM70A
* IP Address:	10.33.1.12
SIP FQDN:	
Type:	Session Manager
Notes:	
Location:	BvwDevSIL
Outbound Proxy:	
Time Zone:	America/Toronto
Minimum TLS Version:	Use Global Setting
Credential name:	

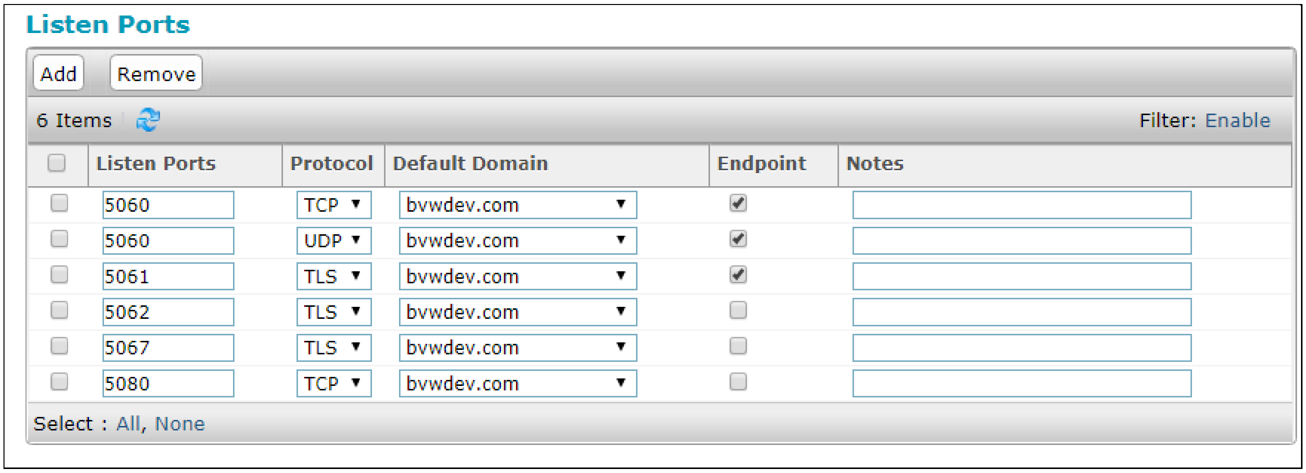
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the SIP domain.

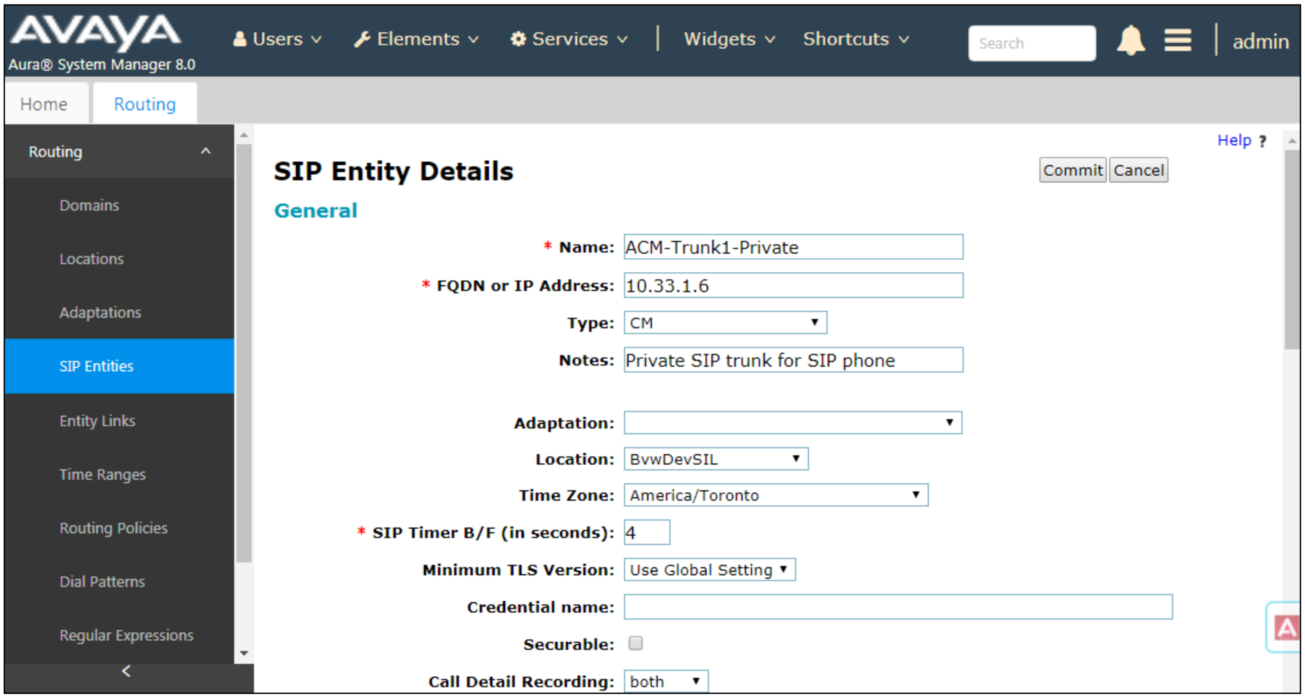
Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, three entries were used. They are the standard ports used for SIP traffic: port 5061 for TLS, port 5060 for UPD and TCP. These ports were provisioned as part of the Session Manager installation and not covered by this document.



☐	Listen Ports	Protocol	Default Domain	Endpoint	Notes
☐	5060	TCP	bvwdev.com	☑	
☐	5060	UDP	bvwdev.com	☑	
☐	5061	TLS	bvwdev.com	☑	
☐	5062	TLS	bvwdev.com	☐	
☐	5067	TLS	bvwdev.com	☐	
☐	5080	TCP	bvwdev.com	☐	

The following screen shows the addition of SIP entity Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager; this requires the creation of a SIP Entity for Communication Manager for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. The **Location** field is set to **BvwDevSIL** which is the Location defined for the subnet where Communication Manager resides. See **Section 6.3**.

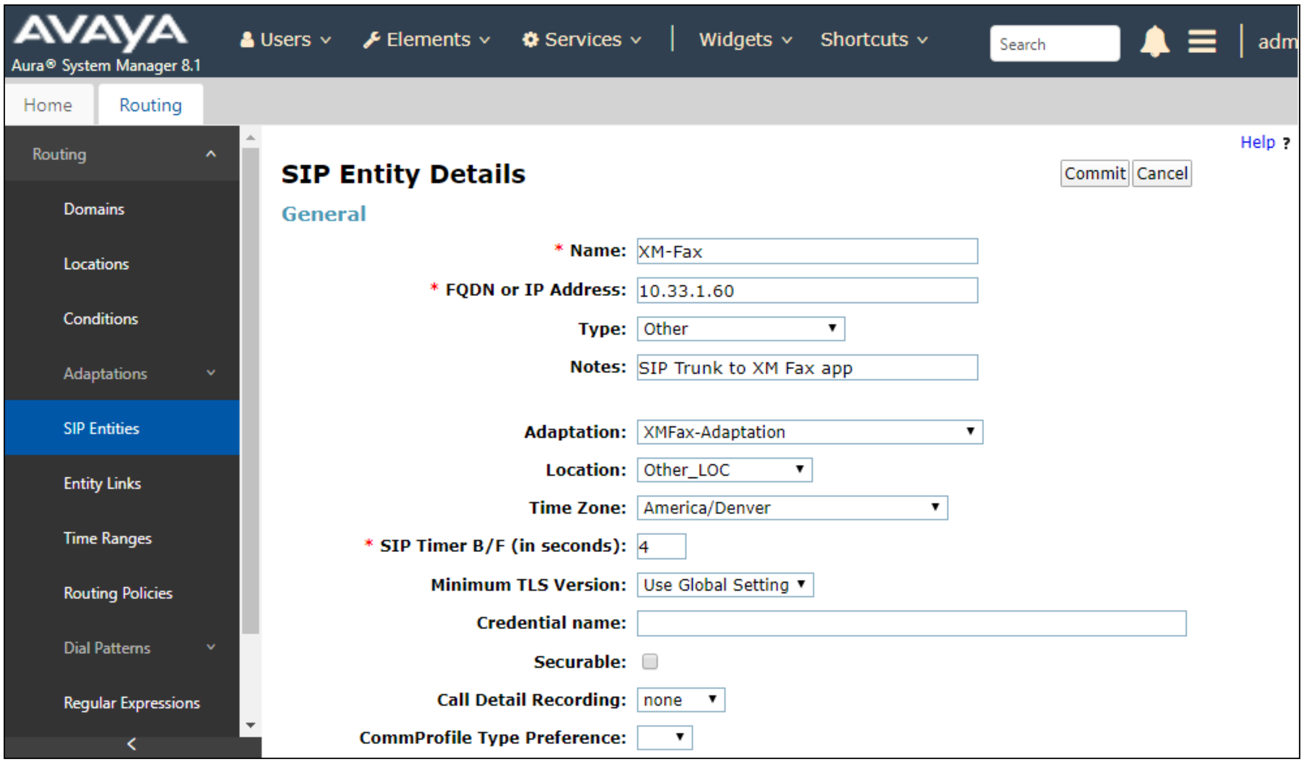


SIP Entity Details

General

* Name:	ACM-Trunk1-Private
* FQDN or IP Address:	10.33.1.6
Type:	CM
Notes:	Private SIP trunk for SIP phone
Adaptation:	
Location:	BvwDevSIL
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	both

The following screen shows the SIP entity of the XM Fax software that is installed on a Windows based client. The **FQDN or IP Address** field is set to the IP address of the client. The **Adaptation** field is set to the adaptation created in **Section 6.4**.



SIP Entity Details

General

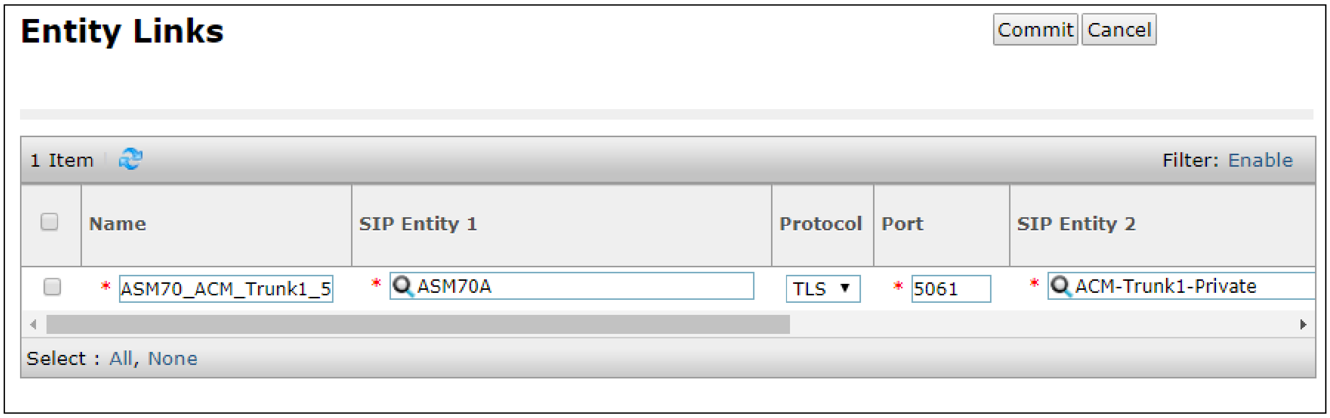
* Name:	XM-Fax
* FQDN or IP Address:	10.33.1.60
Type:	Other
Notes:	SIP Trunk to XM Fax app
Adaptation:	XMFax-Adaptation
Location:	Other_LOC
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	none
CommProfile Type Preference:	

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager and one to the XM Fax software client. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

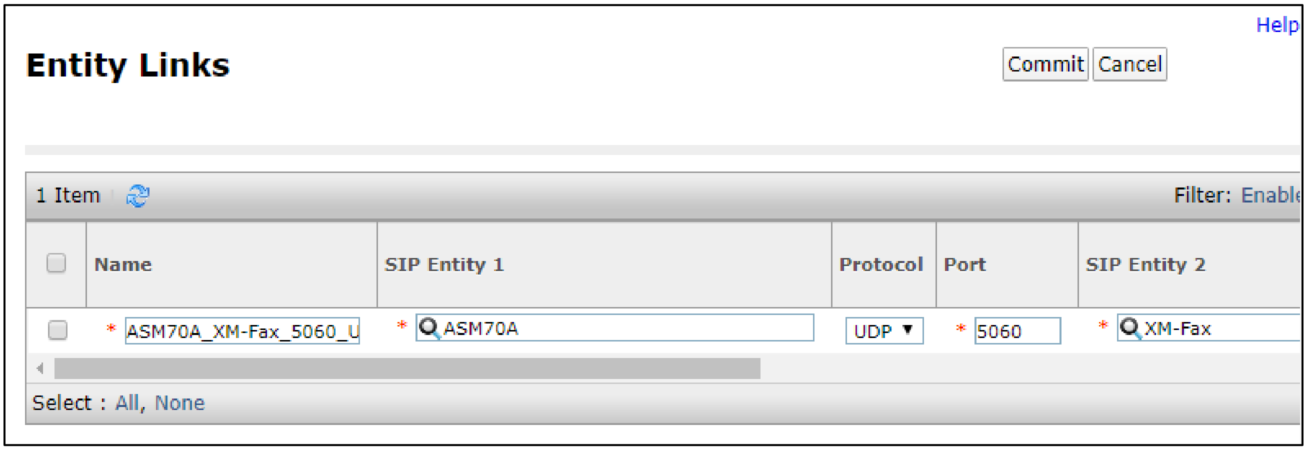
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.5**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in **Section 5.5**.
- **Connection Policy:** Select **trusted** from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group configuration in **Section 5.5**.



□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
□	* ASM70_ACM_Trunk1_5	* ASM70A	TLS	* 5061	* ACM-Trunk1-Private

The following screen illustrates the Entity Link to the XM Fax software client.



Entity Links

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2
□	* ASM70A_XM-Fax_5060_U	* ASM70A	UDP ▼	* 5060	* XM-Fax

6.7. Add Routing Policies

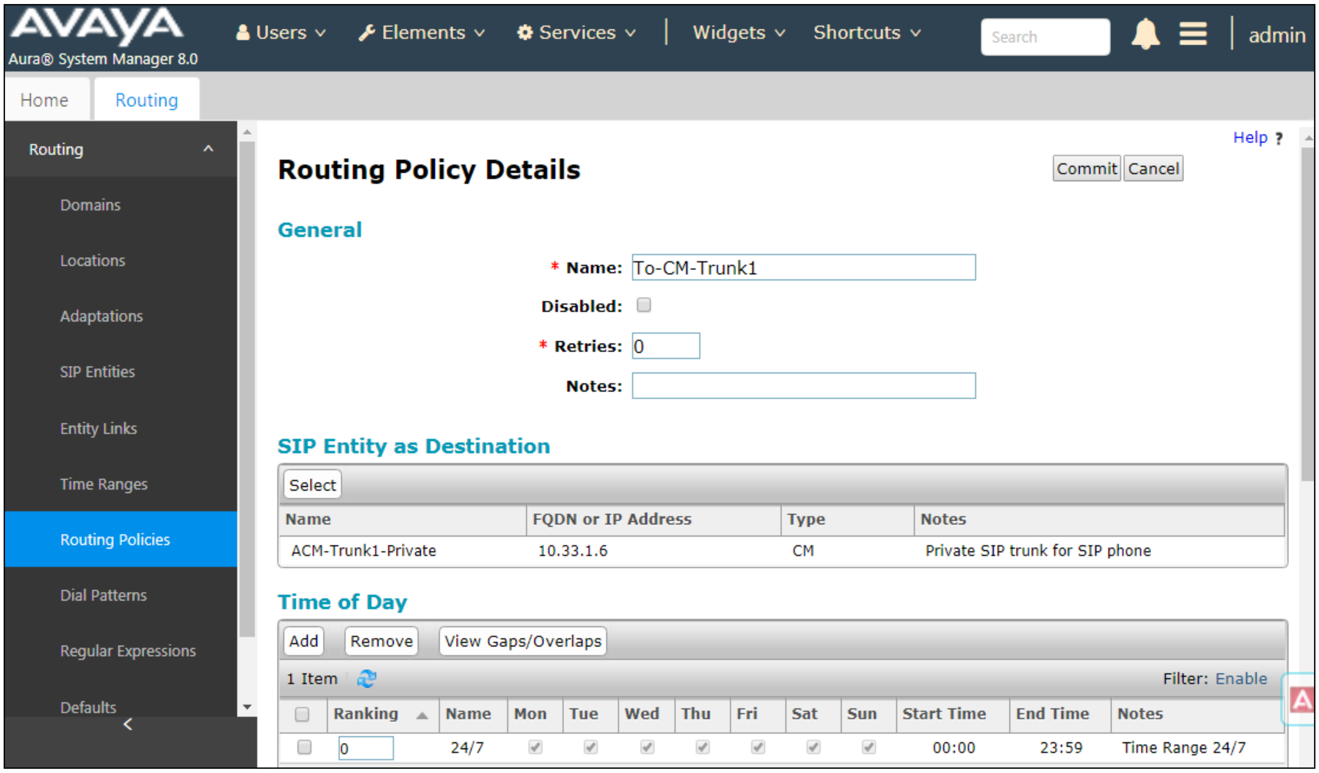
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and one for the XM Fax. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy for Communication Manager.



Routing Policy Details

General

* Name: To-CM-Trunk1

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

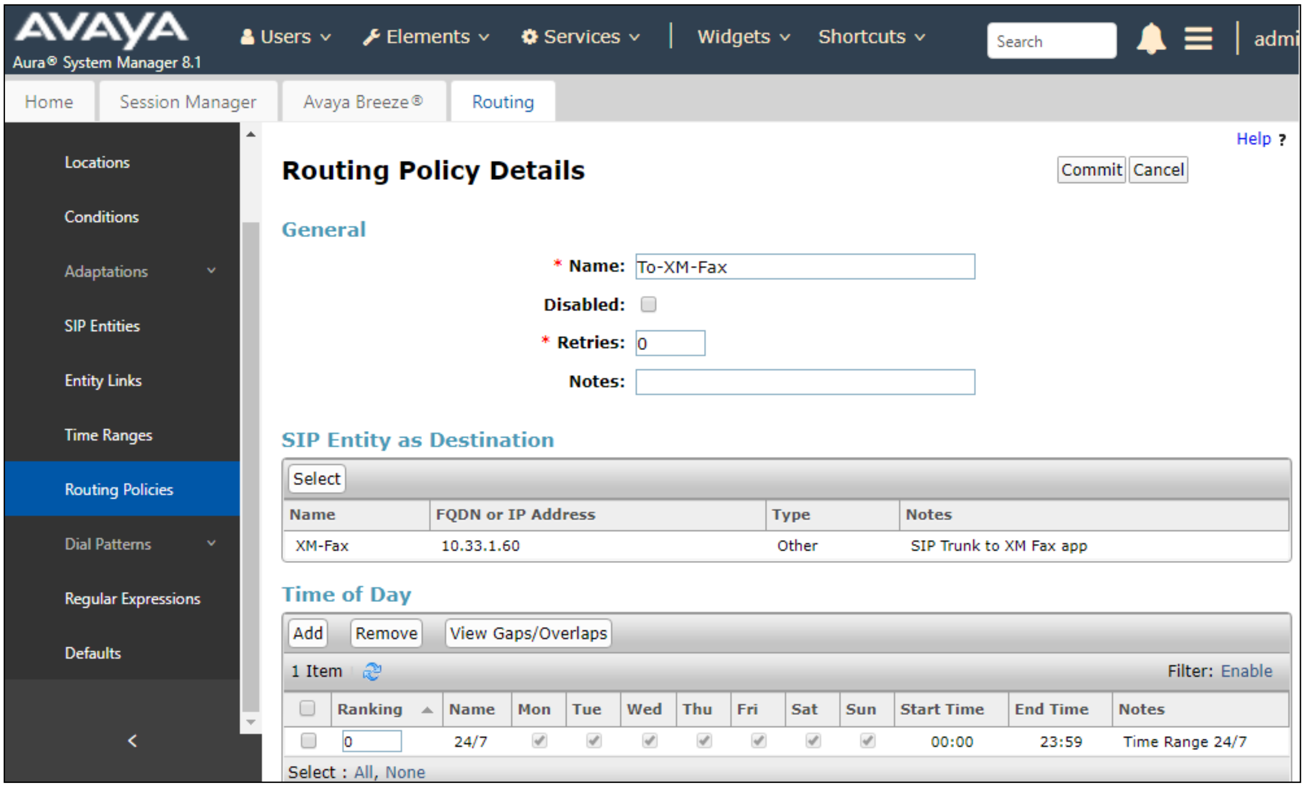
Name	FQDN or IP Address	Type	Notes
ACM-Trunk1-Private	10.33.1.6	CM	Private SIP trunk for SIP phone

Time of Day

1 Item

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

The following screen shows the Routing Policy for the XM Fax software client.



Routing Policy Details

General

* **Name:** To-XM-Fax

Disabled: ☐

* **Retries:** 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
XM-Fax	10.33.1.60	Other	SIP Trunk to XM Fax app

Time of Day

1 Item   Filter: Enable

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

Select : All, None

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to the XM Fax software client and vice versa. Dial Patterns define which Route Policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

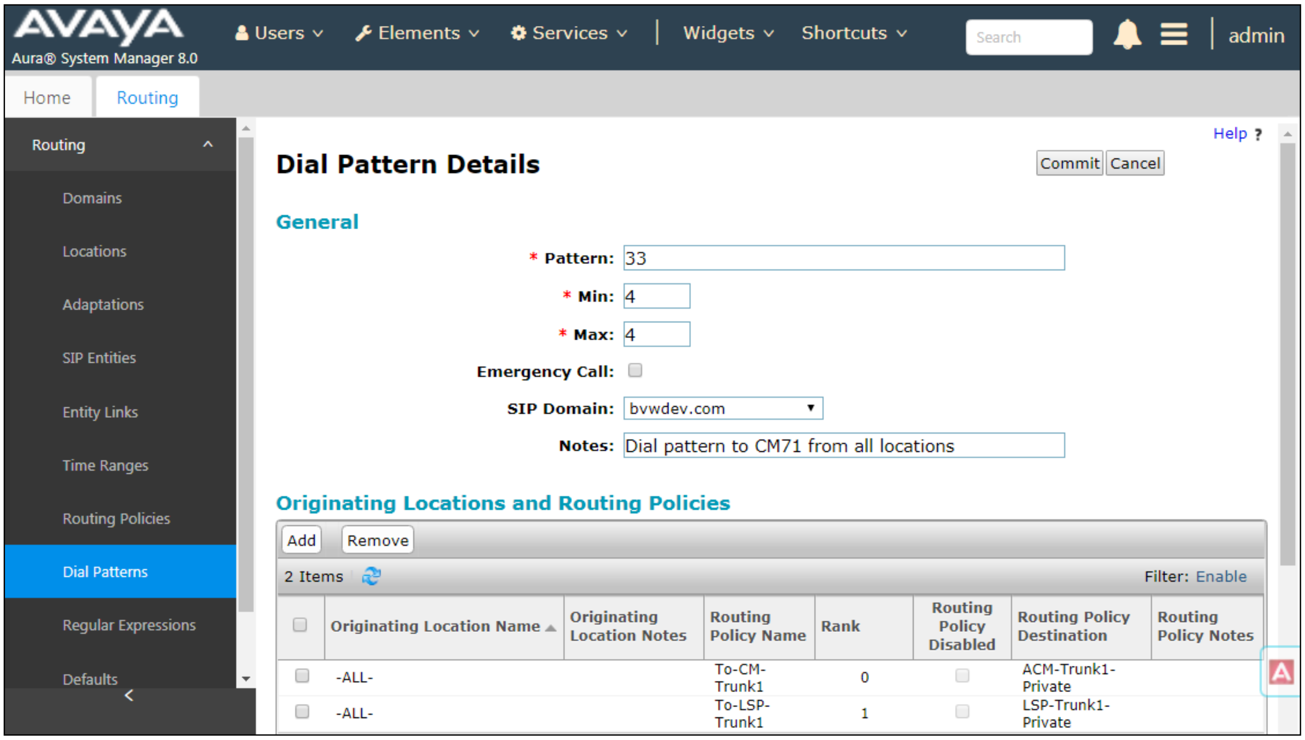
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

Two examples of the Dial Patterns used for the compliance test are shown below. The first example shows the pattern (4 digits) that begins with "33" and has a destination domain of "bvwdev.com" from "All" location use route policy "ACM-Trunk1-Private".



Dial Pattern Details

General

* Pattern: 33

* Min: 4

* Max: 4

Emergency Call: □

SIP Domain: bvwdev.com

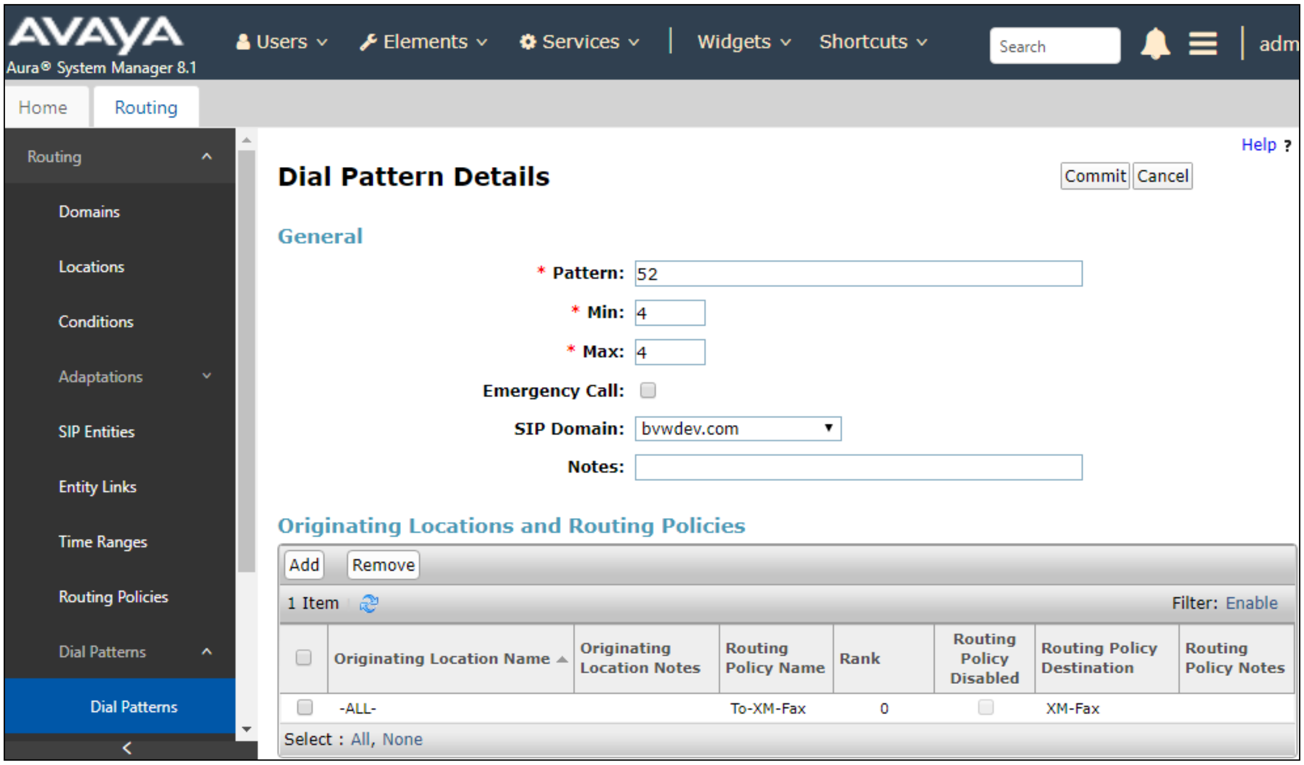
Notes: Dial pattern to CM71 from all locations

Originating Locations and Routing Policies

2 Items

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-CM-Trunk1	0	□	ACM-Trunk1-Private	
□	-ALL-		To-LSP-Trunk1	1	□	LSP-Trunk1-Private	

The second example shows the pattern (4 digits) that starts with a “52” using domain “bvwdev.com” and originating from “All” locations use route policy “To-XM-Fax”.



Dial Pattern Details

General

* Pattern:	52
* Min:	4
* Max:	4
Emergency Call:	□
SIP Domain:	bvwdev.com
Notes:	

Originating Locations and Routing Policies

1 Item

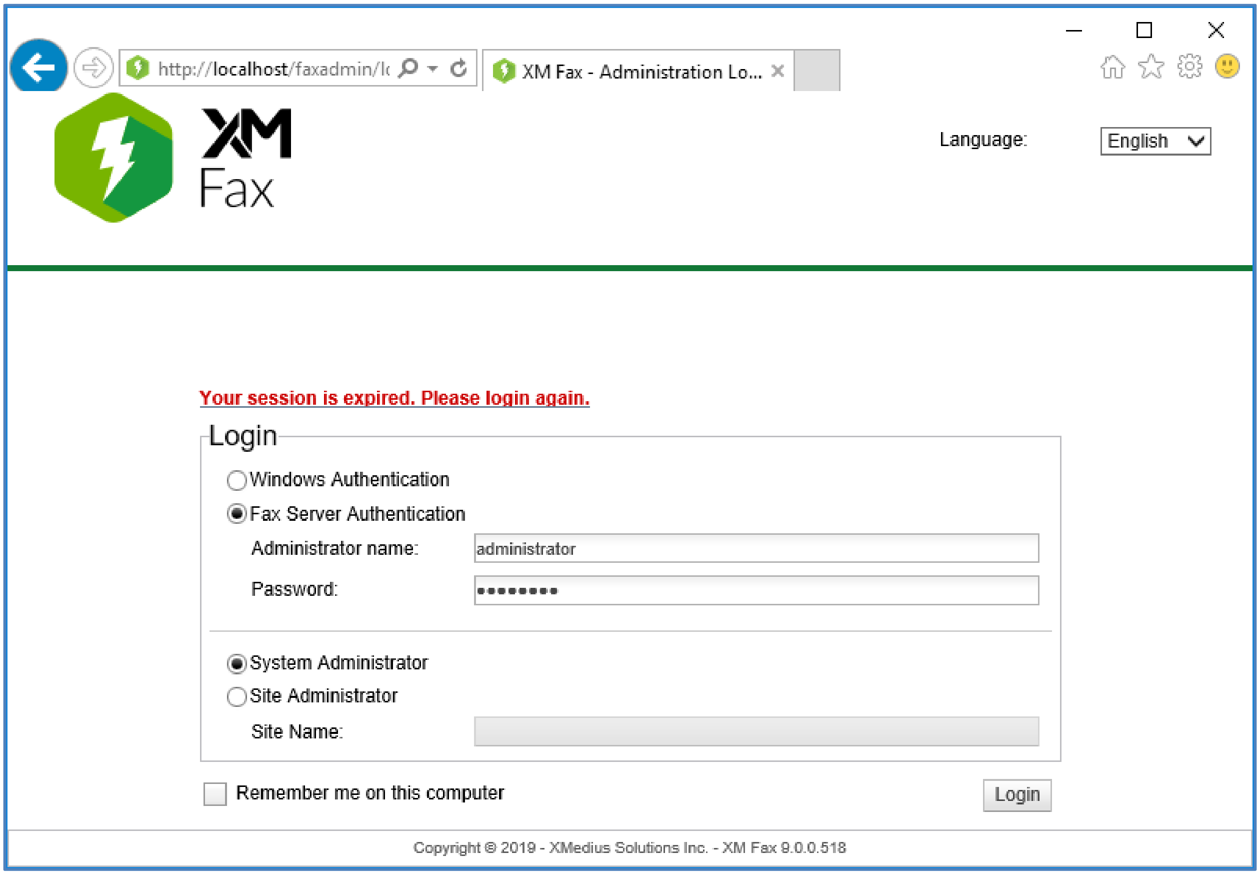
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		To-XM-Fax	0	□	XM-Fax	

Select : All, None

7. Configure XM Fax

This section describes the configuration of XM Fax software.

Launch the **XM Fax – Administration Login** webpage and enter a proper user name and password to login.



Your session is expired. Please login again.

Login

○ Windows Authentication
● Fax Server Authentication

Administrator name: administrator
Password: ●●●●●●●●●

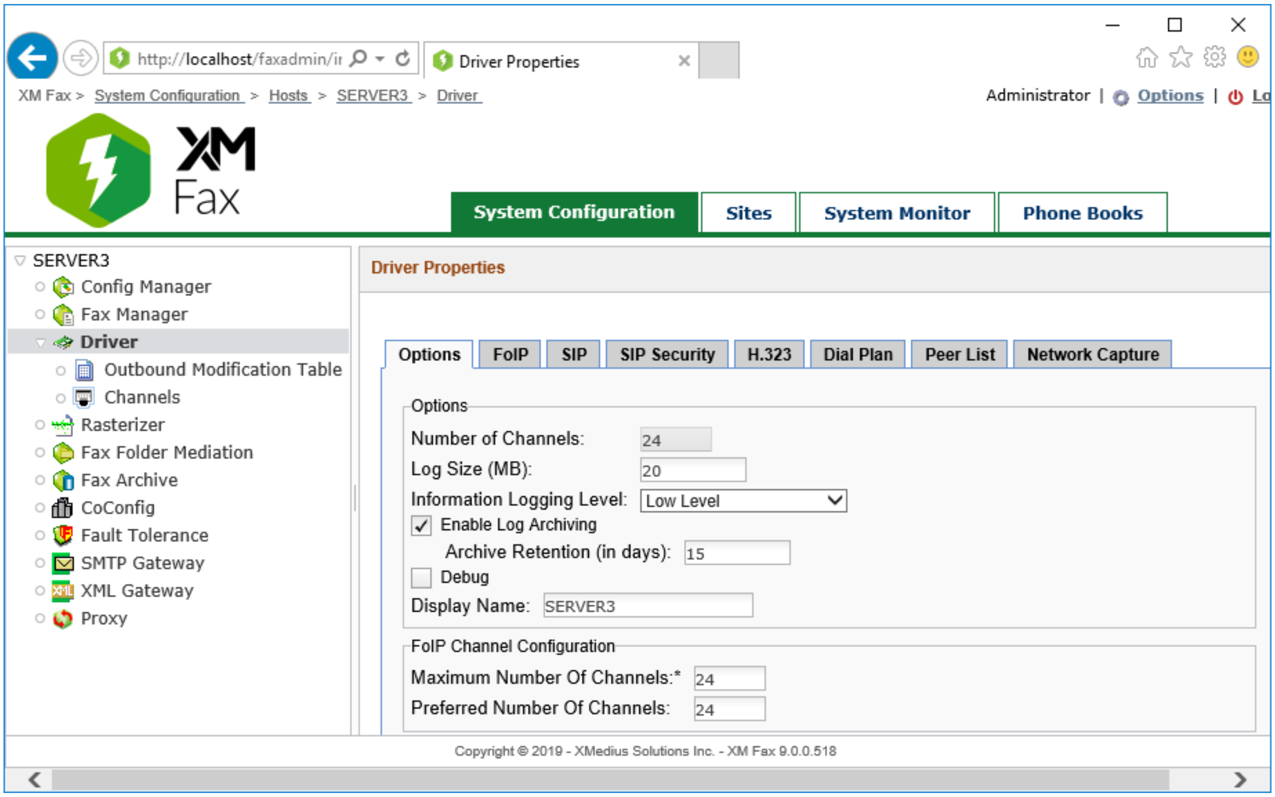
● System Administrator
○ Site Administrator

Site Name:

□ Remember me on this computer

Copyright © 2019 - XMedius Solutions Inc. - XM Fax 9.0.0.518

Select **Driver** icon from the left pane. The **Driver Properties** section displays in the right side of the window. In the **Options** tab, enter a number in the **Number of Channels** field supported by XM Fax.



Driver Properties

Options

Number of Channels: 24

Log Size (MB): 20

Information Logging Level: Low Level

☑ Enable Log Archiving

Archive Retention (in days): 15

□ Debug

Display Name: SERVER3

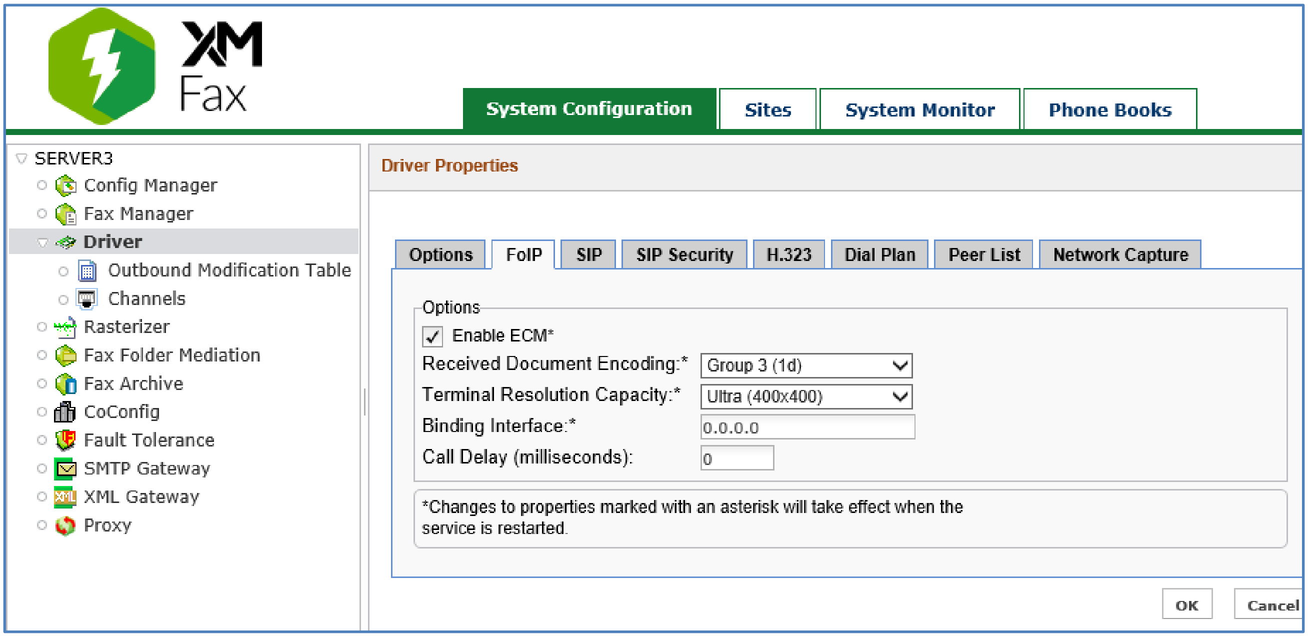
FoIP Channel Configuration

Maximum Number Of Channels:* 24

Preferred Number Of Channels: 24

Copyright © 2019 - XMedius Solutions Inc. - XM Fax 9.0.0.518

Select the **FoIP** tab, check the **Enable ECM** field and keep other fields at default values.



Driver Properties

Options

☑ Enable ECM*

Received Document Encoding:* Group 3 (1d)

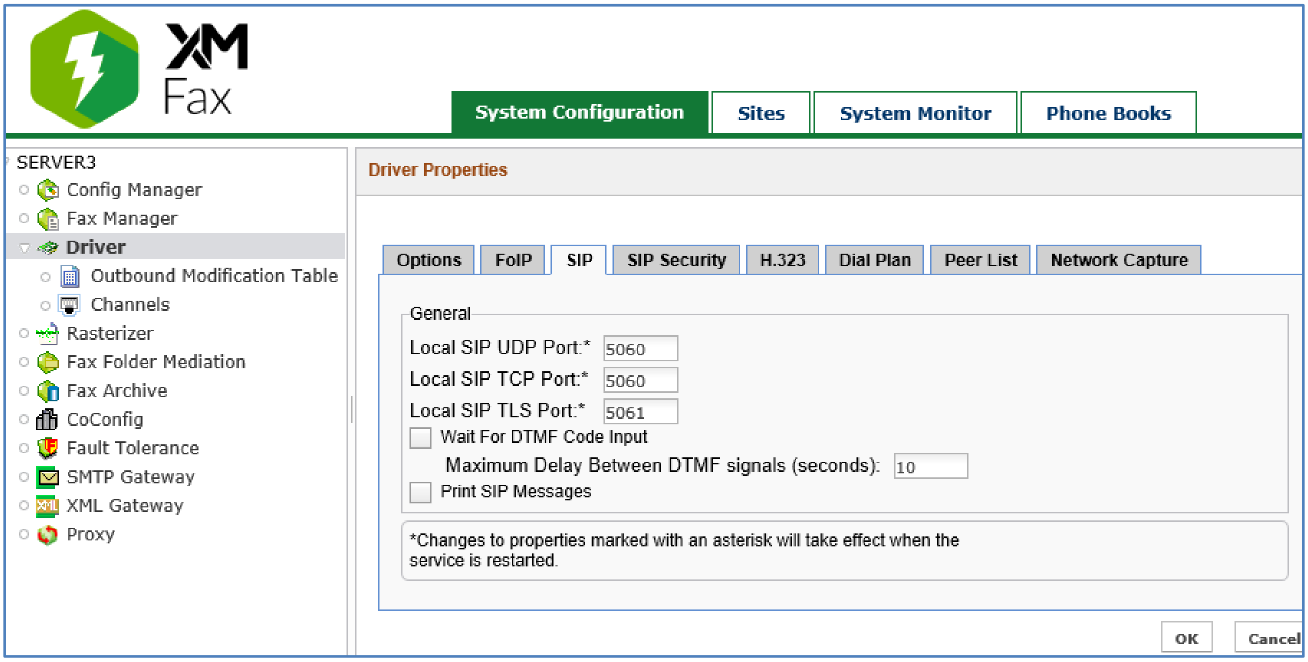
Terminal Resolution Capacity:* Ultra (400x400)

Binding Interface:* 0.0.0.0

Call Delay (milliseconds): 0

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

Leave all fields at default values in the **SIP** tab.



Driver Properties

General

Local SIP UDP Port:* 5060

Local SIP TCP Port:* 5060

Local SIP TLS Port:* 5061

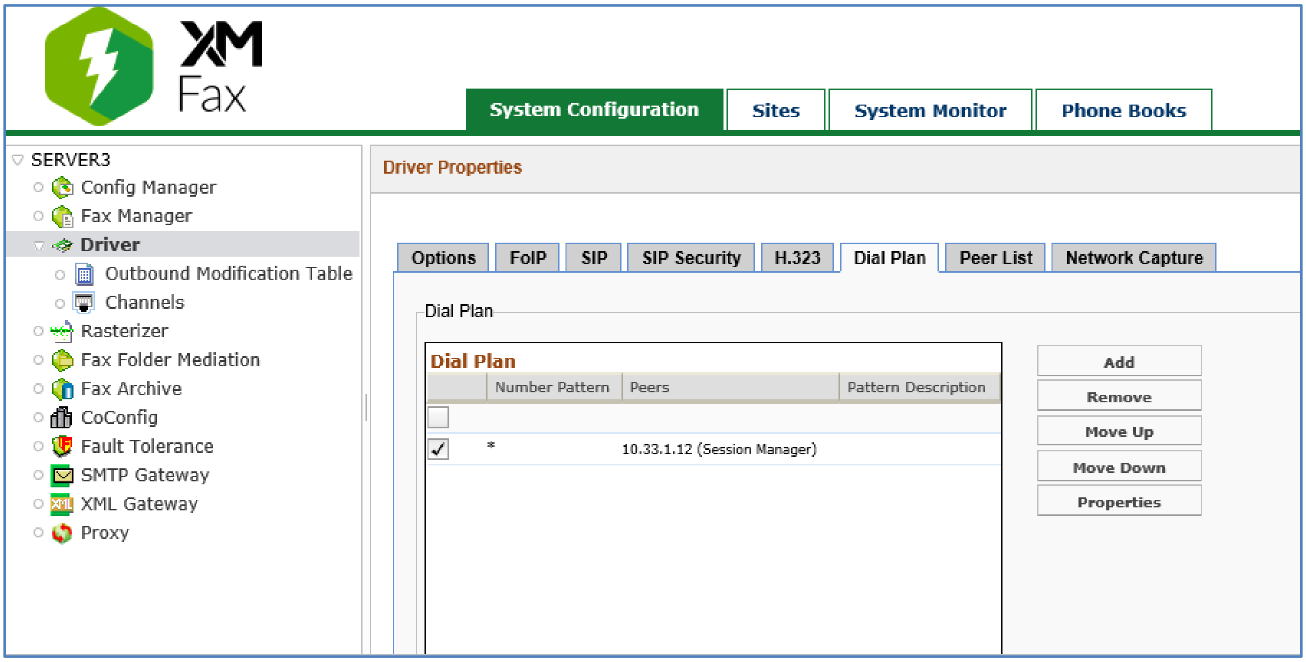
□ Wait For DTMF Code Input

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.

Select **Dial Plan** tab, click on **Add** button to add a pattern for outbound fax call. The dial pattern uses the start * for any dialed number that is sent through the peer with Session Manager.



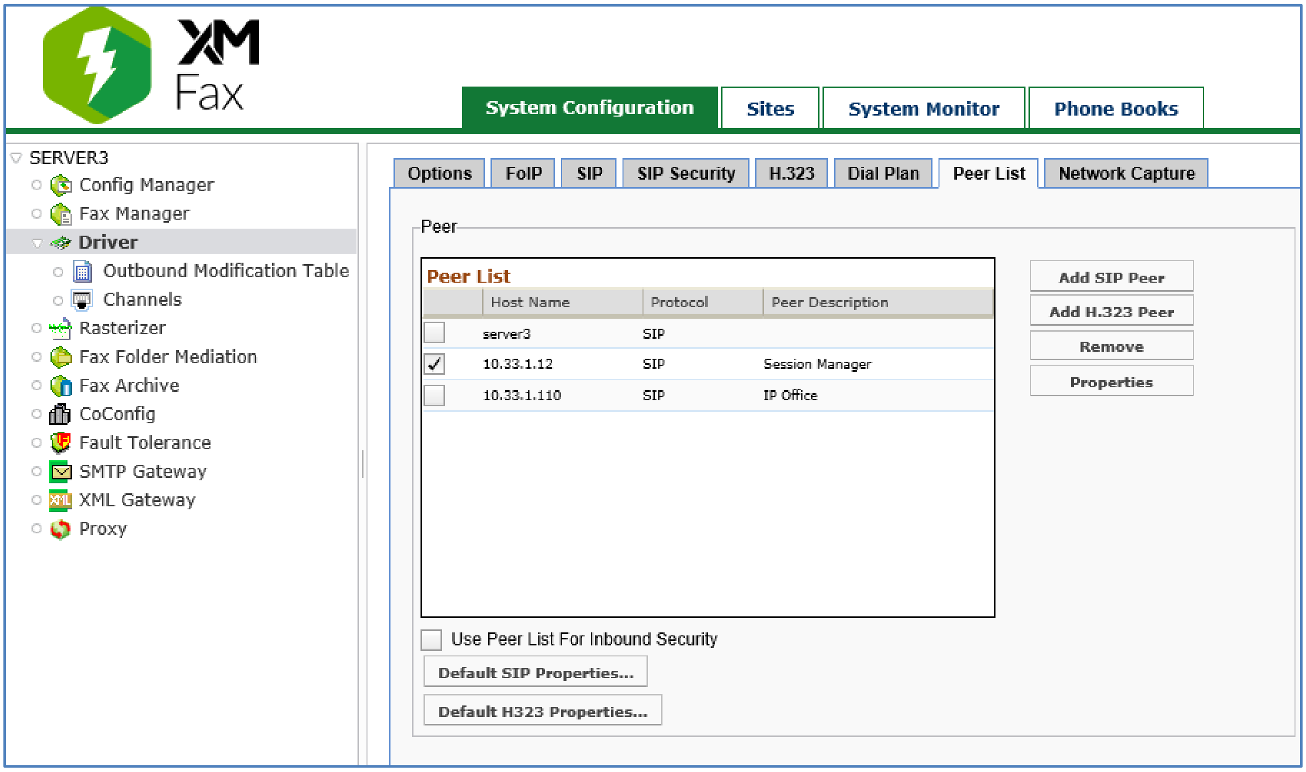
Driver Properties

Dial Plan

Dial Plan

	Number Pattern	Peers	Pattern Description
□			
☑	*	10.33.1.12 (Session Manager)	

Select the **Peer List** tab, click **Add SIP Peer** button to add a SIP Peer for Session Manager.



Peer List

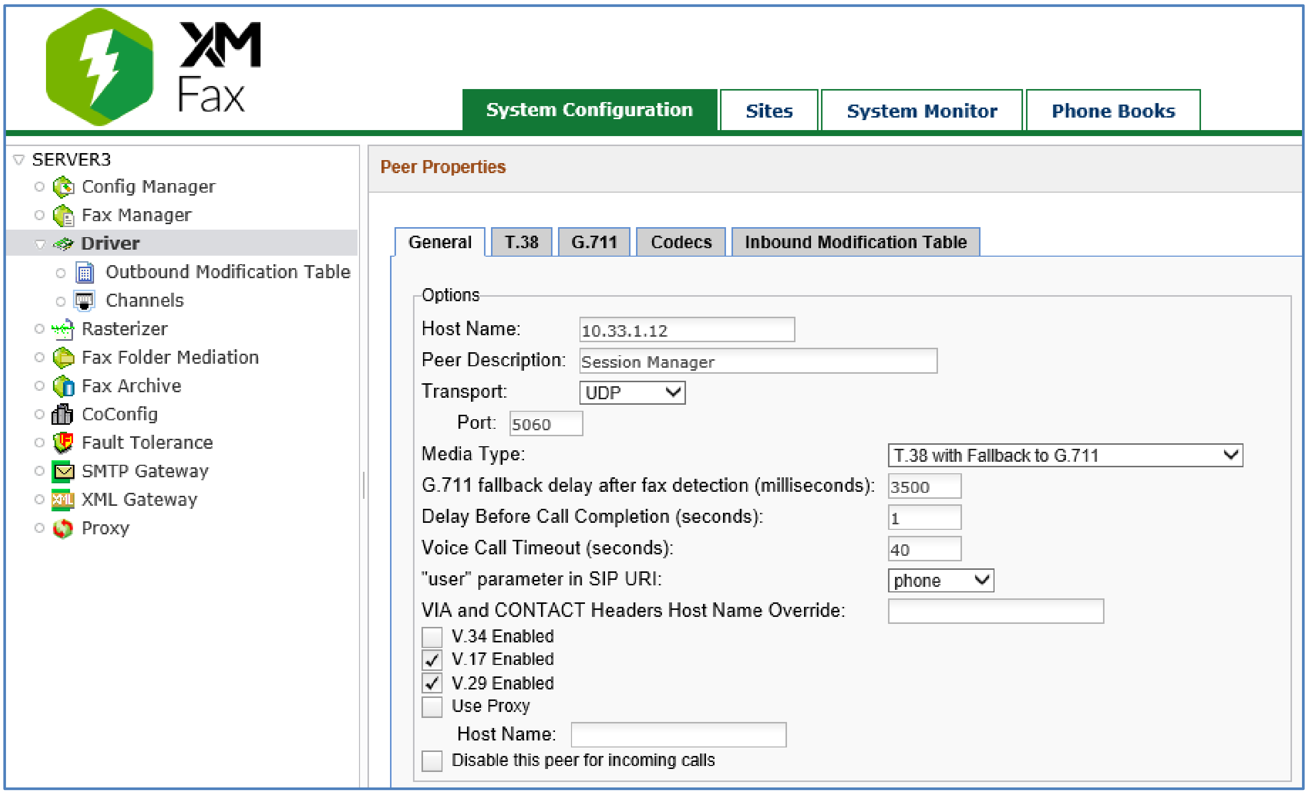
	Host Name	Protocol	Peer Description
□	server3	SIP	
☑	10.33.1.12	SIP	Session Manager
□	10.33.1.110	SIP	IP Office

□ Use Peer List For Inbound Security

The **Peer Properties** section displays in the right side of the window. In the **General** tab, enter the following parameters:

- **Host Name**: enter the SIP entity IP address of Session Manager ***10.33.1.12***
- **Peer Description**: enter a description
- **Transport**: select ***UDP*** port
- **Port**: enter the port ***5060***
- **Media Type**: select ***T.38 with Fallback to G.711***

And keep other fields at default values.



Peer Properties

Options

Host Name: 10.33.1.12

Peer Description: Session Manager

Transport: UDP

Port: 5060

Media Type: T.38 with Fallback to G.711

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

☑ V.17 Enabled

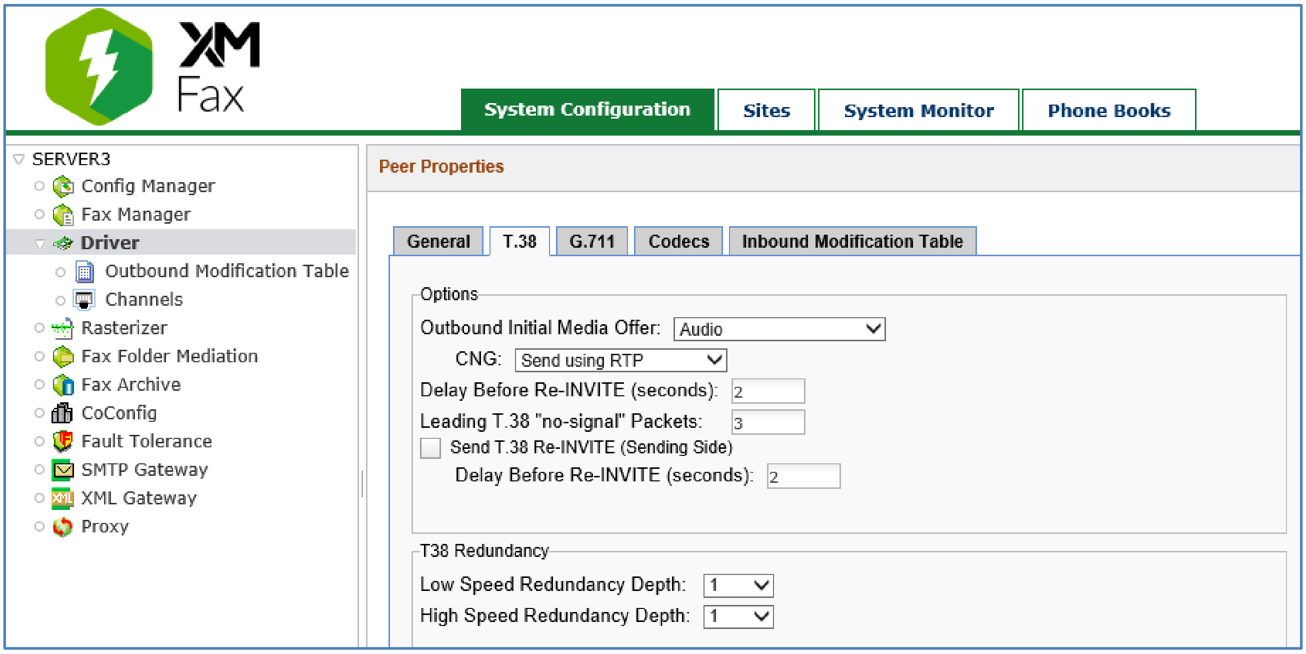
☑ V.29 Enabled

☐ Use Proxy

Host Name:

☐ Disable this peer for incoming calls

Select **T38** tab and leave all fields at default values.



Peer Properties

Options

Outbound Initial Media Offer: Audio

CNG: Send using RTP

Delay Before Re-INVITE (seconds): 2

Leading T.38 "no-signal" Packets: 3

□ Send T.38 Re-INVITE (Sending Side)

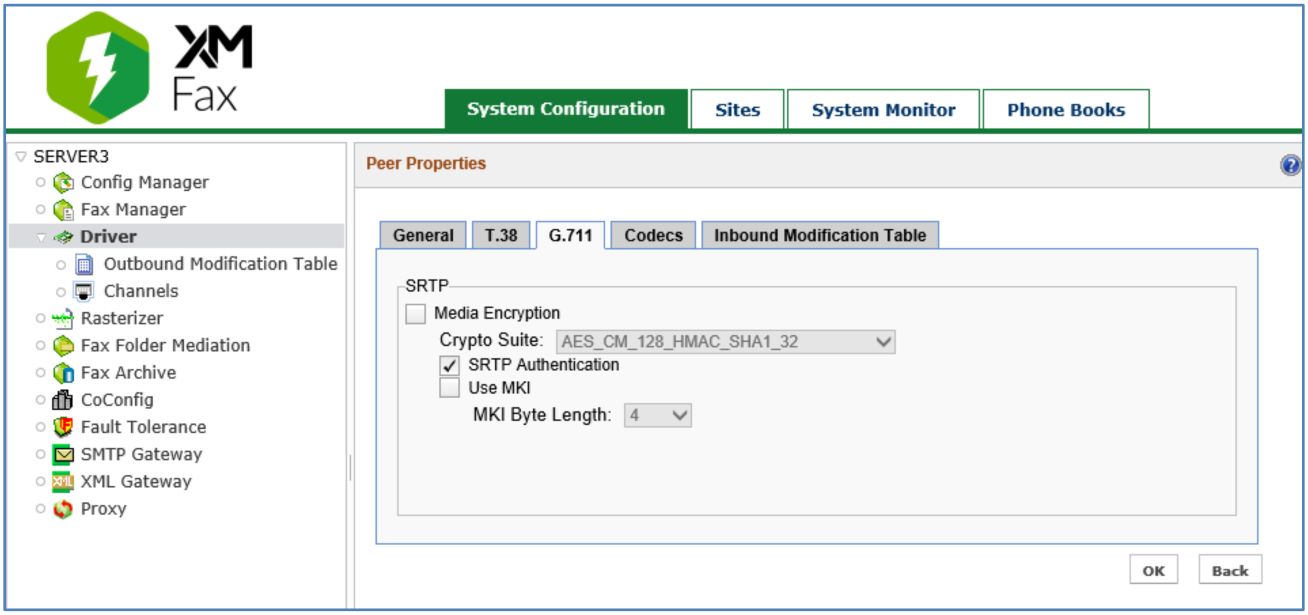
Delay Before Re-INVITE (seconds): 2

T38 Redundancy

Low Speed Redundancy Depth: 1

High Speed Redundancy Depth: 1

Select **G.711** tab and leave all fields at default values.



Peer Properties

SRTP

□ Media Encryption

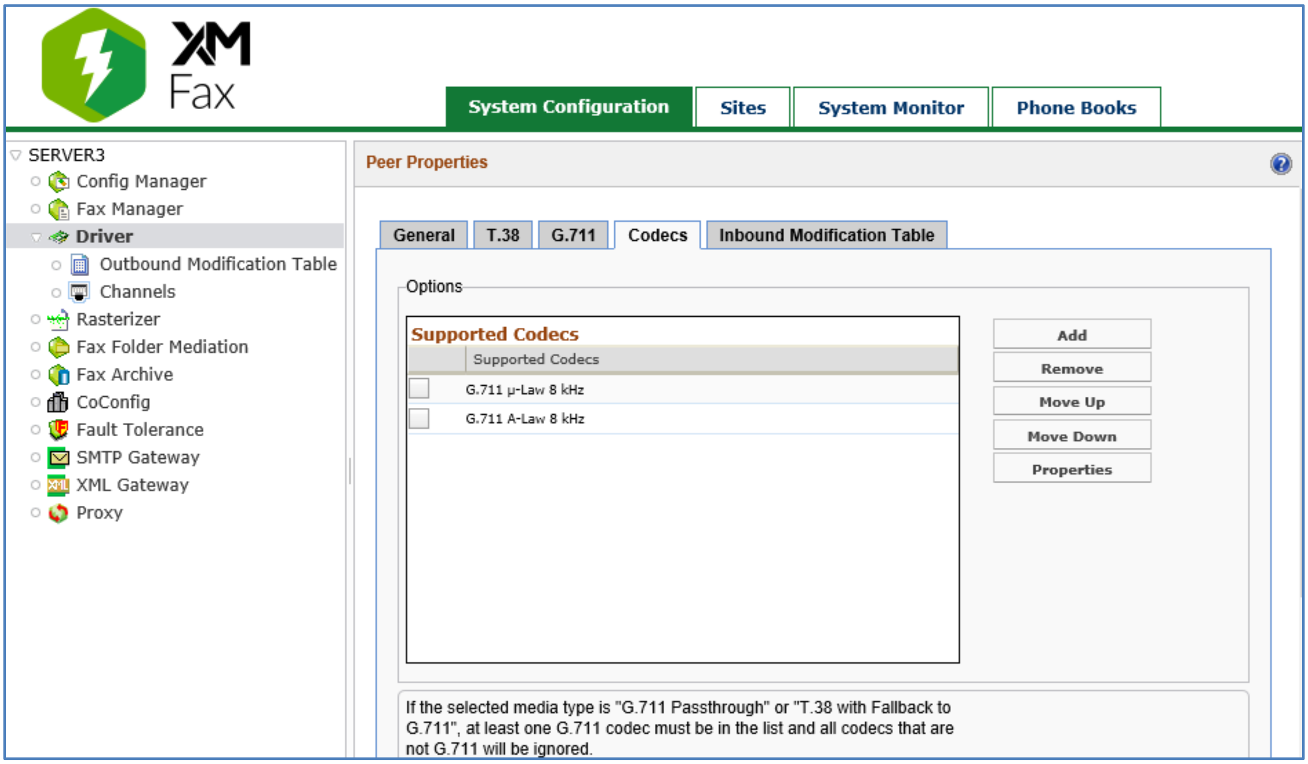
Crypto Suite: AES_CM_128_HMAC_SHA1_32

☑ SRTP Authentication

□ Use MKI

MKI Byte Length: 4

Select **Codecs** tab, in the **Codecs** tab select **Add** button to add a designed codecs to the **Supported Codecs** list. In the compliance test, two codecs ***G.711 Mu-law*** and ***G.711 A-Law*** were used.

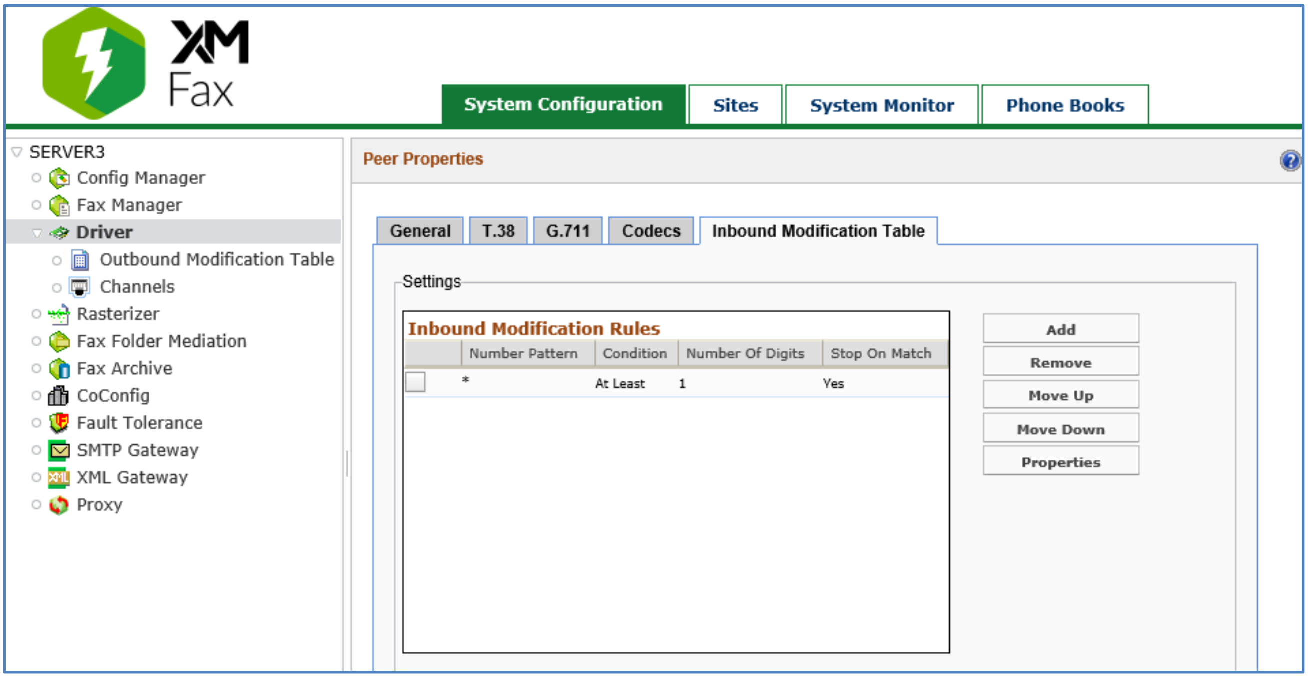


Supported Codecs

	Supported Codecs
□	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.

Select **Inbound Modification Table** tab and then select the **Add** button to add an inbound medication rule as shown in the screenshot below.



Inbound Modification Rules

	Number Pattern	Condition	Number Of Digits	Stop On Match
□	*	At Least	1	Yes

8. Verification Steps

The following steps may be used to verify the configuration:

- From Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling groups configured in **Section 5.5** are in-service.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

- From Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group configured in **Section 5.6** is in-service.

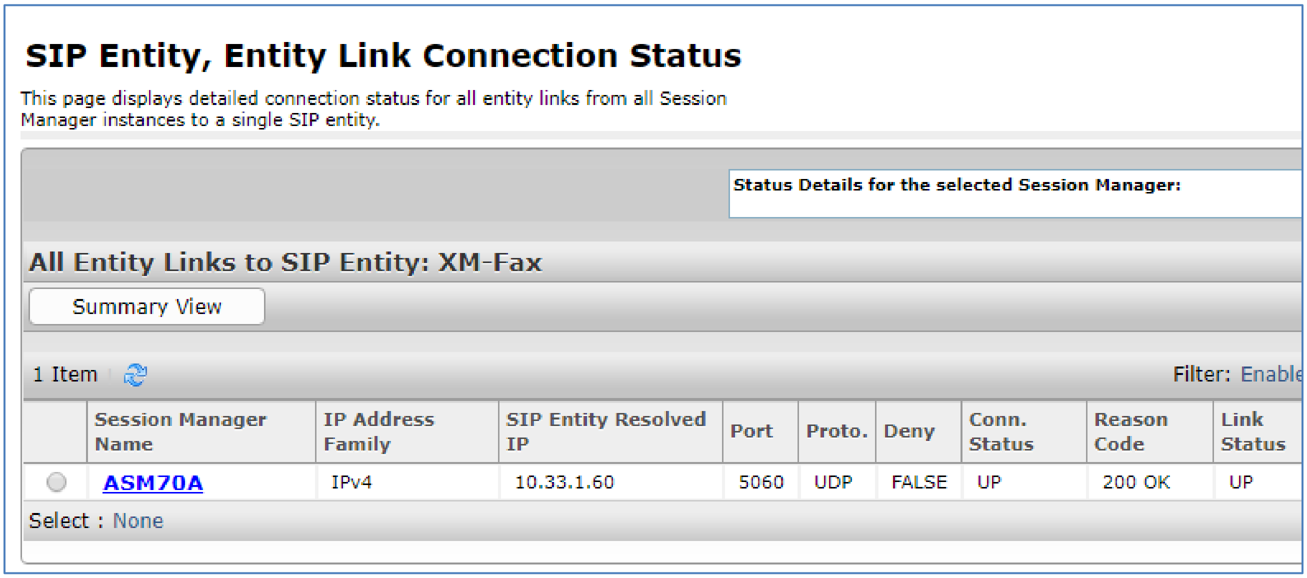
```
status trunk 1
                    TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
```

- Verify that fax calls can be placed to/from the XM fax server from both local and remote sites.
- From Communication Manager SAT, use the **list trace tac** command to verify that fax calls are routed to the expected trunks.

- From System Manager, confirm that the Entity Link between Session Manager and the XM Fax SIP Entity is UP.



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.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: XM-Fax

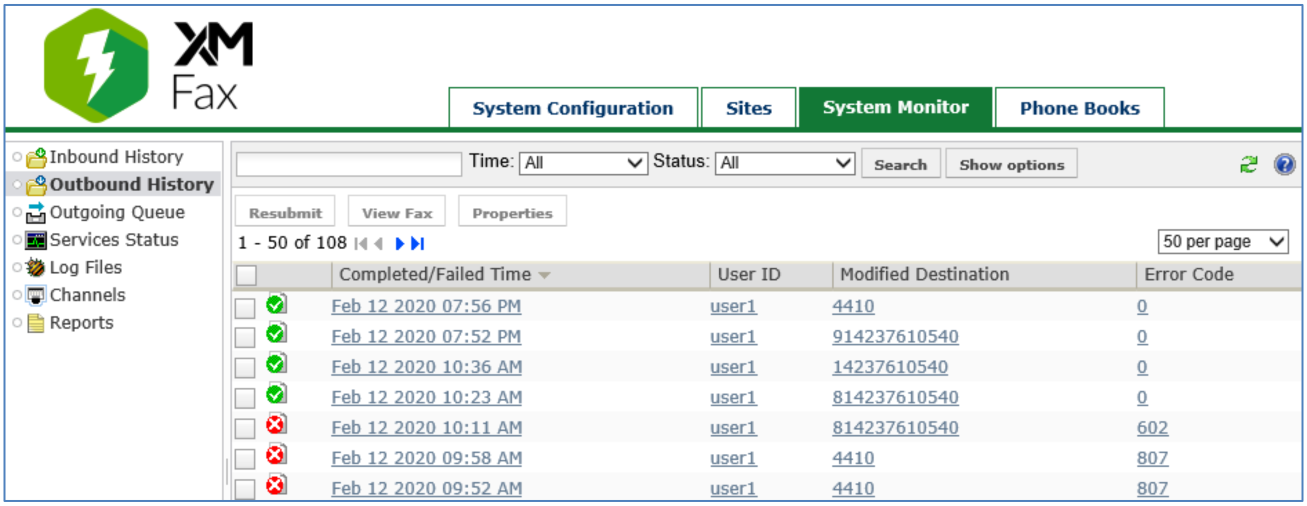
1 Item

Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ASM70A	IPv4	10.33.1.60	5060	UDP	FALSE	UP	200 OK	UP

Select : None

- Verify that fax calls can be placed to/from the XM Fax server from both local and remote sites. The screenshot below shows **System Monitor** of **Outbound History** of fax call in the XM Fax.



Time: All Status: All

1 - 50 of 108

50 per page

□		Completed/Failed Time	User ID	Modified Destination	Error Code
□	✓	Feb 12 2020 07:56 PM	user1	4410	0
□	✓	Feb 12 2020 07:52 PM	user1	914237610540	0
□	✓	Feb 12 2020 10:36 AM	user1	14237610540	0
□	✓	Feb 12 2020 10:23 AM	user1	814237610540	0
□	✗	Feb 12 2020 10:11 AM	user1	814237610540	602
□	✗	Feb 12 2020 09:58 AM	user1	4410	807
□	✗	Feb 12 2020 09:52 AM	user1	4410	807

9. Conclusion

These Application Notes describe the procedures required to configure XMedius XM Fax Software to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Please refer to **Section 2.2** for any exceptions or observations.

10. Additional References

This section references the documentation relevant to these Application Notes. The following and additional Avaya product documentation is available at http://support.avaya.com.

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 8.0.
4. *Administering Avaya Aura® System Manager for Release 8.0*, Release 8.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.
7. *Administering Avaya Aura® Communication Manager*, Release 8.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.0, 555-245-205.

XMedius XM Fax document in its most recent version may be found at https://support.xmediusfax.com (Sign In required)

1. XM Fax Installation and Maintenance Guide
2. XM Fax Administrator Guide – Web (Web interface)
3. XM Fax Administrator Guide – Windows (MMC Snap-In)
4. XM Fax User Guide

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.