Avaya Solution & Interoperability Test Lab

Application Notes for Configuring OceanFax from OceanX Technology Limited with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 using SIP Trunk – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning OceanFax from OceanX Technology to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 using SIP Trunk.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 steps required to connect OceanFax Server from OceanX Technology Limited with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. The OceanFax Server is a FoIP (Fax Over Internet Protocol) solution and is configured to connect via SIP Trunk to Session Manager.

2. General Test Approach and Test Results

The OceanFax Server is connected with Session Manager as a SIP Entity and it is configured as a trusted entity. Faxes are sent in and out of this server on configured channels. A simulated PSTN is setup with a tie trunk link to another Communication Manager.

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 compliance testing included the test scenarios shown below. Internal fax test is conducted by sending fax out from one channel and back through another channel of the same SIP Trunk. A simulated PSTN is setup with a tie trunk link to another Communication Manager.

- Internal Fax calls
- Fax calls sent to the PSTN
- Fax calls received from PSTN
- Fax calls sent to the PSTN via transfer or forwarding on local or remote phone
- Fax calls received from the PSTN via transfer or forwarding on local or remote phone
- Verification of correct status and Caller ID for sent and received fax messages
- Successful transmission and receiving of 30 page fax via PSTN
- Successful recovery from network or power failure

2.2. Test Results

All test cases passed successfully and the following were observed:

- It takes 2 retries for 30 pages of fax to be successfully sent.
- To ensure that OceanFax recovers properly after a reboot, OceanFax Services has to be configured properly, or some services may not restart properly if the SQL Database service has not already started. Refer to **Section 7.2** of **Starting OceanFax services** for further details. User options also need to be set with appropriate number of retries and interval.

2.3. Support

Technical support on OceanFax can be obtained through the following:

- Web: http://www.oceanfax.com
- Phone: +852-3977-0088
- Email: isupport@oceanfax.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The remote party Fax Machine (Windows Fax on PC with modem) is connected to an analog port of a Communication Manager R6.3 via a simulated PSTN link (H.323 tie trunk). For SIP Trunk setup, the OceanFax Server running on a Windows 2008 R2 virtual machine is registered as a trusted SIP entity on a Session Manager R6.3 connecting to a Communication Manager R6.3.

.

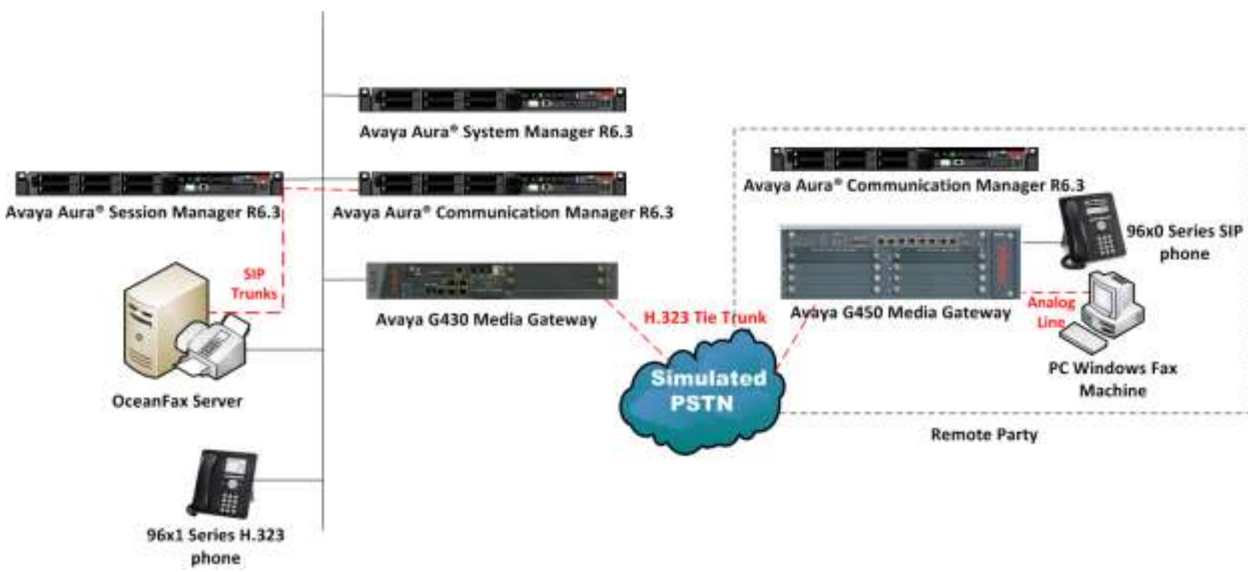


Figure 1: Network Solution of OceanFax Server with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment Description	Software Release
Avaya Aura® Communication Manager running on S8800 Server	6.3 (Build R016x.03.0.124.0-22147)
Avaya Aura® Session Manager running on VMware 5.1	6.3.13.0.631304
Avaya Aura® System Manager running on VMware 5.1	6.3.13.10.3336
Avaya G430 Media Gateway	FW 36.13.0
Avaya 96x1 Series (H.323) Deskphone	6.6028
Windows 2008 Virtual Server R2 running on VMware 5.1	OceanFax Server 3.0 SP2
Windows Fax Machine	Windows 7 SP1

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- System Features and Access Codes
- Administer Dial Plan
- Configure SIP Trunk
- Configure IP Network Region and IP Codec
- Administer Private Numbering
- Administer Route Selection for OceanFax calls

Note: The configuration of the H.323 tie trunk interface as the simulated PSTN is outside the scope of these Application Notes. The OceanFax server will hereafter be called OceanFax in short for configuration.

5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** has sufficient capacity. Each fax call to and from OceanFax uses a minimum of one SIP trunk. Calls that are routed back to Communication Manager to access the PSTN use two SIP trunks.

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

IP PORT CAPACITIES                                             USED
                    Maximum Administered H.323 Trunks: 12000 70
          Maximum Concurrently Registered IP Stations: 18000 10
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
             Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 41000 0
                  Maximum Video Capable IP Softphones: 18000 6
                      Maximum Administered SIP Trunks: 24000 28
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   2
                    Maximum Media Gateway VAL Sources: 250   1
          Maximum TN2602 Boards with 80 VoIP Channels: 128   0
         Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                     Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** and **Private Networking** are set to **y**.

```
display system-parameters customer-options                     Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n              Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n       Station as Virtual Extension? y
                     Multiple Locations? y
                                             System Management Data Transfer? n
          Personal Station Access (PSA)? y                Tenant Partitioning? y
                        PNC Duplication? n         Terminal Trans. Init. (TTI)? y
                   Port Network Support? y                Time of Day Routing? y
                        Posted Messages? y         TN2501 VAL Maximum Capacity? y
                                                         Uniform Dialing Plan? y
                     Private Networking? y       Usage Allocation Enhancements? y
               Processor and System MSP? y
                     Processor Ethernet? y                  Wideband Switching? y
                                                                      Wireless? y
                          Remote Office? y
          Restrict Call Forward Off Net? y
                  Secondary Data Module? y
```

5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction).
An alternative to enabling this feature on a system wide basis is to utilize COR (Class of Restriction) administration. See **Section 10** reference **[1]** for details.

```
change system-parameters features                               Page   1 of  20
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? y
```

Use the **display feature-access-codes** command to verify that a feature access code (FAC) has been defined for both AAR and ARS.

```
display feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *06    Deactivation: *07
Call Forwarding Activation Busy/DA: *08    All: #09    Deactivation: *10
   Call Forwarding Enhanced Status: *11    Act: *12    Deactivation: *13
                         Call Park Access Code: *14
                       Call Pickup Access Code: *15
CAS Remote Hold/Answer Hold-Unhold Access Code: *94
                  CDR Account Code Access Code: *16
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.3. Administer Dial Plan

For the testing, two number ranges were used on Communication Manager. The first range is used for stations configured on Communication Manager and are defined in the dial plan as **ext,** these begin with **1** and are five digits in length. The second range is used to deliver and identify calls to OceanFax, this range begins with digit **7**, are five digits long, and are also defined as **ext** within the dial plan.

```
change dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call      Dialed   Total  Call
    String   Length Type     String   Length Type      String   Length Type
   0           1   attd
   1           5   ext
   2           5   ext
   22          4   ext
   32          4   ext
   33          2   fac
   4           6   ext
   5           4   ext
   6           5   ext
   7           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   dac
```

5.4. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and Session Manager (**sm1**). The host names will be used in for administration of the Signaling Group form in this section.

```
list node-names all

                        NODE NAMES

Type     Name                IP Address
IP       default             0.0.0.0
IP       lsp-g430            10.1.40.10
IP       n                   10.3.10.253
IP       procr               10.1.10.230
IP       procr6              ::
IP       s8500-clan1         10.1.10.21
IP       s8500-clan2         10.1.10.22
IP       s8500-medpro1       10.1.10.31
IP       s8500-medpro2       10.1.10.32
IP       s8500-val1          10.1.10.36
IP       site6               10.1.60.10
IP       sm1                 10.1.10.60
IP       sm2                 10.1.10.42
```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or **tls** (Transport Layer Security). The protocol **tls** is selected in this setup
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Specify the node names for the **procr** of the Communication Manager server and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown in previous page
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown in the previous page
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm1**), also shown in the previous page
- Ensure that the recommended port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields for tls as Transport Method
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.5.** This field logically establishes the **far-end** for calls using this signaling group as network region 6
- Set the **Far-end Domain** field to the appropriate domain and in this Compliance test **sglab.com** is used.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833
- The default values for the other fields may be used

```
add signaling-group 7                                              Page   1 of   2
                                SIGNALING GROUP

 Group Number: 7             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        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: sm1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 6

Far-end Domain: sglab.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
                                                  Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from OceanFax via Session Manager. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field configured earlier, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
change trunk-group 7                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 7                   Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SM1           COR: 1        TN: 1        TAC: #07
   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: 7
                                                    Number of Members: 14
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed value to prevent unnecessary SIP messages during call setup. For the compliance test the value of **1800** was used.

```
change trunk-group 7                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                           Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 1800

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n




 Caller ID for Service Link Call to H.323 1xC: station-extension
```

5.5. Configure IP Network Region and IP Codec

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the SIP domain name configured on Session Manager. In this configuration, the **Authoritative** domain name is **sglab.com**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to OceanFax via Session Manager as **ip-network region 6** is specified in the SIP signaling group.

```
display ip-network-region 6                                         Page   1 of  20
                               IP NETWORK REGION
  Region: 6
Location: 1       Authoritative Domain: sglab.com
    Name: To Session Manager 6  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 6              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the supported audio codecs for calls routed over the SIP trunk to OceanFax via Session Manager. The form is accessed via the **change ip-codec-set n** command, where **n** is the associated ip-codec-set.. Note that IP codec set **6** was specified in the IP Network Region 6 form shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference. The example below includes **G.711MU** (mu-law) and **G.711A** (a-law) codecs which are supported by OceanFax.

```
change ip-codec-set 6                                               Page   1 of   2

                          IP CODEC SET

    Codec Set: 6

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.711A            n          2        20
```

On page 2, set the **FAX Mode** to **t.38-standard** with **Redundancy 0** and **ECM** (Error Correction Mode) to **y**Note that for any internal fax calls between Port Networks and other digital tie trunks except the SIP Trunk to OceanFax, IP Codec FAX Mode has to be set as **pass-through** to mitigate delay because T.38 willl not shuffle between Port Networks (PN) (see **Section 10** reference **[5]** document Appendix E).

```
display ip-codec-set 6                                          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
```

5.6. Administer Private Numbering

Private numbering is used for OceanFax 7xxxx extensions. Use the **change private-numbering n** command, where **n** is the first digit of the extension range to be used for private numbering. Configure the **Ext Code** as **7** and the **Trk Grp(s)** as **7** with **Total Len** as **5**.

```
change private-numbering 7                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private            Total
Len Code             Grp(s)      Prefix             Len
 5  1                6                              5     Total Administered: 5
 5  1                7                              5        Maximum Entries: 540
 5  2                10                             5
 6  4                7                              6
 5  7                7                              5
```

5.7. Administer Route Selection for OceanFax Calls

As digits 7xxxx were defined in the dial plan as **ext** in **Section 5.3**, use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **7** that are **5** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to AAR for further processing.

```
change uniform-dialplan 7                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert             Node
  Pattern         Len Del     Digits      Net Conv Num
 7                 5   0                  aar  n
```

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to OceanFax begin with **7** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 6**, which contains the outbound SIP Trunk Group. Set the Call Type as private **lev0**.

```
change aar analysis 7                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
          7                5    5     6       lev0         n
```

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 6** is used to route calls to trunk group **(Grp No) 7** with the appropriate FRL level. Set **Numbering Format** to **lev0-pvt**.

```
change route-pattern 6                                         Page   1 of   3
                    Pattern Number: 6      Pattern Name: non-IMS to SM
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 7    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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 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
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
```

6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

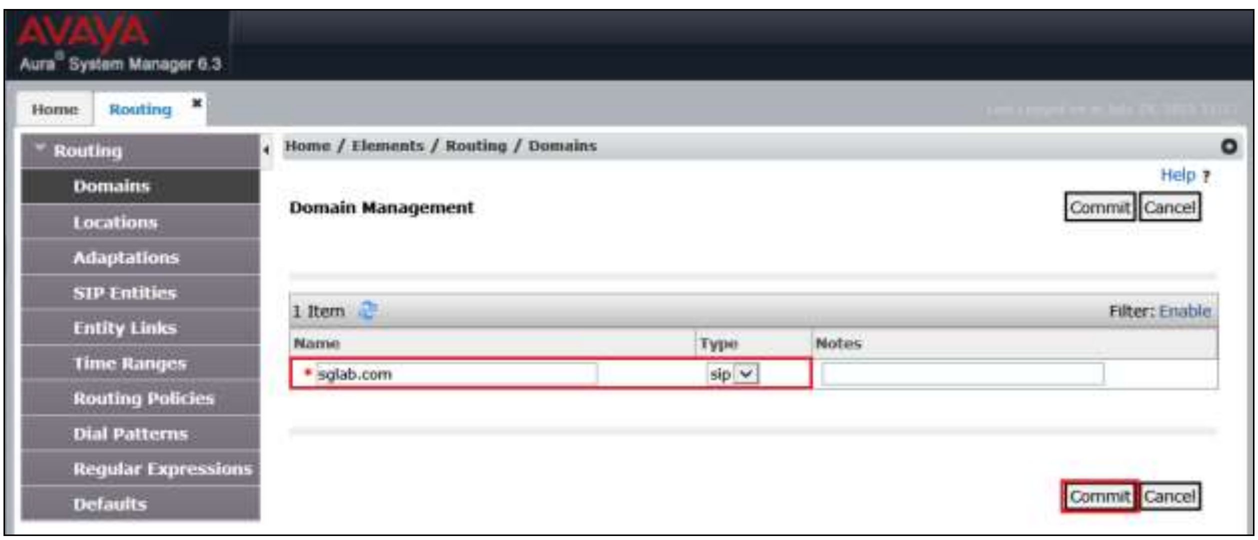
- Log in to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer SIP Entity Link
- Administer Routing Policies
- Administer Dial Patterns

6.1. Log in to Avaya Aura® System Manager

Access System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown).

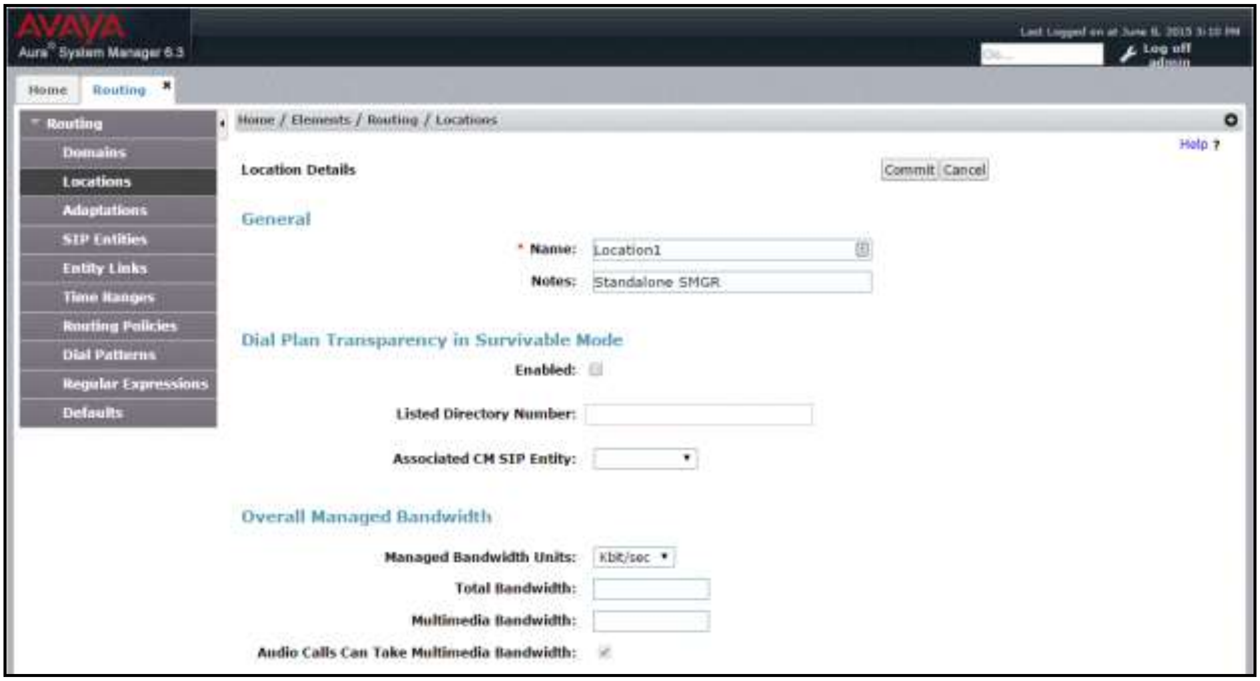
6.2. Administer SIP Domain

SIP domains are created as part of Session Manager basic configuration. There will be at least one SIP Domain for which System Manager is the authoritative SIP controller. In these sample notes it is **sglab.com**. Navigating from the Home screen, under the **Elements** section click **Routing → Domains → New** (not shown), enter the domain **Name,** select the **Type** as **sip** and click **Commit**.

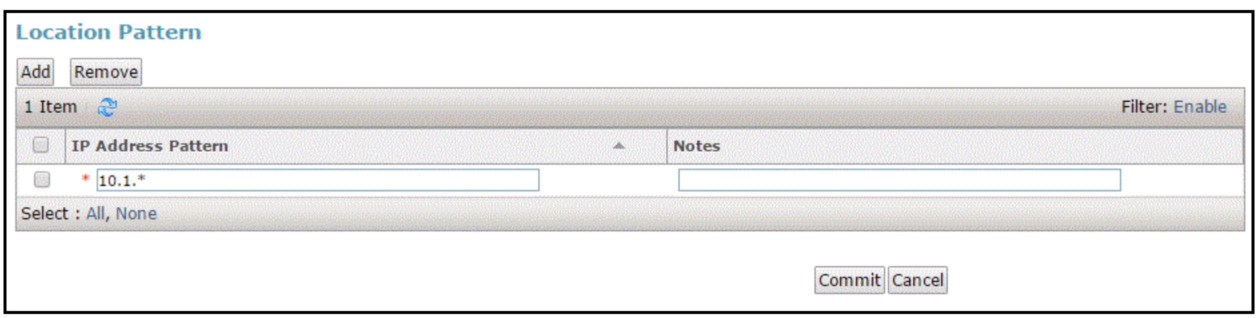


6.3. Administer Location

Session Manager uses the origination location to determine which dial patterns to look at when routing a call. In this example, one Location has been created which will reference both the Session Manager and OceanFax location. Navigate to **Home → Elements → Routing → Locations → New** (not shown) enter an identifying **Name**, as shown below.



At the bottom of the same page the **Location Pattern** is defined. Click **Add** and enter the IP address range used to logically identify the location. In this case the **IP Address Pattern** is **10.1.*** as shown below. Click **Commit**.

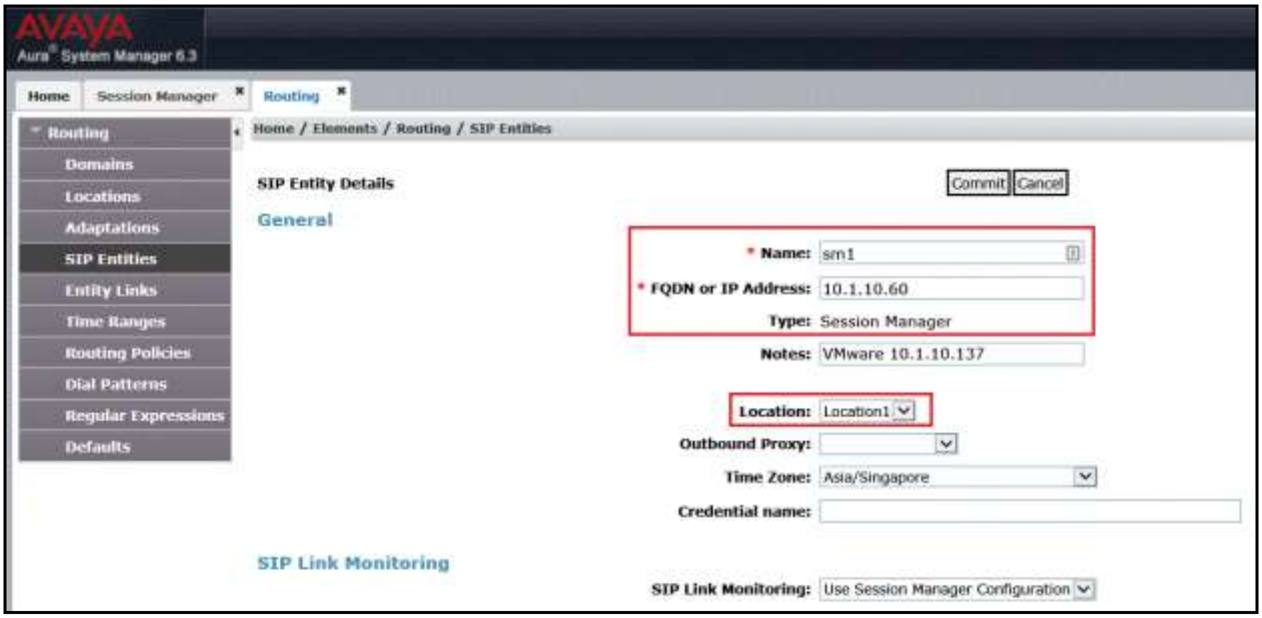


6.4. Administer SIP Entities

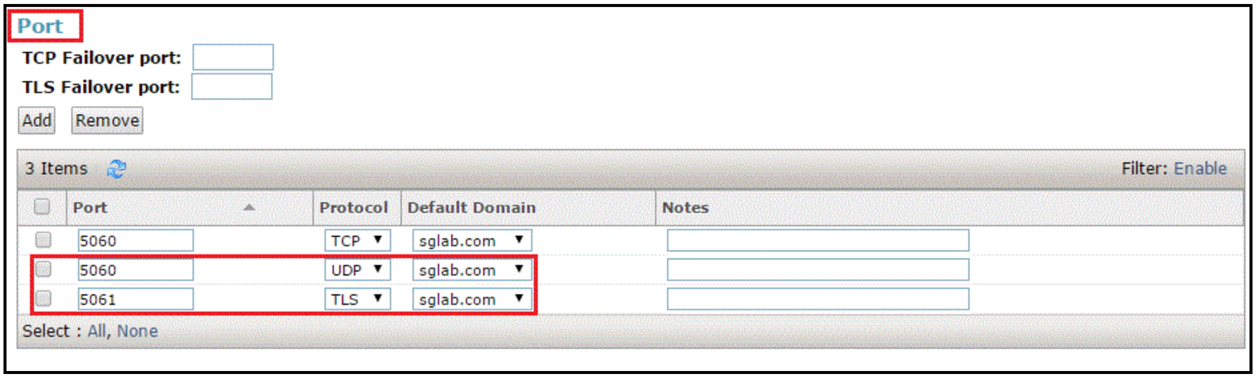
Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for Session Manager SIP Signaling Interface, Communication Manager and OceanFax Solution respectively.

6.4.1. Configure Session Manager SIP Signaling Interface Entity

Click **Home → Elements → Routing → SIP Entities → New** (not shown). Assign an identifying **Name**, the **FQDN or IP Address** for Session Manager SIP Signaling Interface, set the **Type** to **Session Manager** and the **Location** to the Location configured in **Section 6.3** and click on **Commit** (not shown)**.**

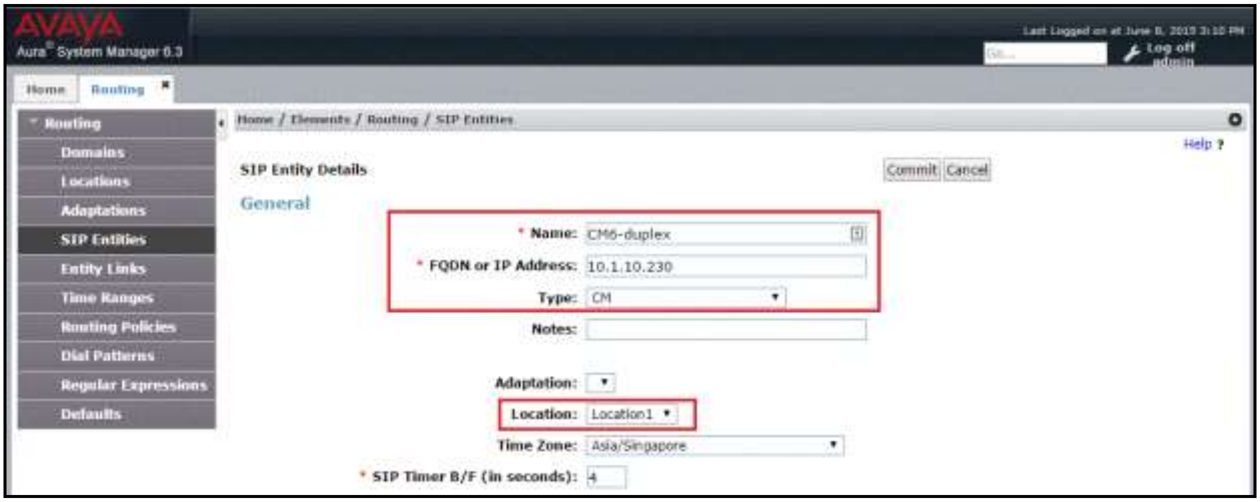


Tick the box next to the entity that was just created and click **Edit** (not shown)**.** Scroll down the page until the **Port** section is displayed, click **Add** and configure the **Port** as **5061** the **Protocol TLS** and the **Default Domain** as the domain configured in **Section 6.2** this corresponds with the signaling group configured in **Section 5.4.** Repeat this for the **UDP** connection which will be established to the OceanFax, as shown below. Click **Commit**.



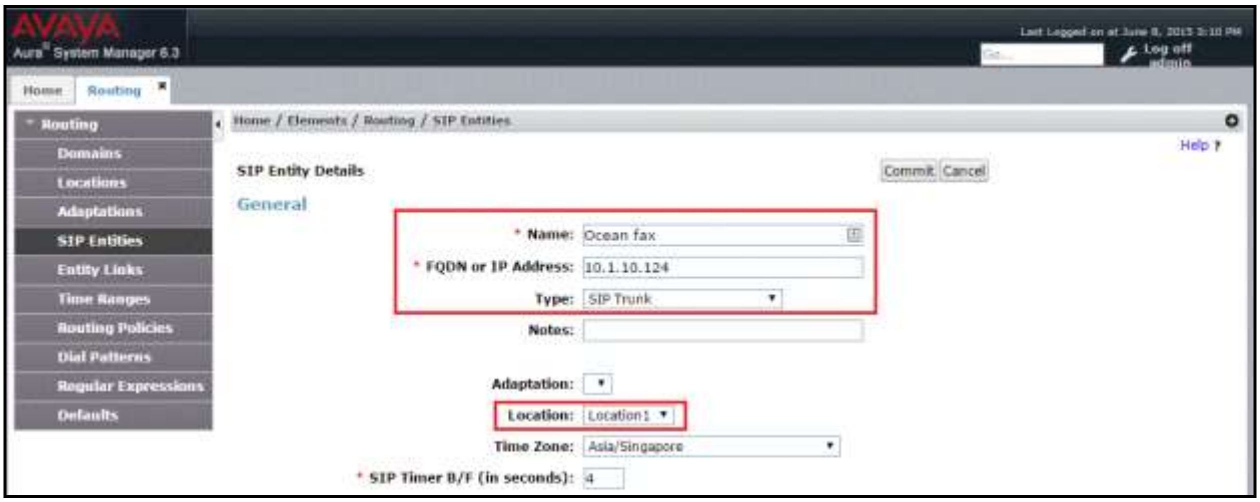
6.4.2. Configure Avaya Aura® Communication Manager Entity

Click **Home → Elements → Routing → SIP Entities → New** (not shown).Assign an identifying **Name**, the **FQDN or IP Address** for the processor, set the **Type** to **CM** and the **Location** to the Location configured in **Section 6.3** and click **Commit**.



6.4.3. Configure OceanFax SIP Entity

Click **Home → Elements → Routing → SIP Entities → New** (not shown) assign an identifying **Name**, the **FQDN or IP Address** for the OceanFax, set the **Type** to **SIP Trunk**, leave all other settings default and click **Commit**.



6.5. Administer SIP Entity Link

A SIP Trunk between Session Manager and a telephony system is described by an Entity Link. An entity link needs to be created between Session Manager and both Communication Manager and OceanFax.

6.5.1. Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Aura® Communication Manager

Click on **Home → Elements → Routing → Entity Links → New** (not shown). Assign an identifying **Name** and choose the entity assigned to Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TLS**, enter **5061** for the **Port**, for **SIP Entity 2** choose Communication Manager and set the **Port** to **5061**, select **Trusted** from the **Connection Policy** drop-down list. Click **Commit**.

6.5.2. Administer SIP Entity Link from Avaya Aura® Session Manager to OceanFax

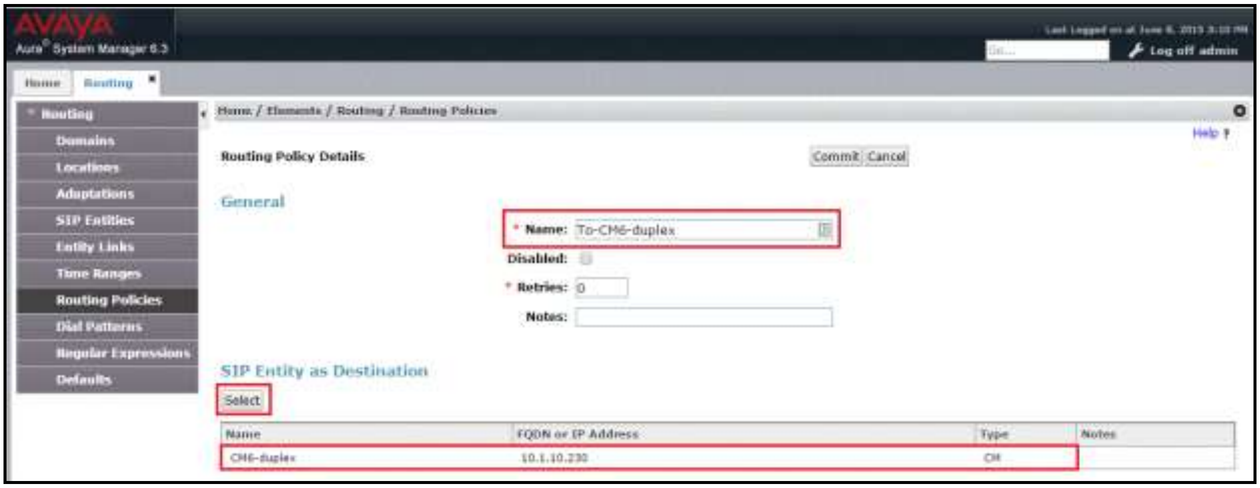
Click on **Home → Elements → Routing → Entity Links → New** (not shown) assign an identifying **Name** choose the entity assigned to Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **UDP**, enter **5060** for the **Port**, choose the OceanFax entity as SIP Entity 2 and set the **Port** to **5060**, select **Trusted** from the **Connection Policy** drop-down list. Click **Commit**. This establishes the SIP Trunk between Session Manager and OceanFax.

6.6. Administer Routing Policies

To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to an attached system. Two routing policies must be created, one routing policy for Communication Manager and a second routing policy for OceanFax. These will be associated with the Dial Patterns created in **Section 6.7**.

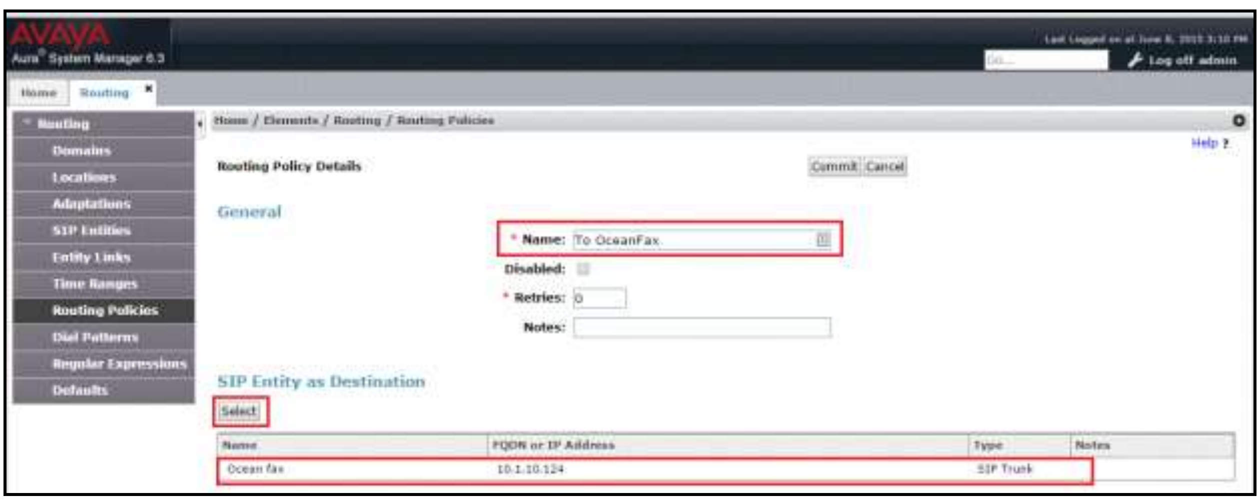
6.6.1. Create Routing Policy to Avaya Aura® Communication Manager

Click **Home → Elements → Routing → Routing Polices →New** (not shown) assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the Communication Manager SIP Entity and click **Select**. Click **Commit** when done.



6.6.2. Create Routing Policy to OceanFax

Click **Home → Elements → Routing → Routing Polices →New** assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the Ocean fax SIP Entity and click **Select**. Click **Commit** when done.

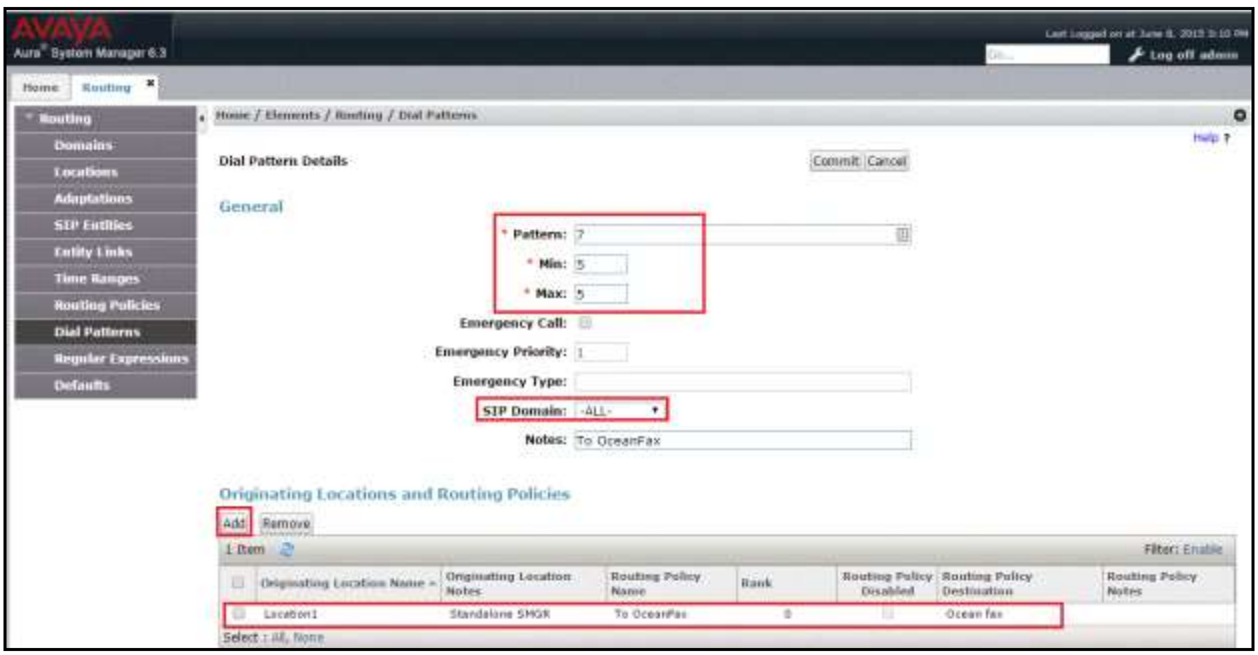


6.7. Administer Dial Patterns

As one of its main functions, Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate system.

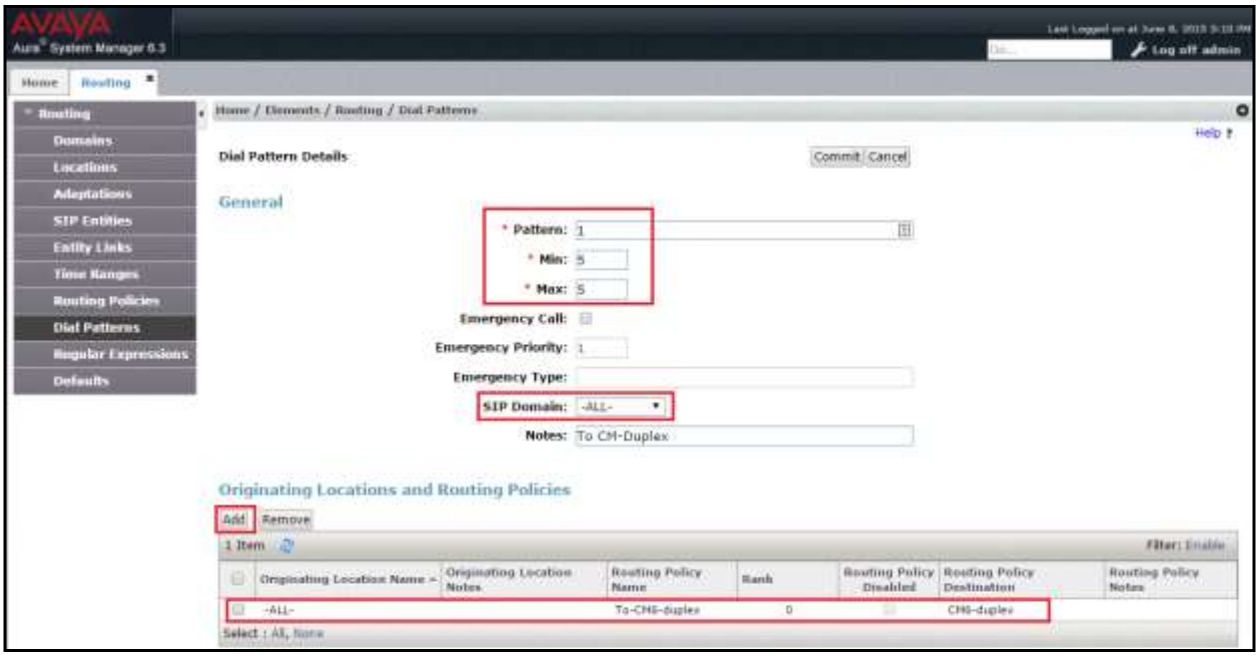
6.7.1. Create Dial Pattern to OceanFax

In **Section 5.6** Communication Manager is configured to route the dialed numbers beginning **7**xxxx to Session Manager. To create a Dial Pattern to route **7**xxxx from Session Manager to OceanFax, click **Home → Elements → Routing → Dial Patterns →New** (not shown). For the field **Pattern,** enter the numbers presented to Session Manager by Communication Manager which are destined for OceanFax. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section (not shown) click the location created in **Section 6.3**, in the **Routing Policies** section (not shown) click the routing policy created for OceanFax. Click **Select**. Click **Commit**.



6.7.2. Create Dial Pattern to Avaya Aura® Communication Manager

An additional Dial Pattern must be created on Session Manager to route incoming calls from OceanFax to Communication Manager stations 1xxxx. To create a Dial Pattern to route 1xxxx from Session Manager to Communication Manager, click **Home → Elements → Routing → Dial Patterns →New.** Under **Pattern** enter the numbers presented to Session Manager by OceanFax destined for Communication Manager, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**. In the **Originating Locations and Routing Policies** section of the web page, click **Add.** In the **Origination Location** section (not shown)**,** click **All**, in the **Routing Policies** section (not shown) click the routing policy created for Communication Manager. Click **Select.** Click **Commit**.



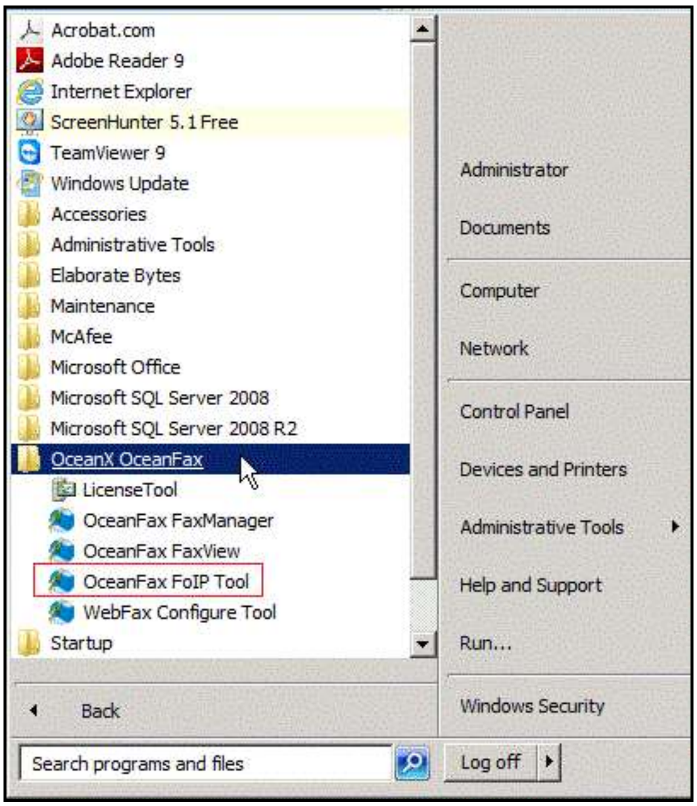
7. Configure OceanFax Server

The installation of the appropriate software, database and drivers as well as the license required will not be detailed here. Please refer to the OceanFax installation guide referenced in **Section 10** for more details. The configuration of OceanFax consists of the following.

- Configure Controller
- Starting the OceanFax services
- Adding a User

7.1. Configure Controller

Click on **Start → OceanX OceanFax →OceanFax FoIP Tool.**

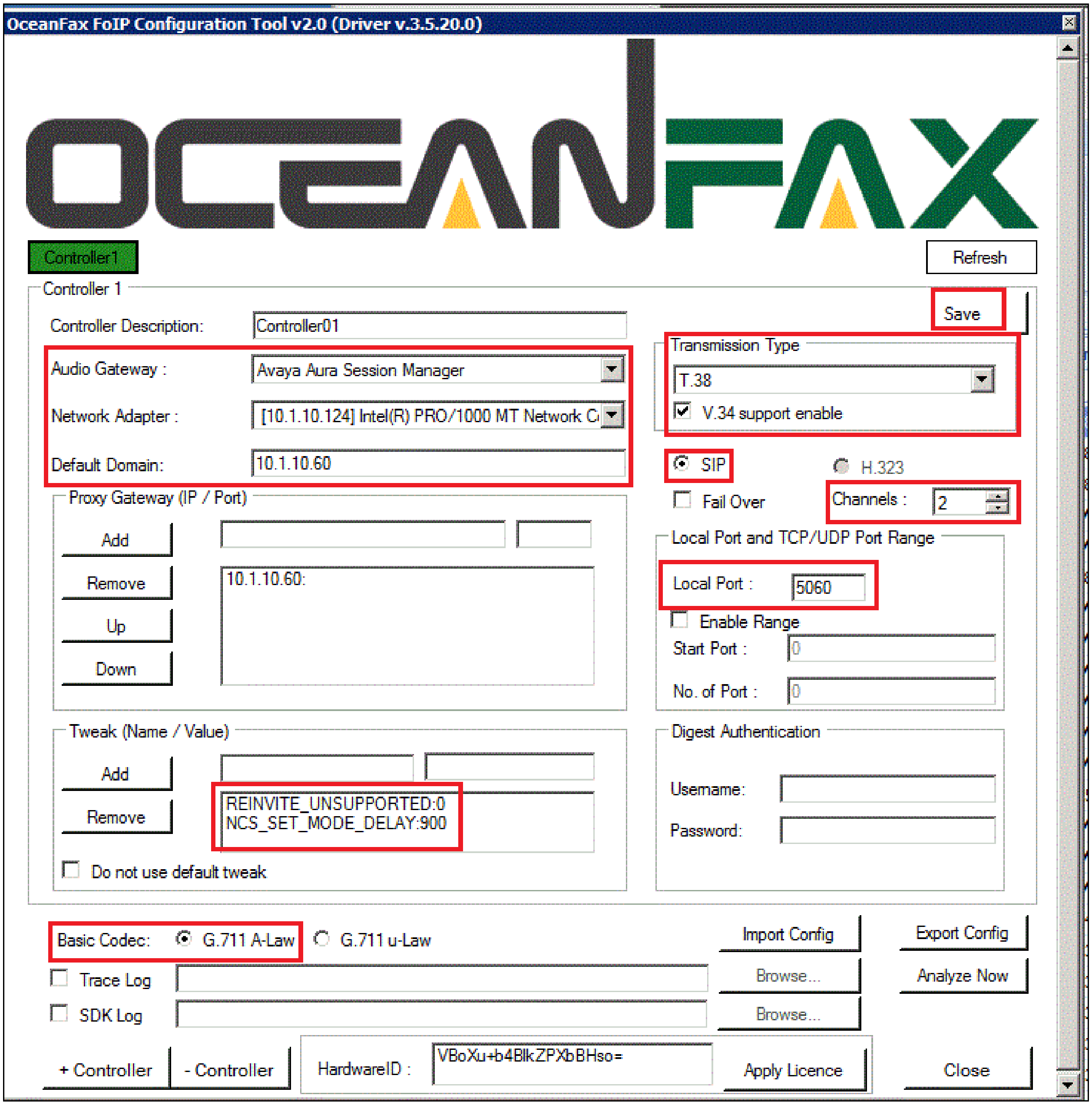


Configure the OceanFax controller as follows:

- Select from the drop down menu **Avaya Aura Session Manager** as the Audio Gateway
- Select the appropriate **Network Adapter** for connection to the fax network. The IP address of the OceanFax is shown here for ease of identification
- In the **Default Domain** enter the IP Address of Session Manager SIP signaling interface entity as configured in **Section 6.4.1**
- Select the **Transmission Type** as **T.38** which corresponds to the setting for IP Codec in **Section 5.5**. For fax to work with V.34, checked **V.34 support enable**

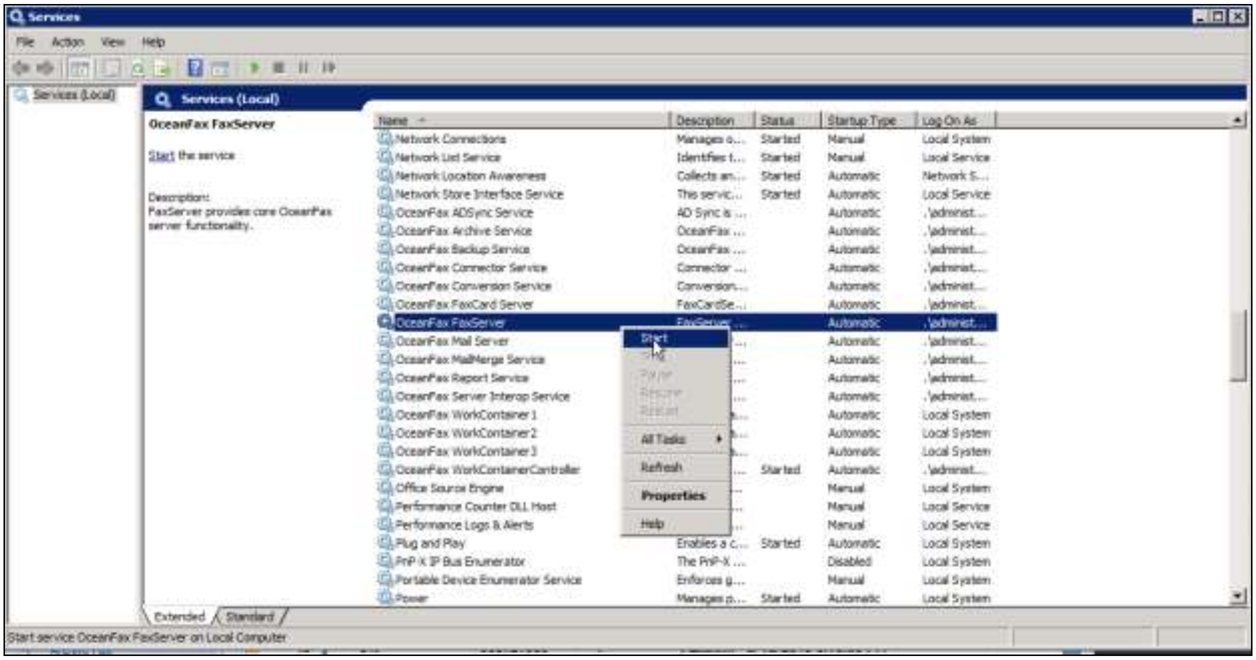
- Select **SIP** for telephony protocol and set the appropriate number of **Channels** required
- Set the **Local Port** as **5060** under the section for **Local Port and TCP/UDP Port Range** for SIP signaling.
- Select the **Basic Code**c as either **G.711 A-Law** or **G.711u-Law** which are both supported by Communication Manager set in the IP Codec form in **Section 5.5**
- Under the section **Tweak**, the tweak strings and values are listed for fine tuning to support Session Manager SIP protocol

Click **Save** at the top right corner for the system to remember the settings.



7.2. Starting OceanFax services

In Window Services, search for OceanFax services. Right-click and start the **OceanFax FaxServer** service first. Right click and start the other OceanFax services as appropriate.

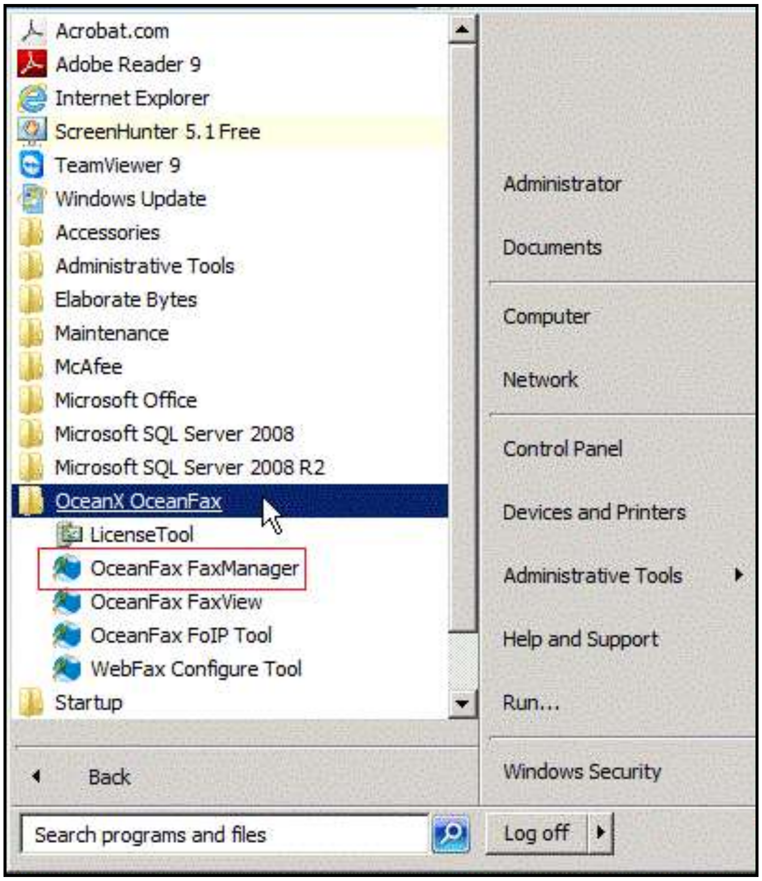


Sometimes the OceanFax FaxServer service could not automatically start after reboot because the MSSQL server services have not yet started.

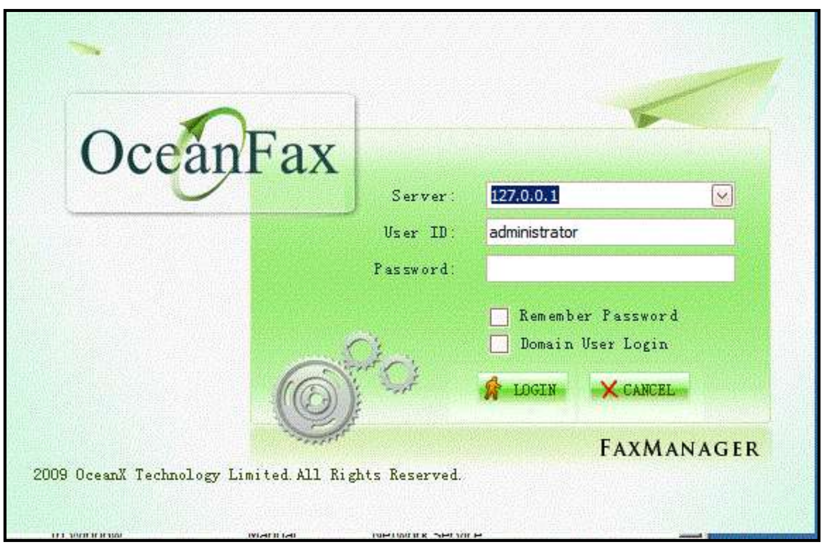
There are two options available for each of the OceanFax service:

- Set the **OceanFax FaxServer** service to be **Automatic (Delayed Start)** via services.msc and /or
- Set the **OceanFax FaxServer** service dependencies with **MSSQL$SQLEXPRESS** in windows registry so that the FaxServer service will only start when the MSSQL server express service has been started successfully.

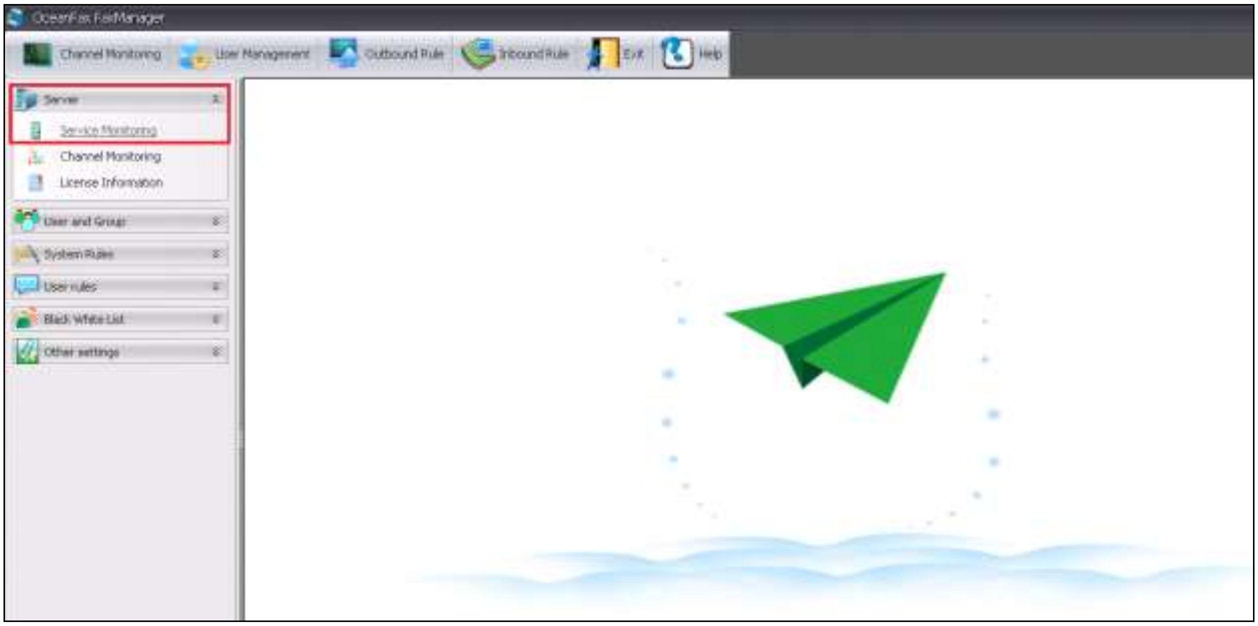
The OceanFax window services can be also viewed in OceanFax FaxManager. Click on **Start→Programs→OceanX OceanFax→OceanFax FaxManager**



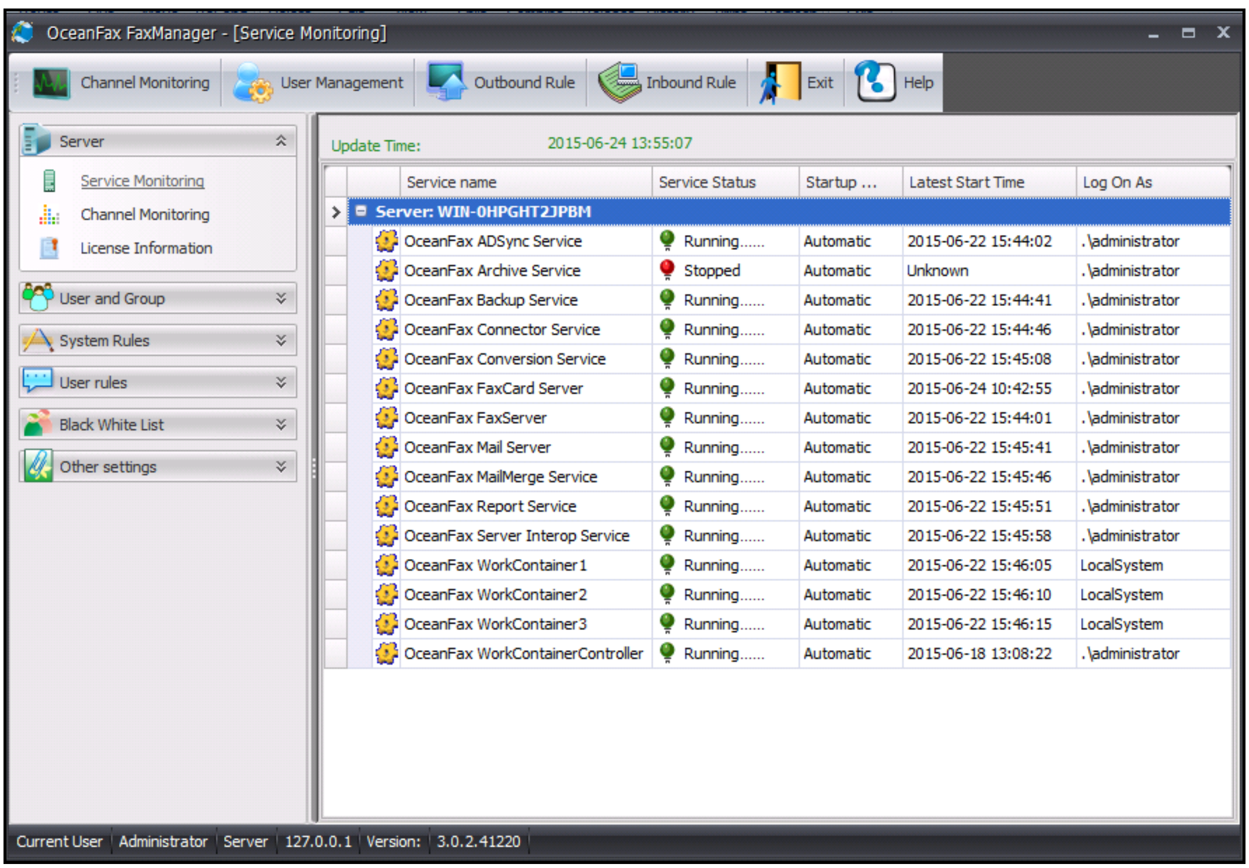
Enter the proper credentials then click on **LOGIN**



In the left window select **Server→Service Monitoring**,

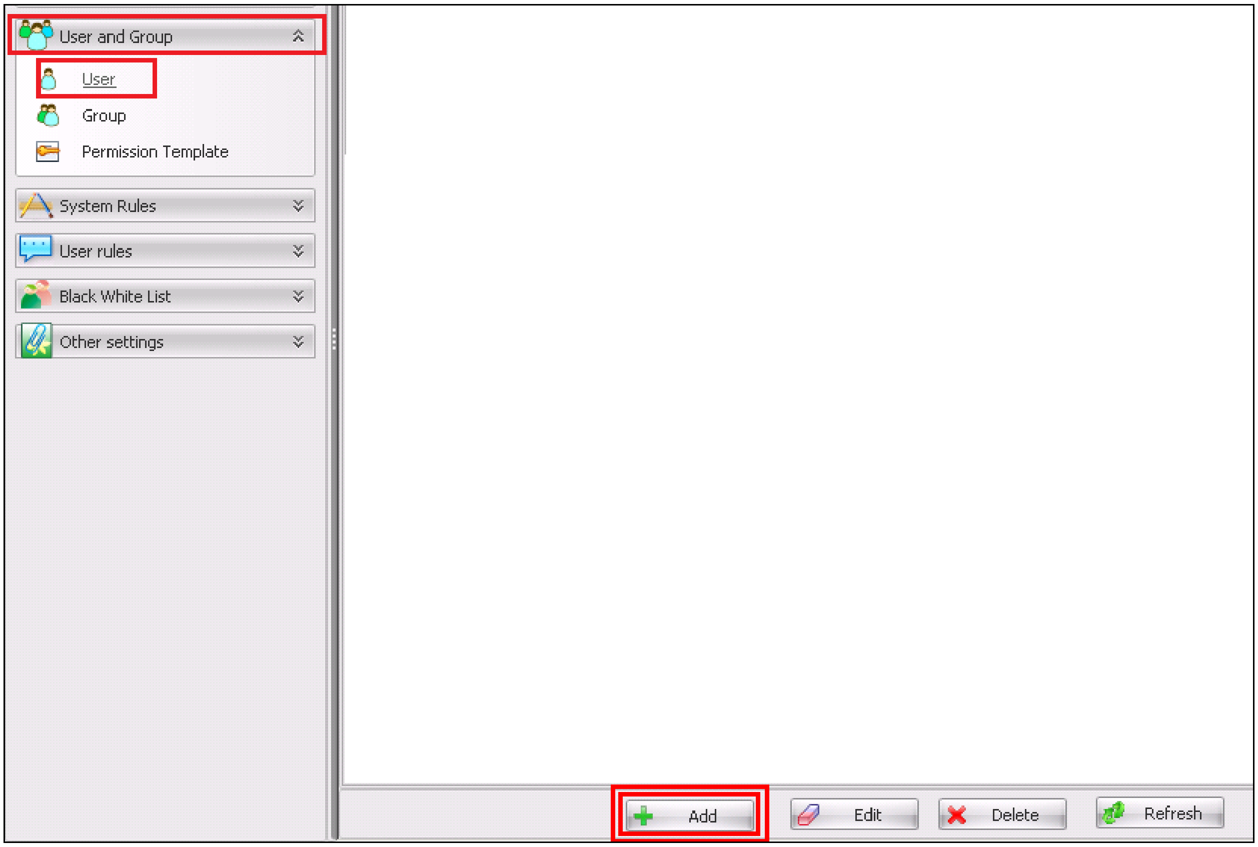


A list of service opens in the main window. The list of services correspond to what is seen on the windows services.msc shown in the earlier part of this section.

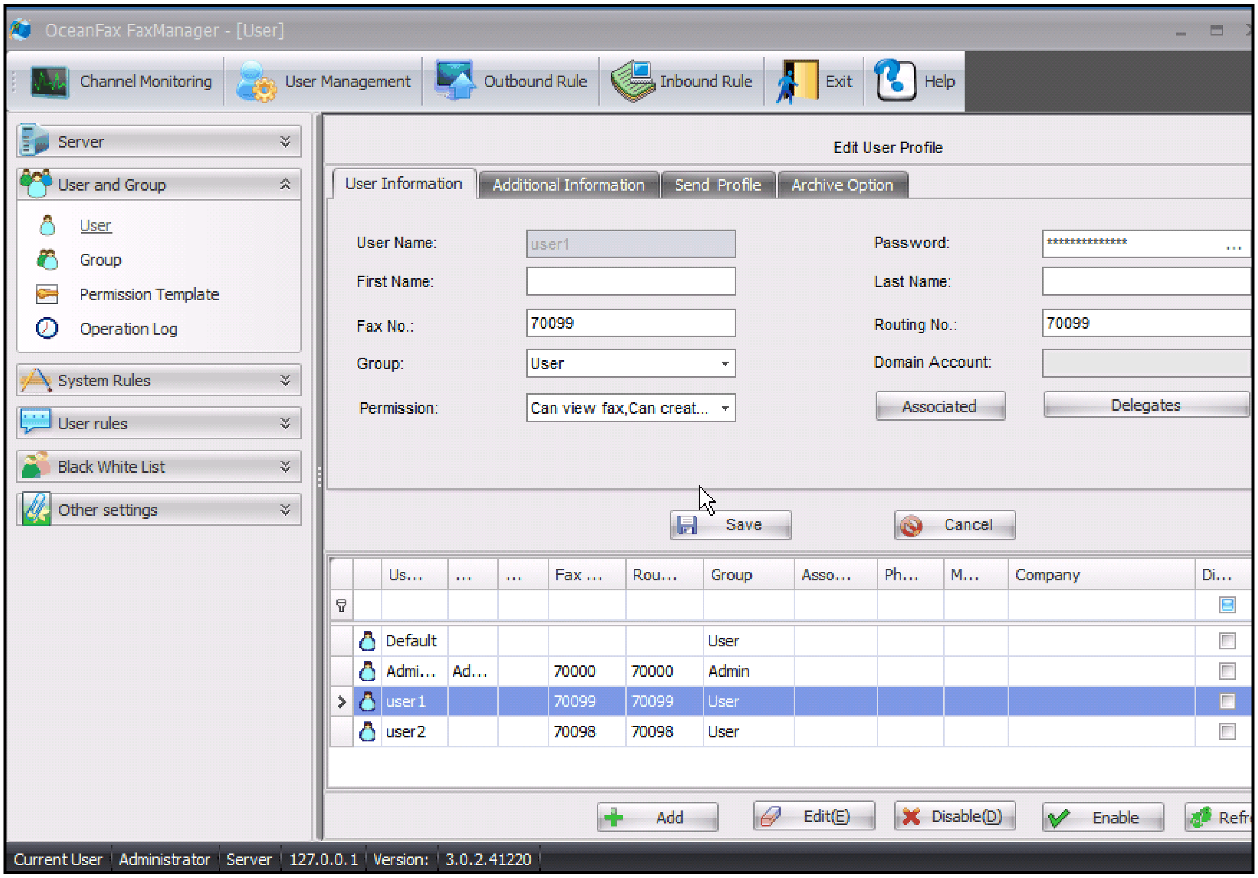


7.3. Adding a user

In order to route calls to OceanFax a number will need to be associated with OceanFax. Login to OceanFax Manager as described in **Section 7.2** above. Select **User and Group** in the left window and under **User and Group** click on **User**. Click on **+Add** at the bottom of the screen highlighted below to add a new user.

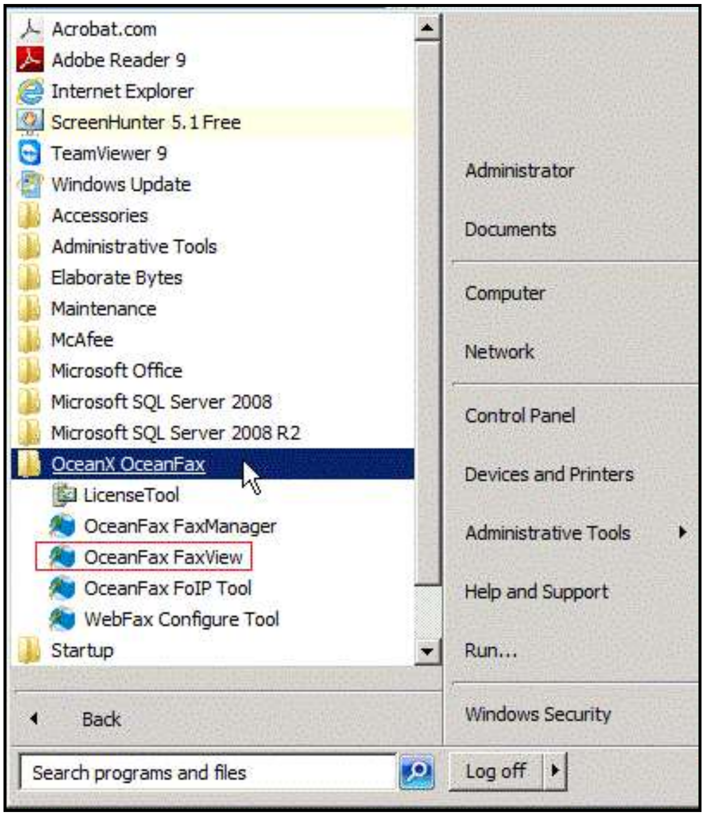


The **User Name** and **Password** entered here will create a user account that allow the user to login and view the faxes that are sent and received. The routing number (**Routing No**) associated with the user is the number used to send faxes to the user.



8. Verification Steps

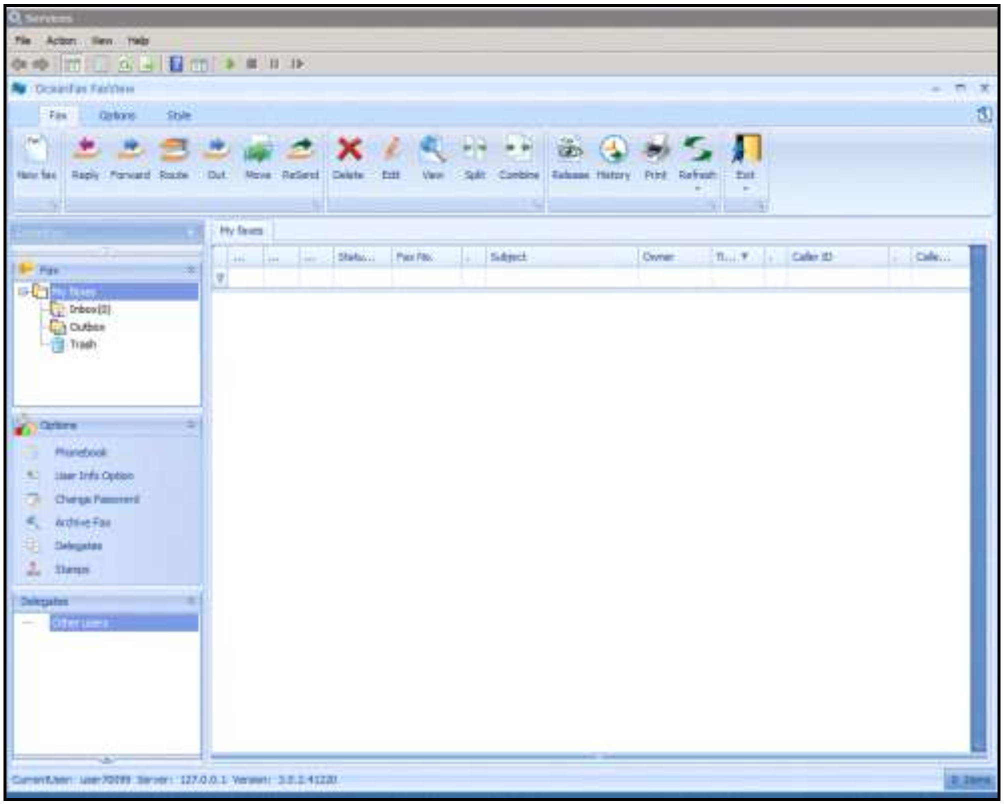
The following steps can be taken to ensure that faxes can be sent to and from the OceanFax. Click on **Start→OceanX OceanFax→OceanFax FaxView**.



Enter the proper credentials for the required user and click on **LOGIN**.

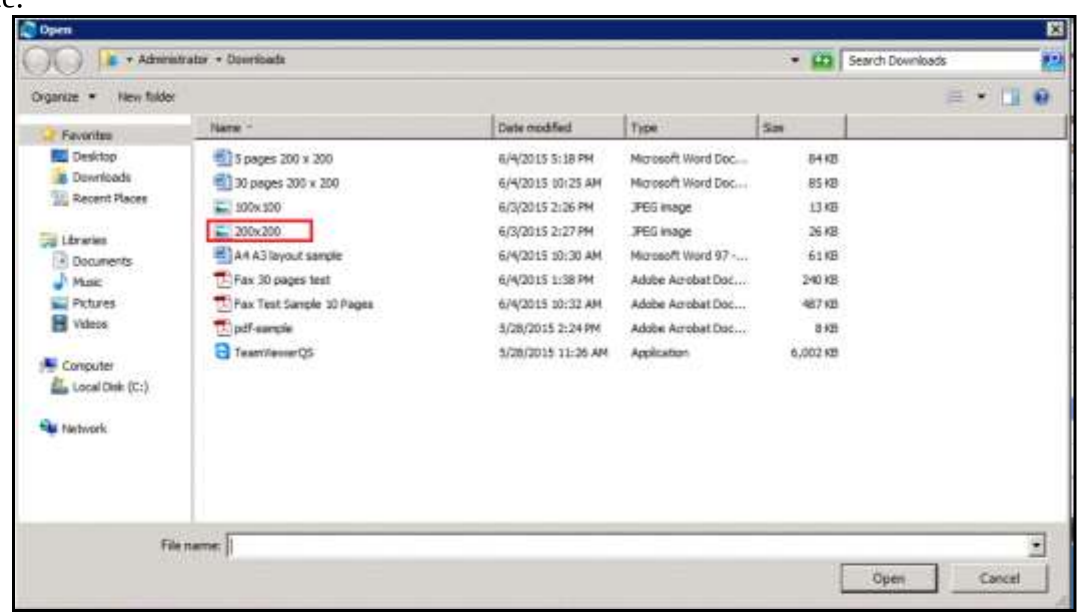
8.1. Sending a FAX

Click on **New Fax** in the top left corner.

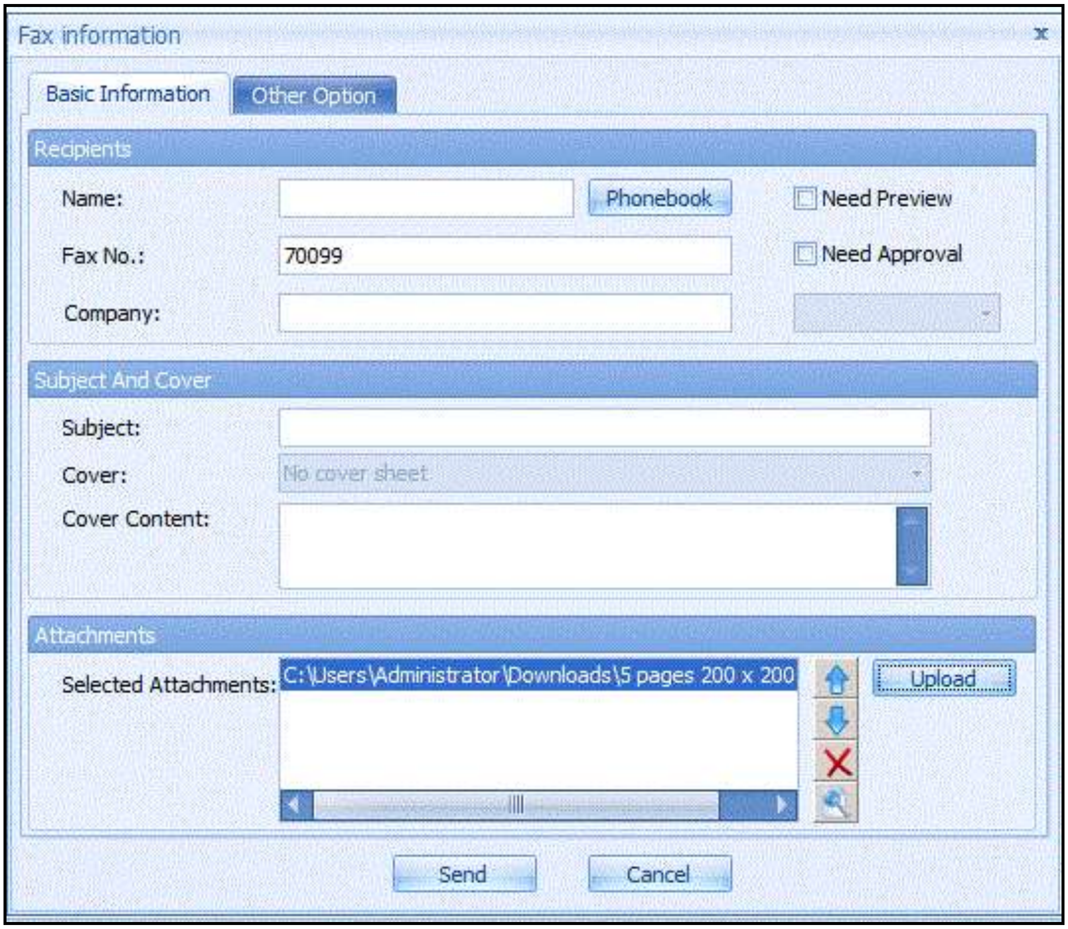


Enter the **Fax No**. of the fax that is to receive the fax message and select **Upload** to add the fax to be sent.

Browse to the location and select the fax message to be sent and click on **Open**. Note that Microsoft Office and Adobe Acrobat Reader is required to be installed if OceanFax is to support conversion of MS Office and PDF attachments respectively by the OceanFax Conversion Service.

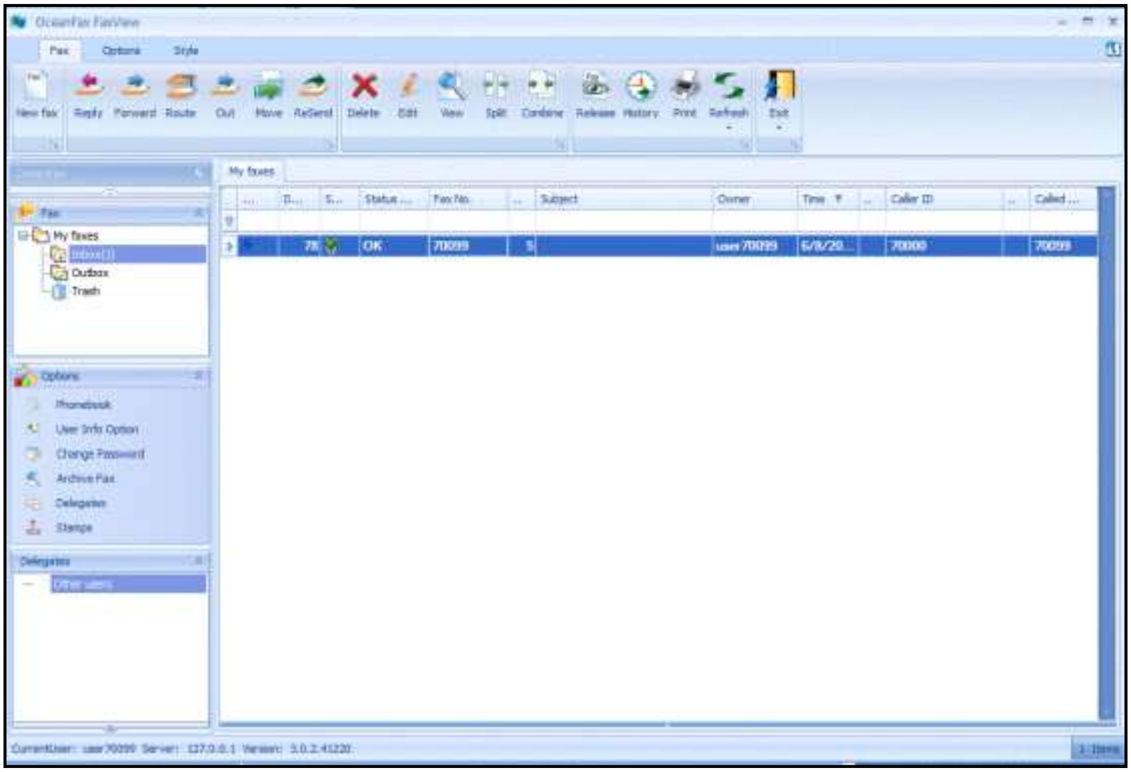


Once the fax message has been added, click on **Send** to send the fax message.



8.2. Receiving a fax

A received fax message can be found in the inbox as shown below. In order to view the fax message, double-click on the required message (not shown).



9. Conclusion

These Application Notes describe the configuration steps required for OceanFax to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 by registering the OceanFax Server as a SIP Entity on Avaya Aura® Session Manager. Please refer to **Section 2.2** for test results and observations.

10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com where the following documents can be obtained.

[1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Issue 10, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, Dec 2014, Issue 14, Document ID 555-245-205

[3] *Deploying Avaya Aura® Session Manager*, Release 6.3, Nov 2014, Issue 6

[4] *Administering Avaya Aura® Session Manager*, Release 6.3, Jun 2014, Issue 5, Doc ID 03-603324

[5] *Application Notes & Test Requirements for T.38 Fax Interoperability* Wwhite Paper, May 2013, Issue 1.1

The OceanFax product documentation can be obtained from the OceanX.

[6] *OceanFax Administrator's Guide*,1st Aug 2014

[7] *OceanFax Installation Guide*,1st Aug 2014

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.