Avaya Solution & Interoperability Test Lab

Application Notes for Configuring OceanFax from OceanX Technology Limited with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 – Issue 1.0

Abstract

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

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 from OceanX Technology Limited with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2. The solution from OceanX consists of a fax server called Brooktrout configured as a SIP endpoint on Session Manager.

2. General Test Approach and Test Results

The OceanFax Brooktrout Server is registered with Session Manager as a SIP entity and has an internal fax number of 4400; this means that calls to 4400 are directed to the OceanFax Server. In order to test internal fax calls to and from the OceanFax server faxes are sent in on one channel and out on another channel. In order to test a fax call to the PSTN another fax machine configured on a secondary Communication Manager is used.. The OceanFax Brooktrout supports UDP/SIP Trunk/T.38 and T.30 over G711.

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. When sending "internal faxes", a fax is sent out on one channel and received on another channel using the same Fax Server. When sending PSTN faxes a simulated PSTN is used to another Communication Manager which had another fax machine connected on an analog port.

- Internal Fax calls
- Fax calls sent to PSTN
- Fax calls received from PSTN
- Verification of correct status and Caller ID for sent and received fax messages
- Successful transmission and receipt of a thirty page fax to PSTN
- Successful recovery from network and power failure

2.2. Test Results

All test cases passed successfully except the following:

- When using an internal Avaya extension to transfer a Fax call to/from the OceanFax server the fax transmission failed.
- It was observed that if there was a break in transmission when receiving a fax document the partially received document was totally discarded by the OceanFax server.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for OceanFax can be obtained from the following location:

OceanX LTD
www.oceanfax.com
support@oceanfax.com

3. Reference Configuration

Figure 1 shows the reference configuration used for this compliance testing. In order to send a fax to the OceanFax Server and receive a fax from the OceanFax server a PC with a modem running Windows Fax from Windows XP is connected to an analog port of a Communication Manager R6.0.1. The OceanFax Brooktrout server running on a Windows 2008 R2 virtual server is registered as a SIP endpoint on Session Manager R6.2 connecting to Communication Manager R6.2. These two faxes are setup to simulate fax machines on two different sites.

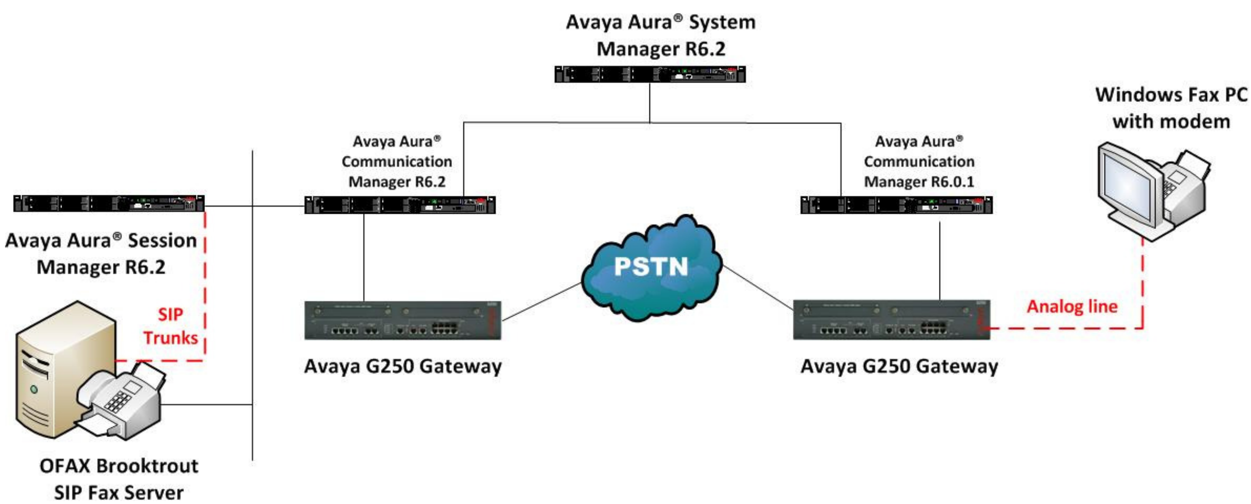


Figure 1: Network Solution of OceanFax Brooktrout Server with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4 (6.2.0.0.15669)
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP4 (R016x.02.0.823.0-20199)
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP3 (6.2.3.0.623006)
Avaya G250 Media Gateway	R6.2
Windows Fax Machine	Windows XP SP3 FAX
OceanFax server with Brooktrout SR140 for FOIP (Fax Over IP) running on Windows 2008 Virtual Server R2	R3.1
To simulate PSTN call Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.0.1

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 required 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
- Administer Route Selection for OceanFax calls

Note: The configuration of the PRI interface to the PSTN is outside the scope of these Application Notes.

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 or 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 250
           Maximum Concurrently Registered IP Stations: 18000 2
             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: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 3**, ensure that **ARS** is 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? y                       DCS (Basic)? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** is 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? n
                                             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
```

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. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). Refer to **Section 10** for supporting documentation.

```
display system-parameters features                            Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    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: attd
    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? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. In the example below **5** is used for AAR and **9** for ARS.

```
display feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: *24
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 5
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
```

5.3. Administer Dial Plan

For the testing, two number ranges were used on Communication Manager. Extensions beginning with **2** and **3** and are four digits in length. The second range is used to deliver and identify calls to OceanFax; this range begins with digits **44**, which are four digits long, and are defined as **udp** in the dial plan.

```
display 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
   2           4   ext
   3           4   ext
   44          4   udp
   5           1   fac
   600         4   ext
   7           3   dac
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

5.4. Configure SIP Trunk

In the **IP NODE NAMES** form, note the IP Address of the **procr** and the Session Manager (**SM100**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager.

```
display node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               192.168.50.16
aes62vmpg           10.10.40.10
default             0.0.0.0
g250-dcp            192.168.50.18
procr               192.168.50.13
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **devcon.avaya**. 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 Session manager as **ip-network region 1** is specified in the SIP signalling group.

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

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to OceanFax. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 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), which are supported by OceanFax.

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

                          IP Codec Set

    Codec Set: 1

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

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

- Enter the command **change signalling group** x where x is the signalling group present for SIP
- 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 **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect the peer server as Session Manager (**SM**)
- Set the **Near-end Node Name** to **procr** as shown **IP NODE NAMES** form above
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM100**)
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the far-end for calls using this signaling group in network region 1
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain
- 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 **Direct IP-IP Audio Connections** field is set to **y**
- The default values for the other fields may be used

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM100
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain:
                                             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? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from OceanFax. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the 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, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP TRK                    COR: 1        TN: 1        TAC: *11
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with OceanFax to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

```
change trunk-group 1                                            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): 600

 Disconnect Supervision - In? y  Out? y


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

5.5. Administer Route Selection for OceanFax Calls

As digits 44xx were defined in the dial plan as udp (**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 **44** that are **4** digits in length will be matched. No digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 4                                          Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                 Percent Full: 0

  Matching                    Insert              Node
  Pattern        Len Del      Digits       Net Conv Num
  44              4   0                    aar  n
```

Use the **change aar analysis** command to further configure the routing of the dialed digits. Calls to OceanFax begin with **44** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 44                                              Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed                  Total      Route     Call   Node   ANI
    String                 Min  Max  Pattern     Type   Num    Reqd
    44                     4    4     1          unku          n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**.

```
change route-pattern 1                                              Page   1 of   3
                    Pattern Number: 1   Pattern Name: SIPTRK
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    0                                                               n   user
 2:                                                                      n   user
 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            unre                                       none
 2: y y y y y n  n            rest                                       none
 3: y y y y y n  n            rest                                       none
 4: y y y y y n  n            rest                                       none
 5: y y y y y n  n            rest                                       none
 6: y y y y y n  n            rest                                       none
 6: 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:

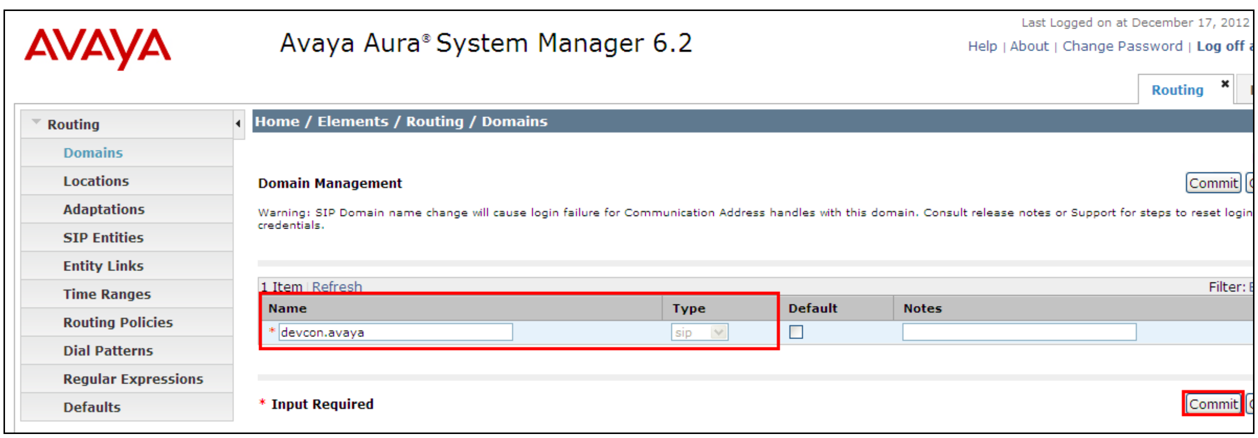
- Log in to Avaya Aura® Session Manager
- Administer SIP Domain
- Administer Location
- Administer SIP Entities
- Administer Routing Policies
- Administer Dial Patterns

6.1. Log in to Avaya Aura® System Manager

Access the 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).

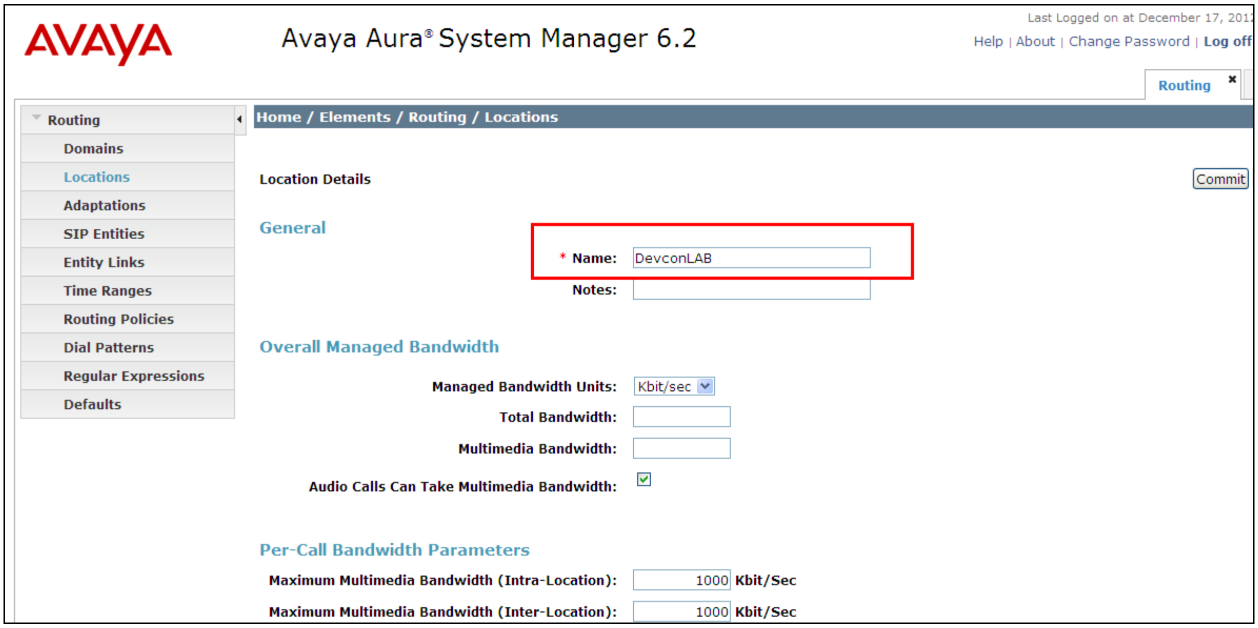
6.2. Administer SIP Domain

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

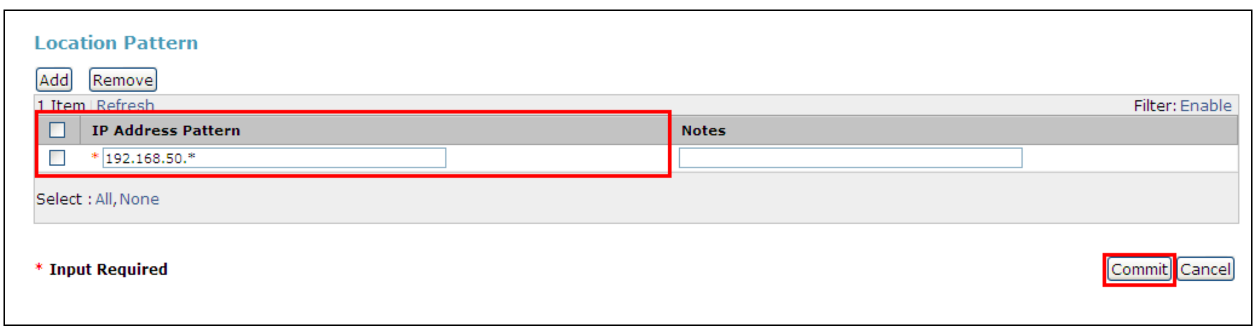


6.3. Administer Location

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 location and the 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 **192.168.50.*** as shown below. Click **Commit** when done.

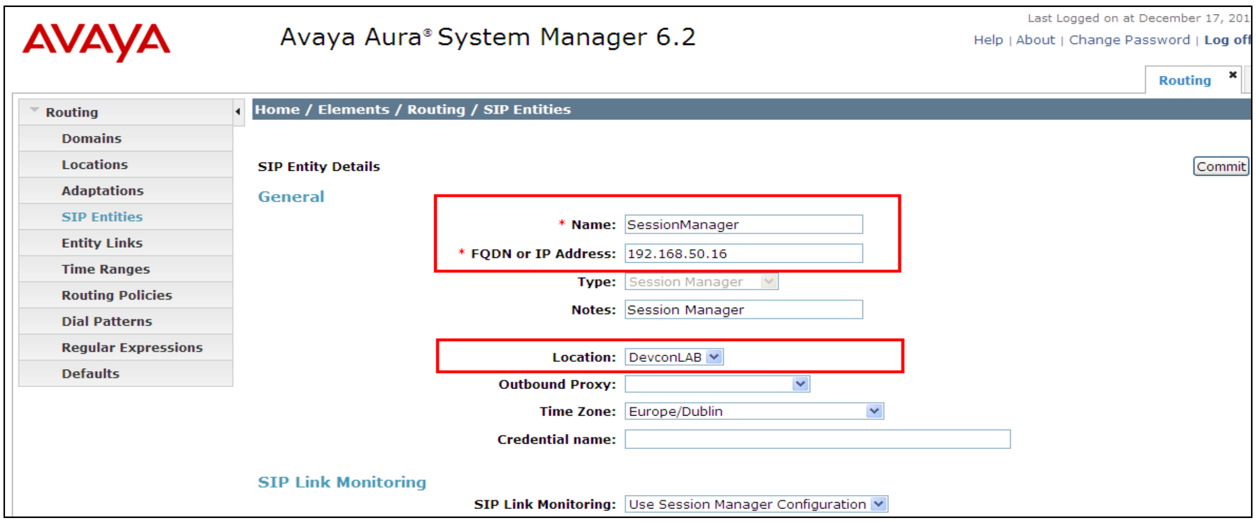


6.4. Administer SIP Entities

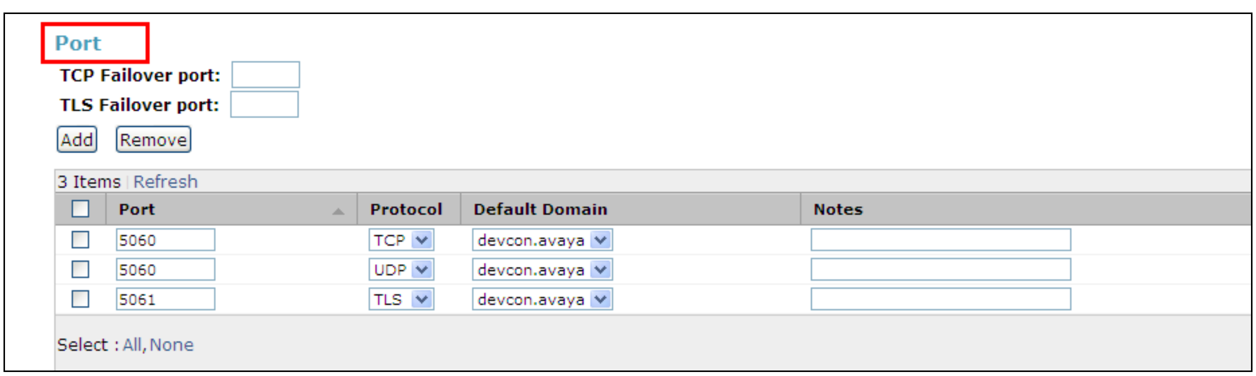
Each SIP device (other than Avaya SIP Phones) that communicates with Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for Session Manager SIP Signaling Interface, Communication Manager and OpenGate Solution respectively.

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.**

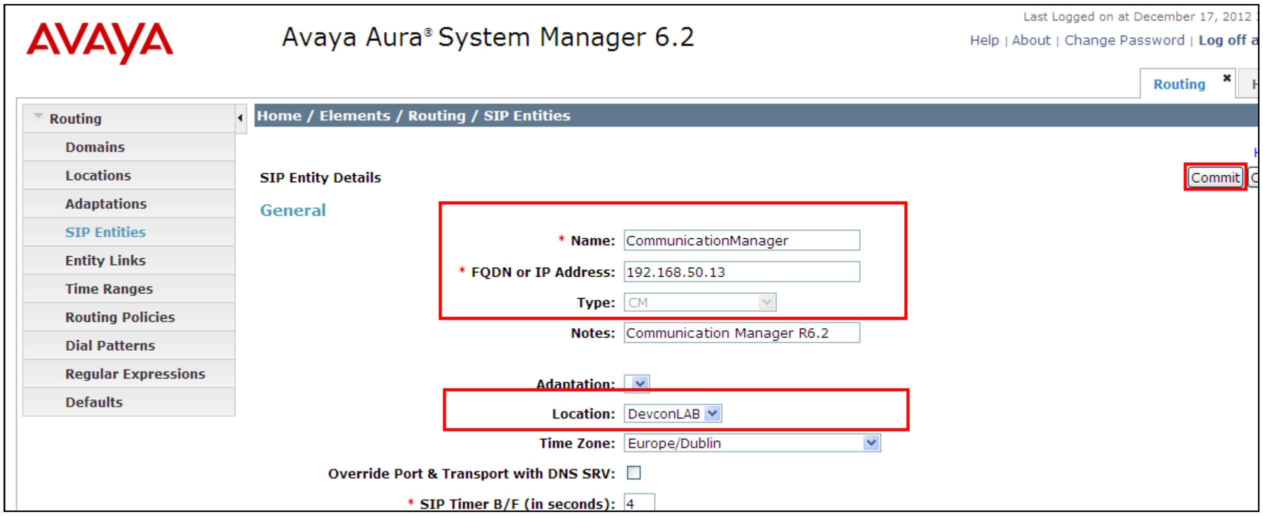


Tick the box next to the entity that was just created and click **Edit** (not shown)**.** Scroll down the page until the **Port** section is displayed, click **Add** and configure the **Port** as **5060** the **Protocol TCP** and the **Default Domain** as the domain configured in **Section 6.2**. This corresponds to the signaling group domain configured in **Section 5.4.** Repeat this for the **UDP** connection which will be established to the OceanFax server, as shown below. Click **Commit** when done.



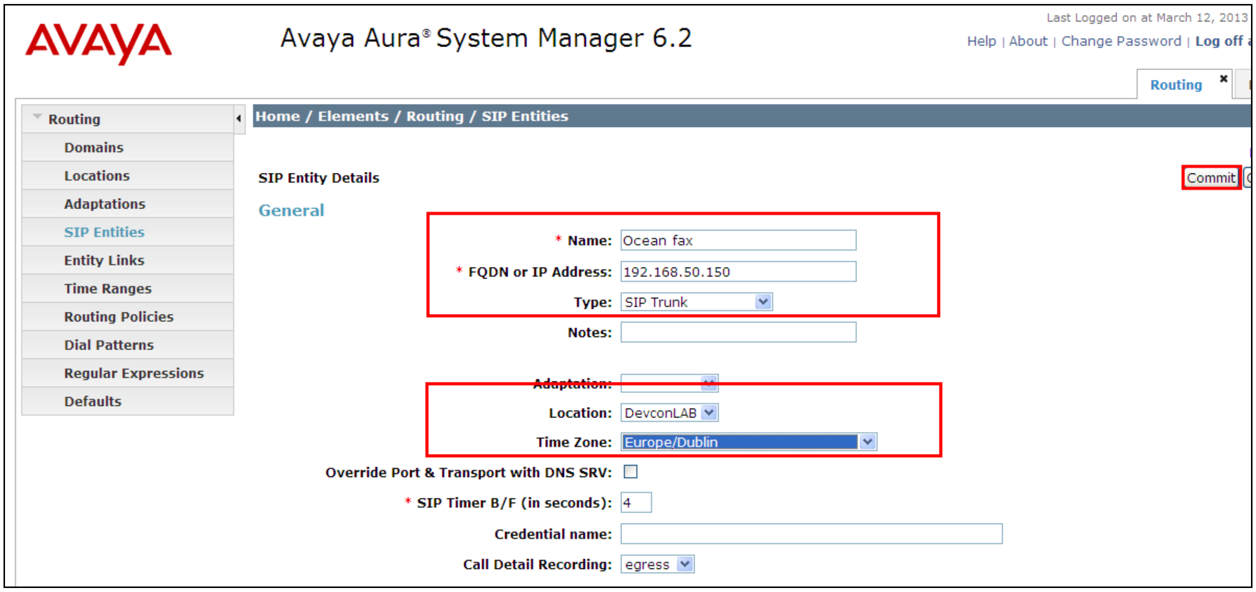
6.5. Configure Avaya Aura® Communication Manager Entity

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



6.6. 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 server, set the **Type** to **SIP Trunk**, leave all other settings default and click **Commit**.

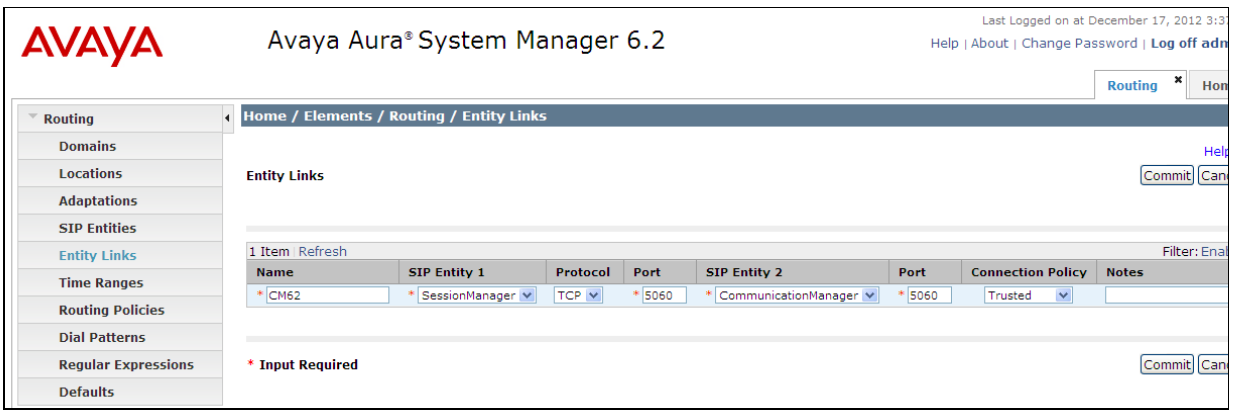


6.7. Administer SIP Entity Link

A SIP Trunk between a 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.

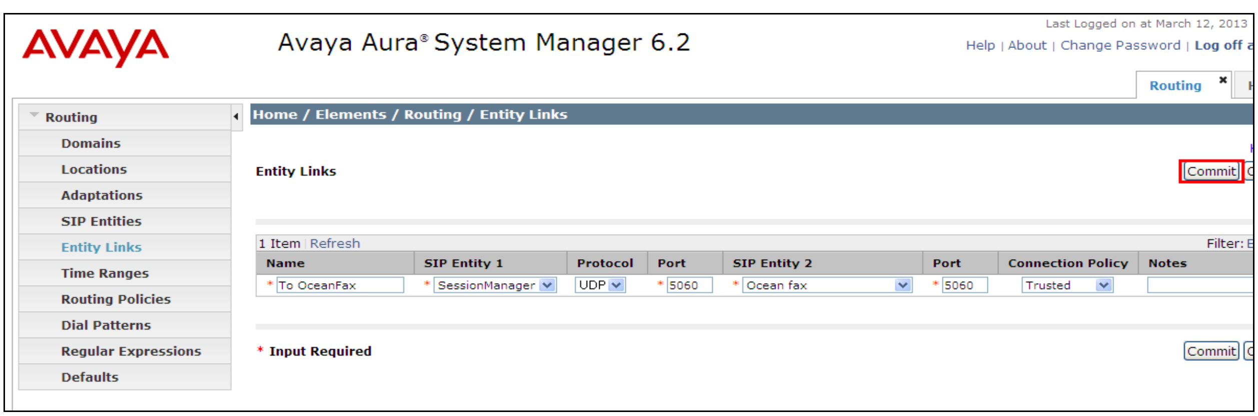
6.7.1. Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Aura® Communication Manager

Click on **Home → Elements → Routing → Entity Links → New** (not shown). Assign an identifying **Name** choose the entity assigned to the Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **TCP**, enter **5060** for the **Port**, choose the Communication Manager entity as **SIP Entity 2** and set the **Port** to **5060**, ensure **Trusted** is selected for the Connection Policy. Click **Commit** when done.



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

Click on **Home → Elements → Routing → Entity Links → New** assign an identifying **Name**. Choose the entity assigned to the 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** when done. This establishes the Session Manager end of the SIP Trunk to OceanFax.

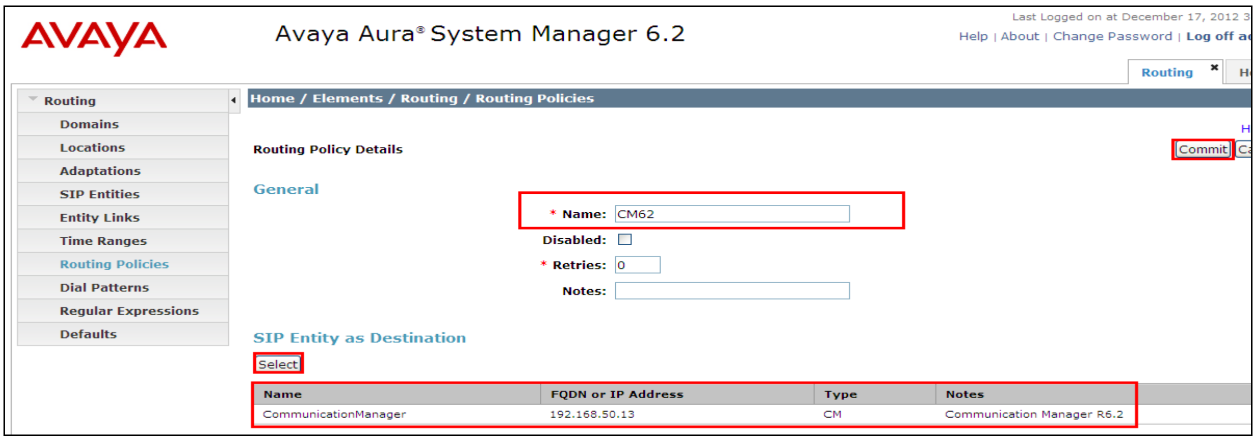


6.8. Administer Routing Policies

To complete the routing configuration, a Routing Policy is created. Routing policies direct how calls will be routed to a SIP Entity. Two routing policies must be created, one for the Communications Manager and the second for OceanFax. These will be associated with the Dial Patterns created in **Section 6.9**.

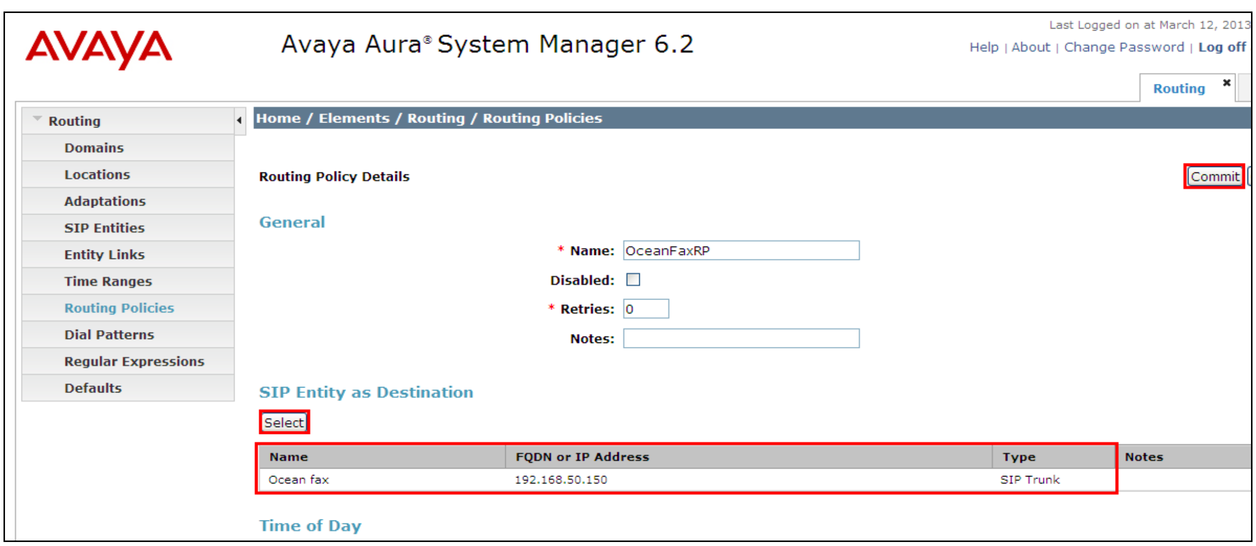
6.8.1. Create Routing Policy to Avaya Aura® Communication Manager

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



6.8.2. Create Routing Policy to OceanFax

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

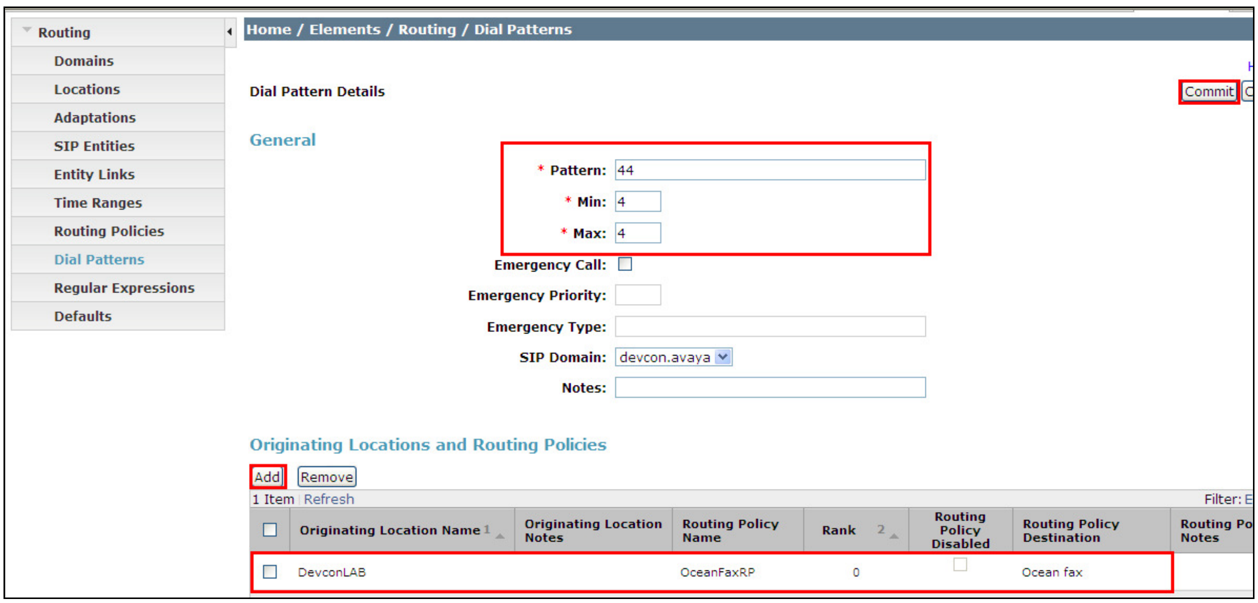


6.9. Administer Dial Patterns

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.

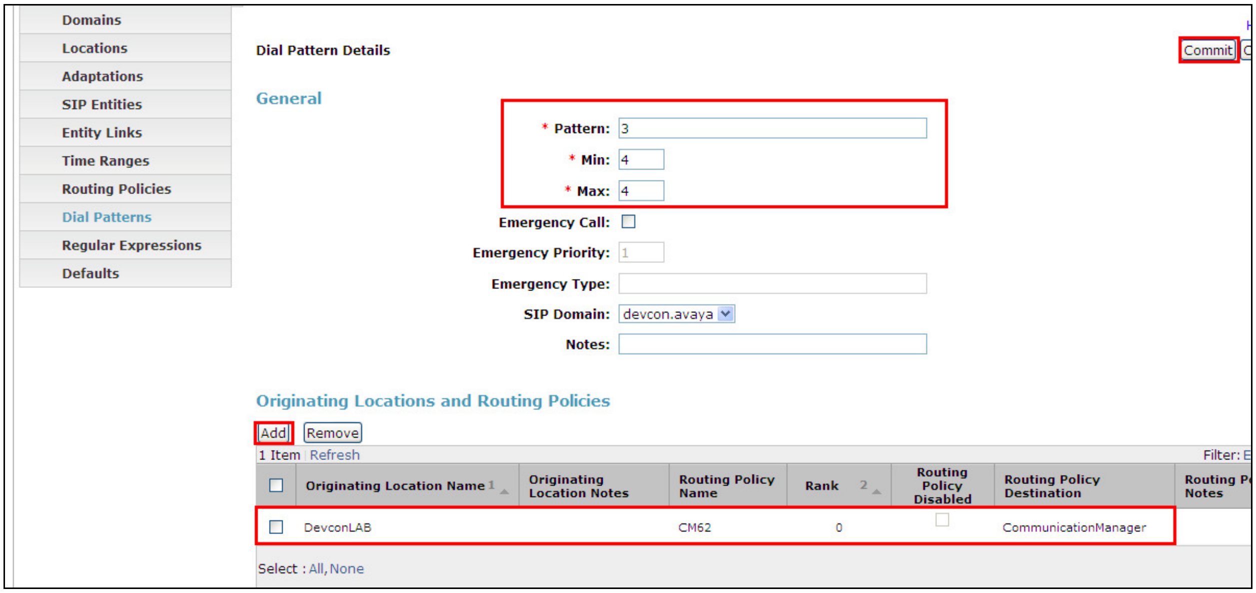
6.9.1. Create Dial Pattern to OceanFax

In **Section 5.5** Communication Manager is configured to route the dialed numbers beginning **44**xx to Session Manager. To create a Dial Pattern to route **44**xx from Session Manager to OceanFax click **Home → Elements → Routing → Dial Patterns →New** (not shown). Under **Pattern** enter the numbers presented to Session Manager by Communication Manager destined for OceanFax in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**. In the **Origination Location** section select the domain created in **Section 6.2** above in the **Routing Policies** section click the routing policy created for OceanFax. Click **Select** when done (not shown). Click **Commit** when complete.



6.9.2. Create Dial Pattern to Avaya Aura® Communication Manager

An additional Dial Pattern must be created on Session Manager to route incoming calls from OpenGate to Communication Manager stations 3xxx. To create a Dial Pattern to route 3xxx from Session Manager to Communication Manager, click **Home → Elements → Routing → Dial Patterns →New** (not shown). Under **Pattern** enter the numbers presented to Session Manager by OpenGate destined for Communication Manager, in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to that which was created in **Section 6.2**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**. A new window opens, (not shown)**,** in the **Origination Section**, select the domain name created in **Section 6.2** above. In the **Routing Policies** section click the routing policy created for Communication Manager. Click **Select** when done (not shown). Click **Commit** when finished.



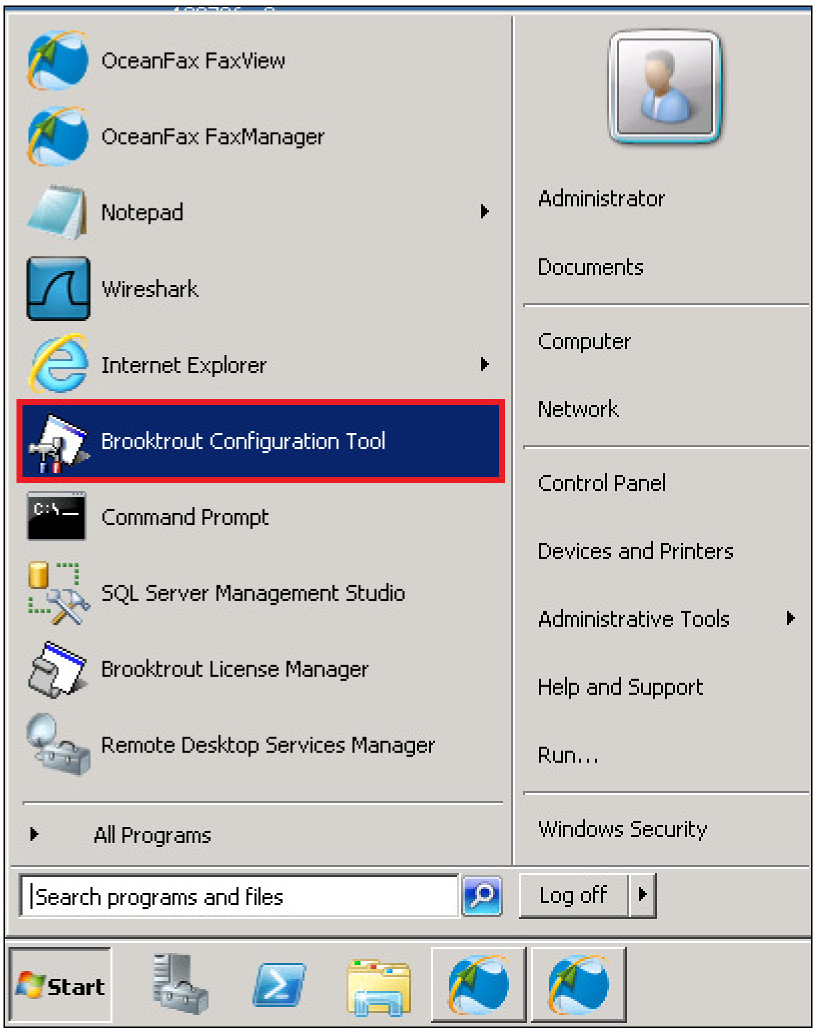
7. Configure OceanFax Server

The configuration of OceanFax consists of three separate configurations on the OceanFax server.

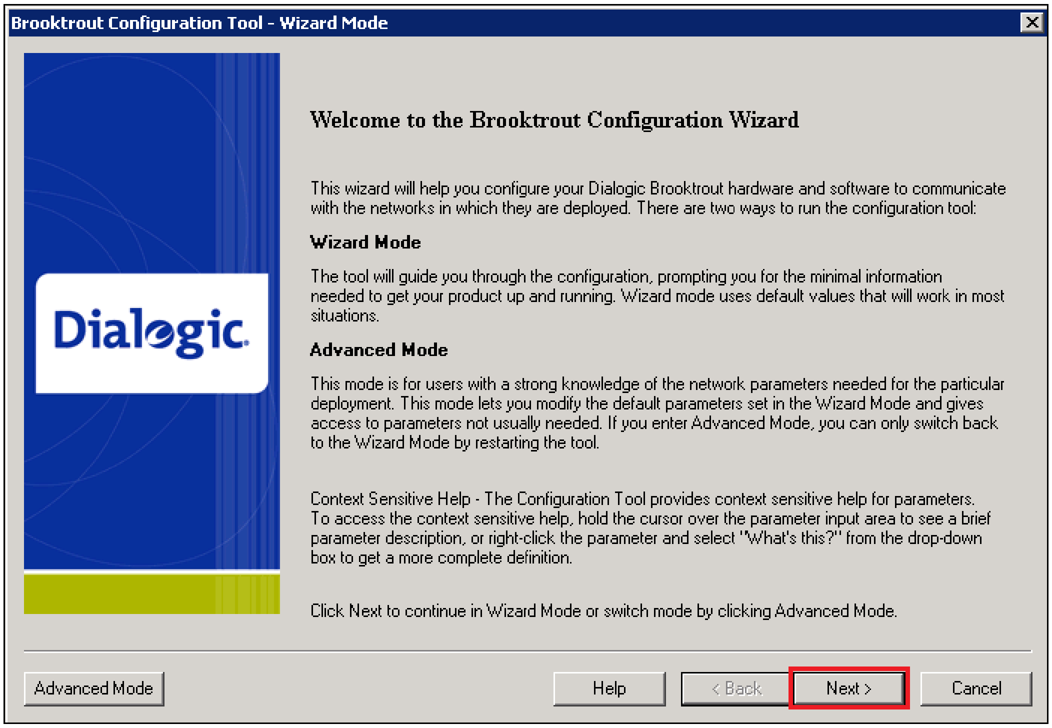
- Brooktrout Configuration Tool
- Create a Dial Rule on OceanFax
- Adding a User

7.1. Brooktrout Configuration Tool

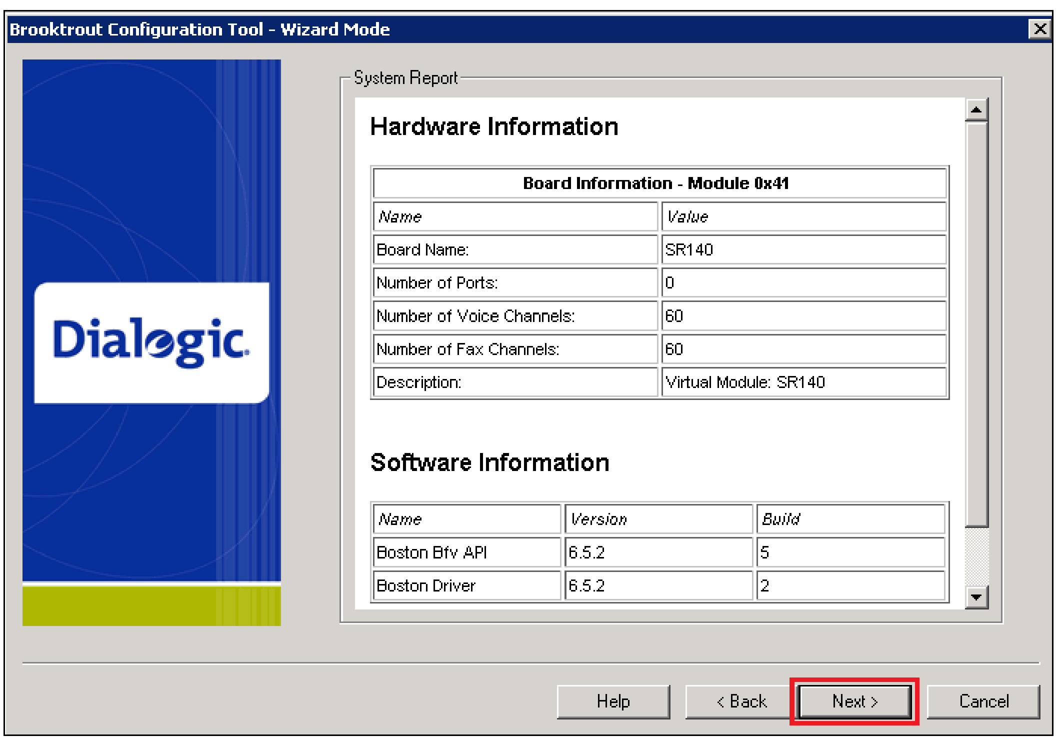
On the OceanFax server, click on **Start → Brooktrout Configuration Tool**.



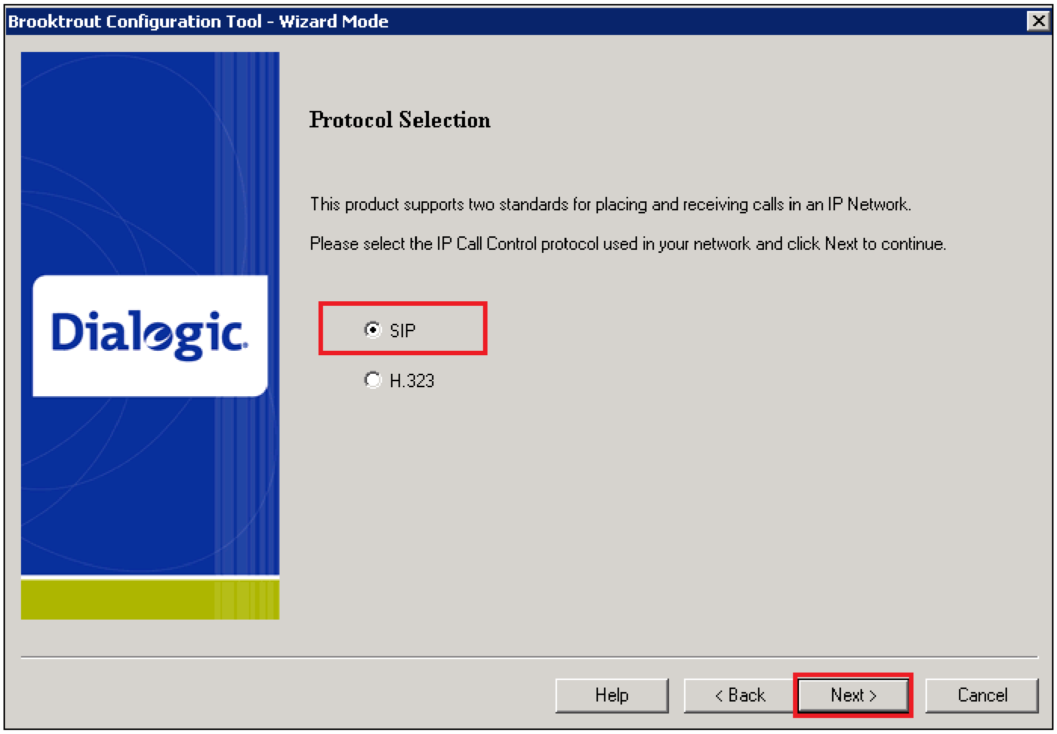
The **Brooktrout Configuration Tool – Wizard Mode** is opened, click on **Next** to continue.



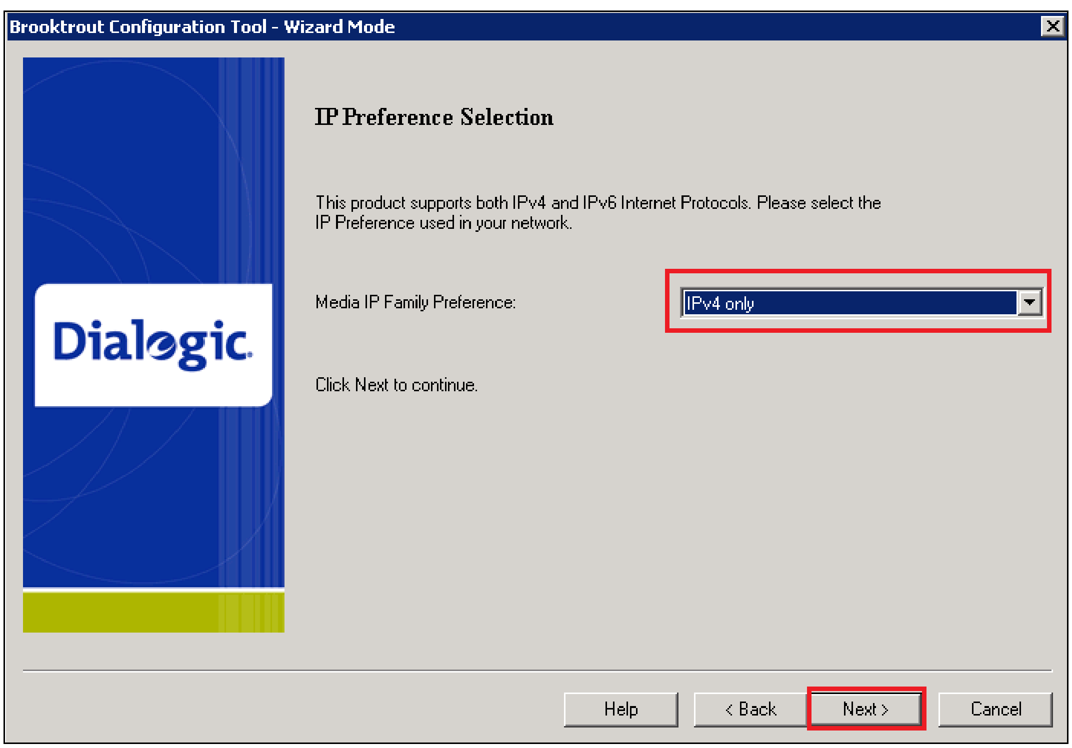
Information on the Hardware and Software is shown, click on **Next** to continue.



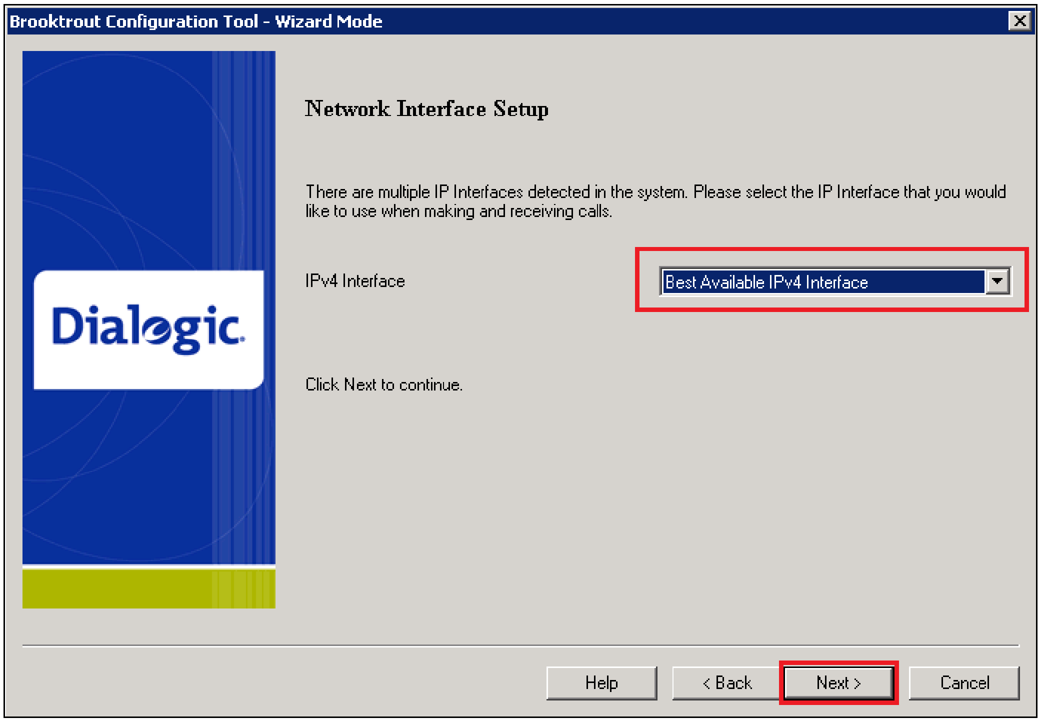
Ensure that **SIP** is selected for the **Protocol Selection**, click **Next** to continue.



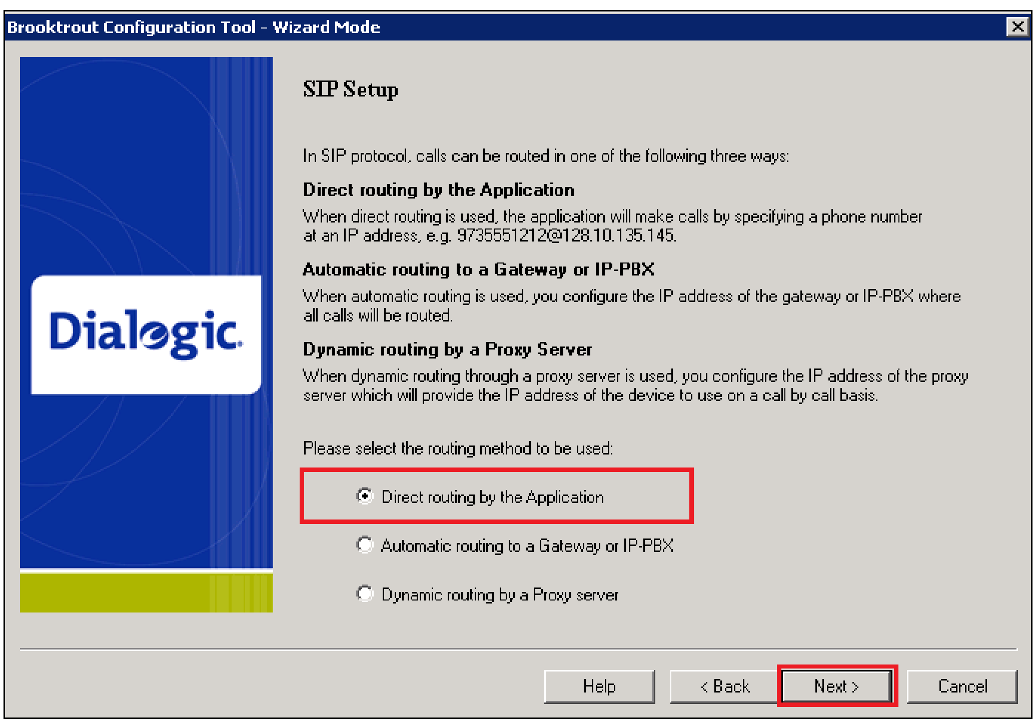
Select **IPv4 only** for the **Media IP Family Preference** and click on **Next**.



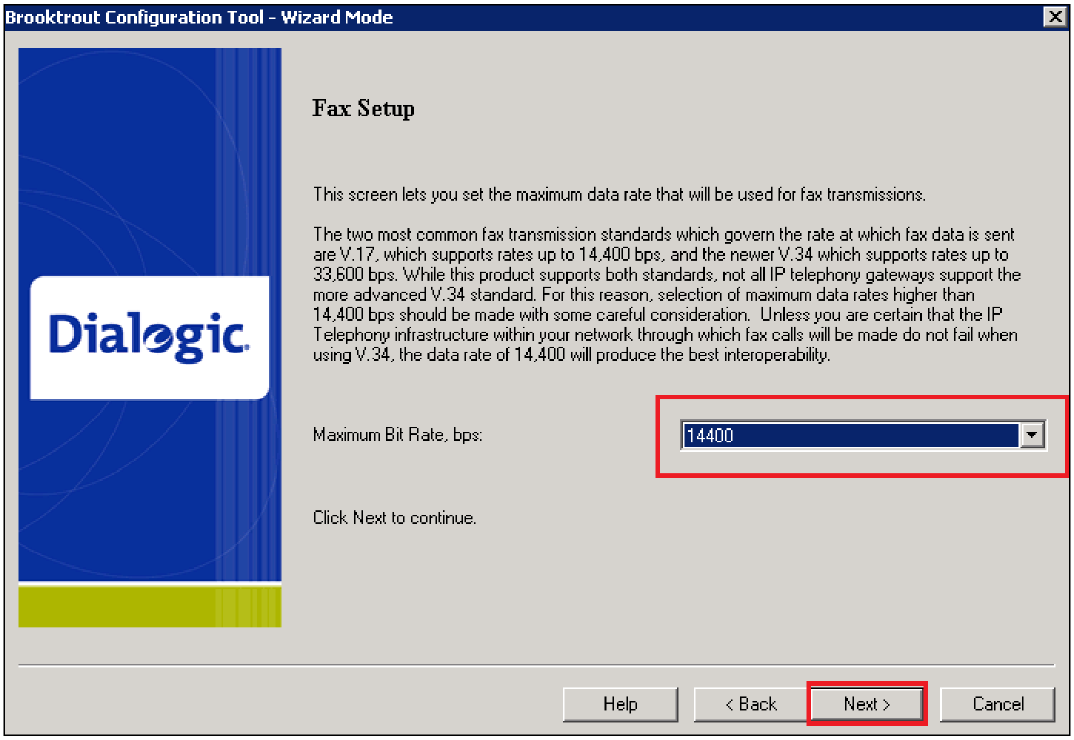
Select **Best Available IP4 Interface** and click on **Next**.



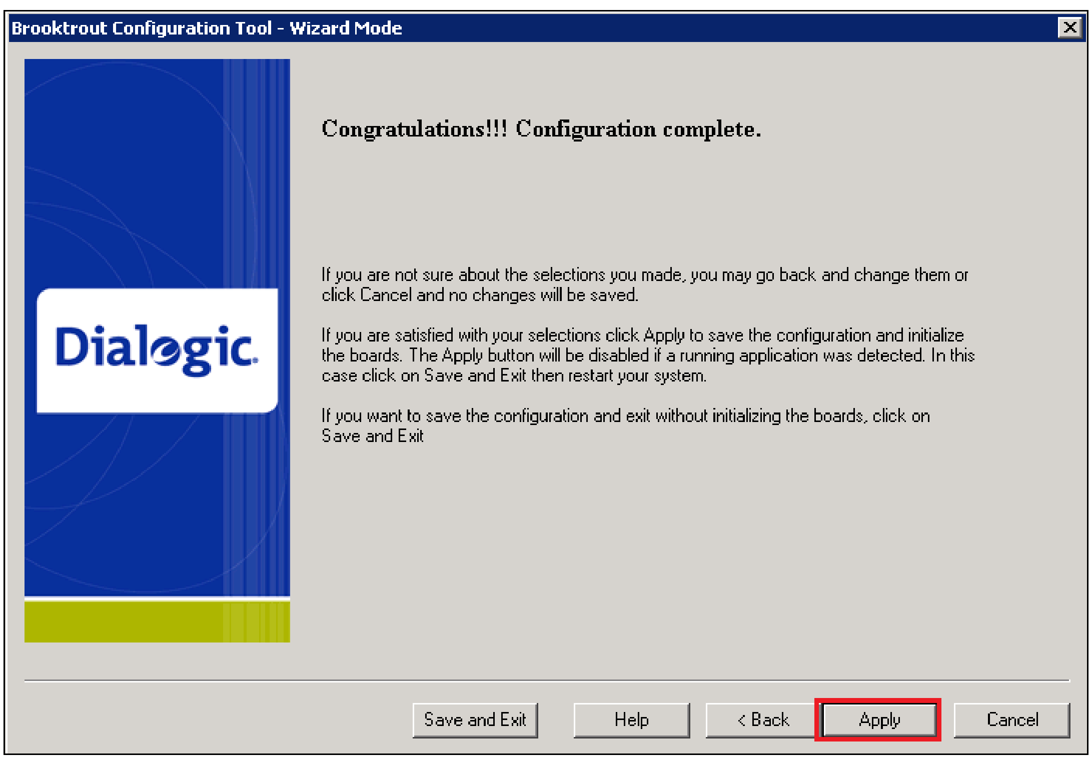
For the **routing method** select **Direct routing by the Application**, click on **Next** to continue.



Choose **14400** for the **Maximum Bit Rate, bps**, then click on **Next**.

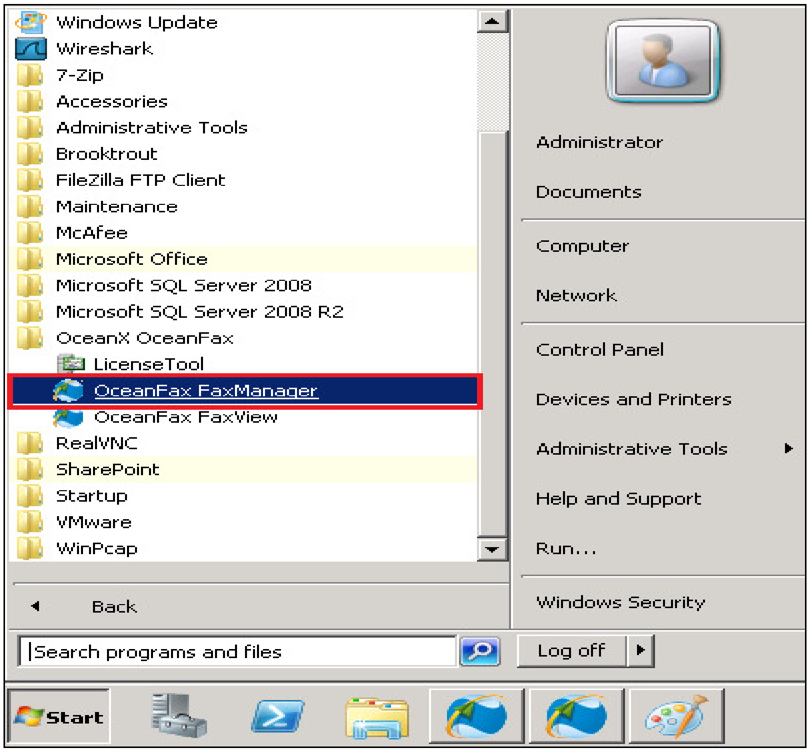


Click on **Apply** and then **Save and Exit** to finish the setup.

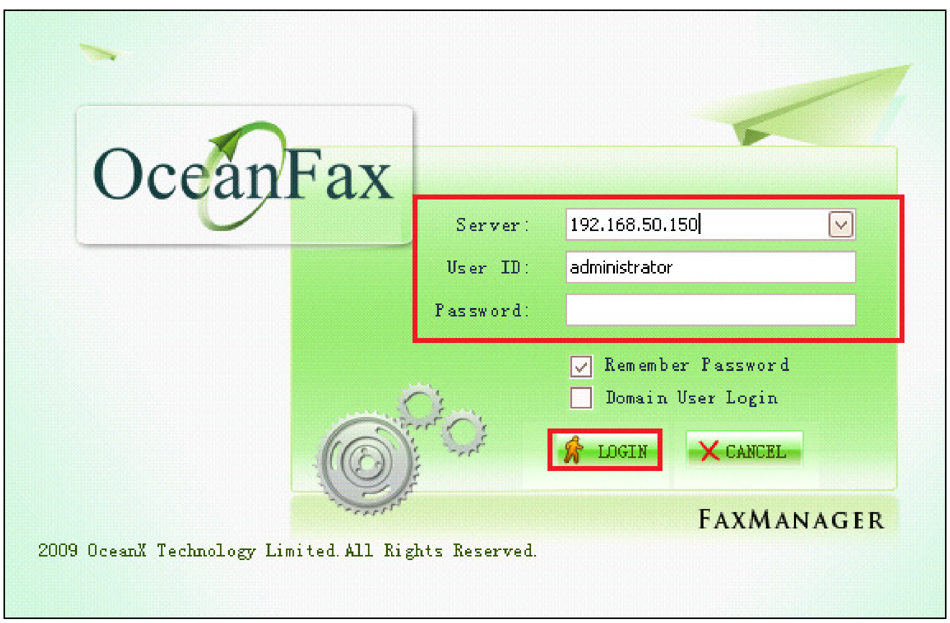


7.2. Create a Dial Rule on OceanFax

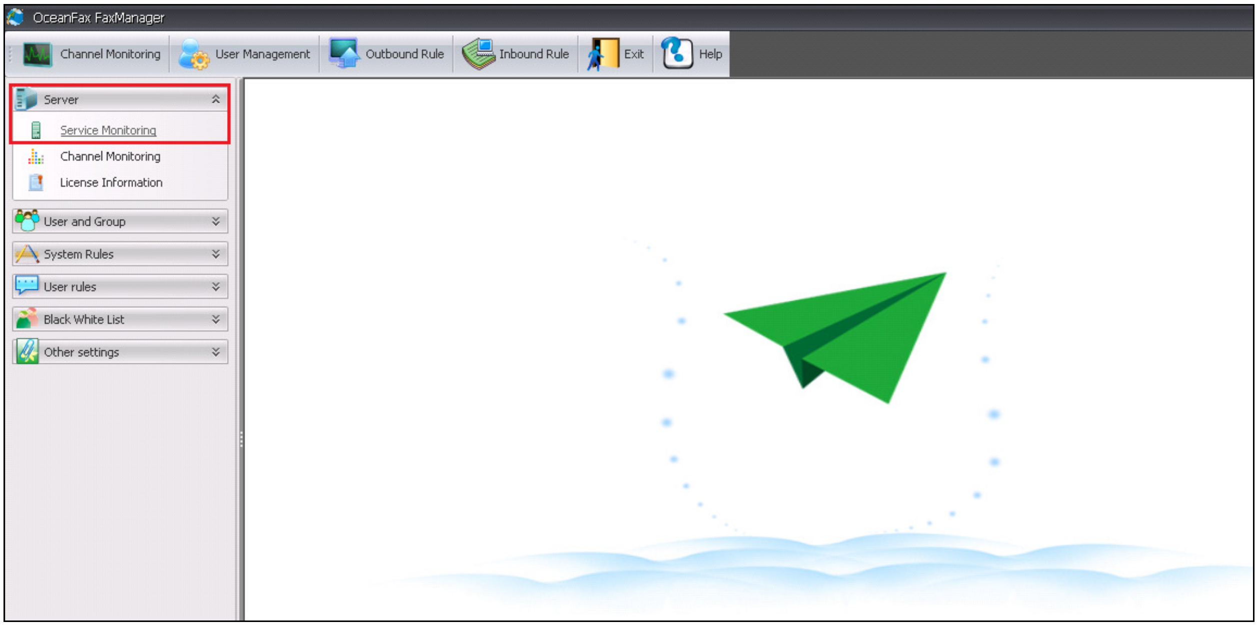
Click on **Start→Programs→OceanX OceanFax→OceanFax FaxManager**



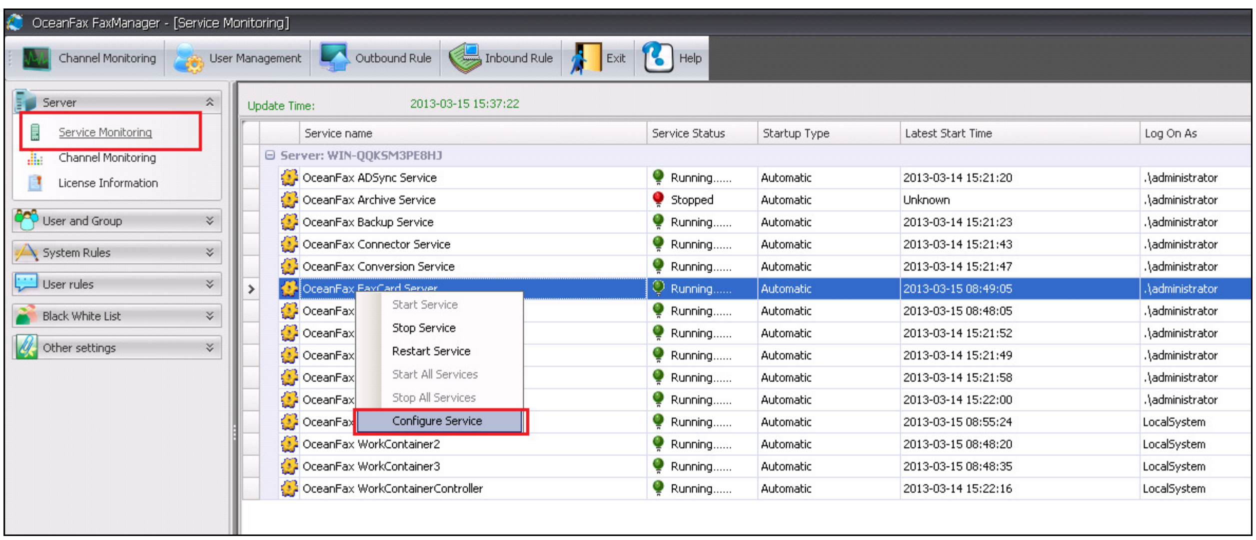
Enter the proper credentials then click on **LOGIN**.



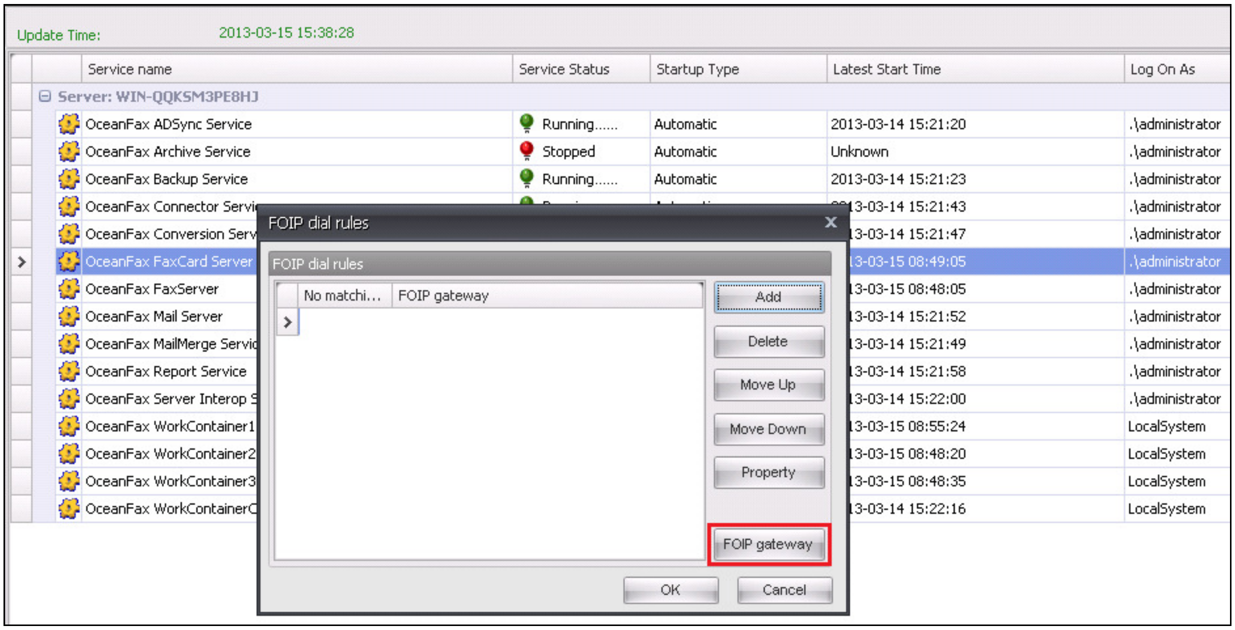
In the left window select **Server→Service Monitoring**,



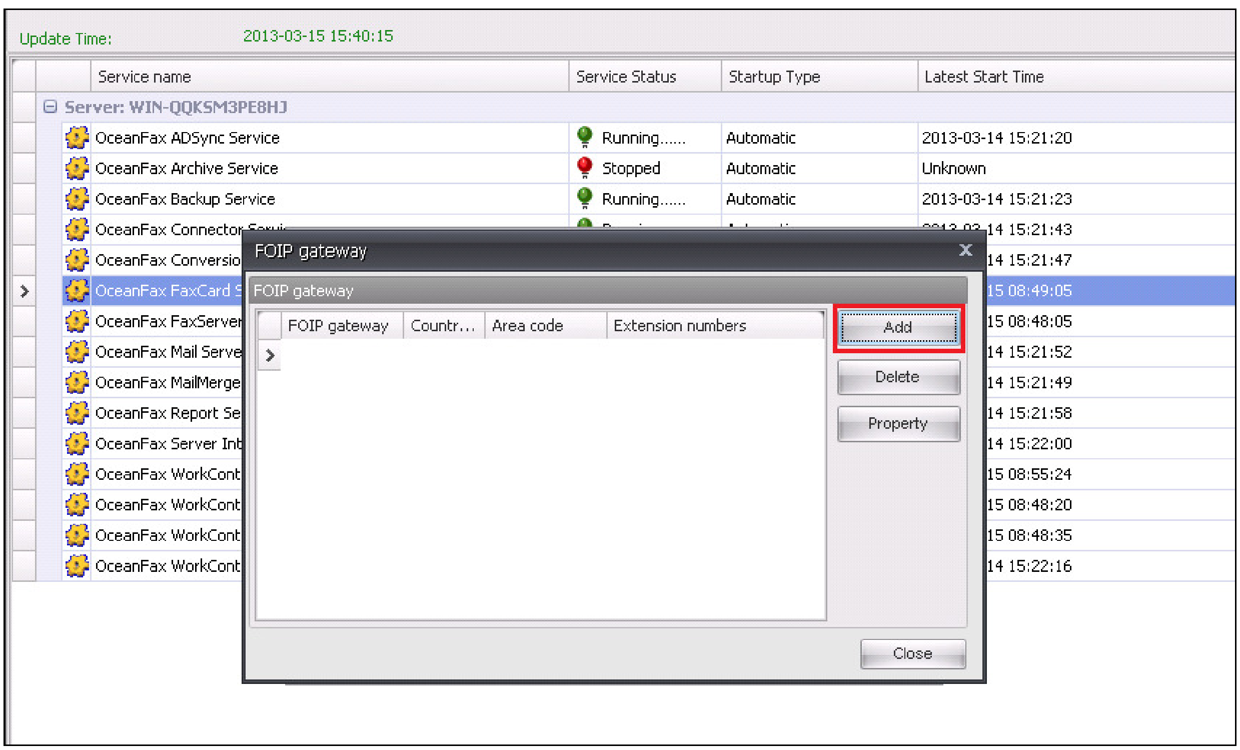
A list of services opens in the main window. Highlight **OceanFax FaxCard Server** and right click on this. Select **Configure Service** as is shown below.



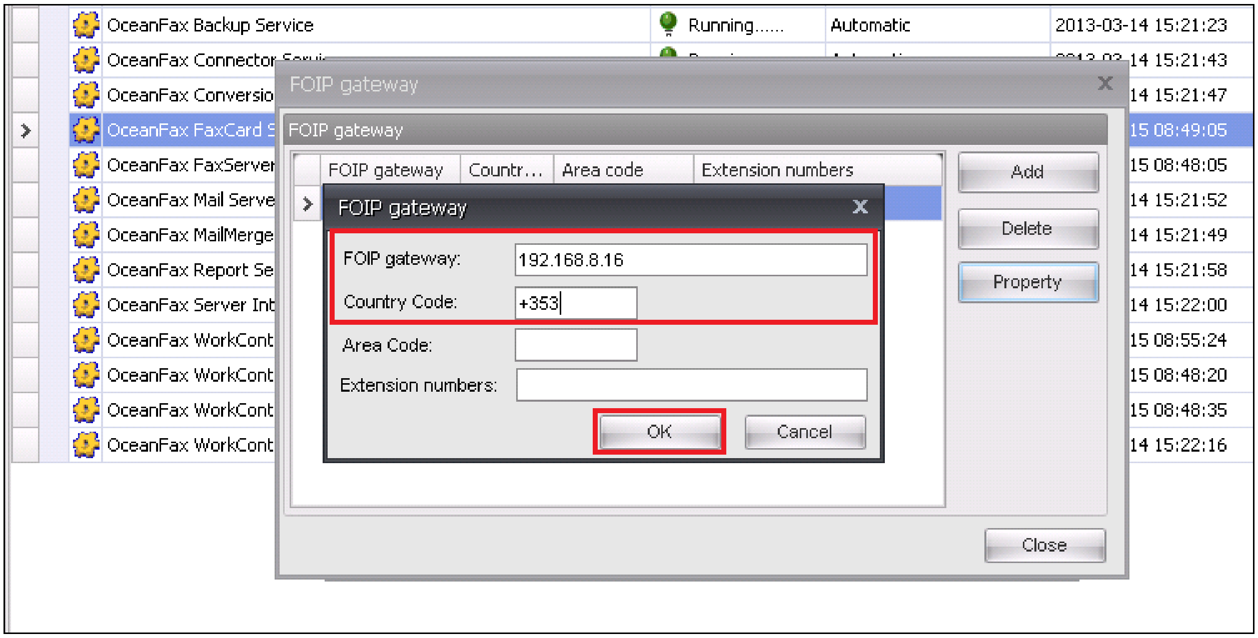
A new window is opened for the **FOIP dial rules**. Click on **FOIP gateway** at the bottom right of this window.



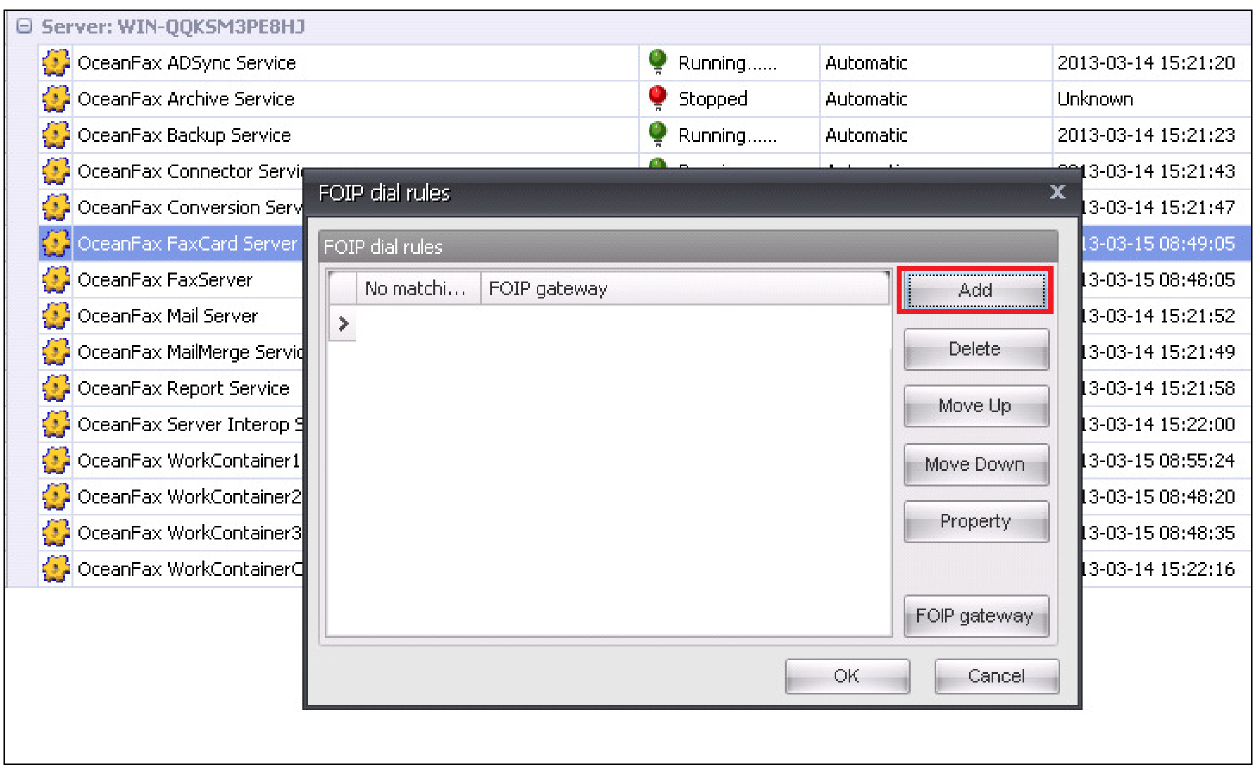
The **FOIP gateway** window is opened, click on **Add** at the top right of the window.



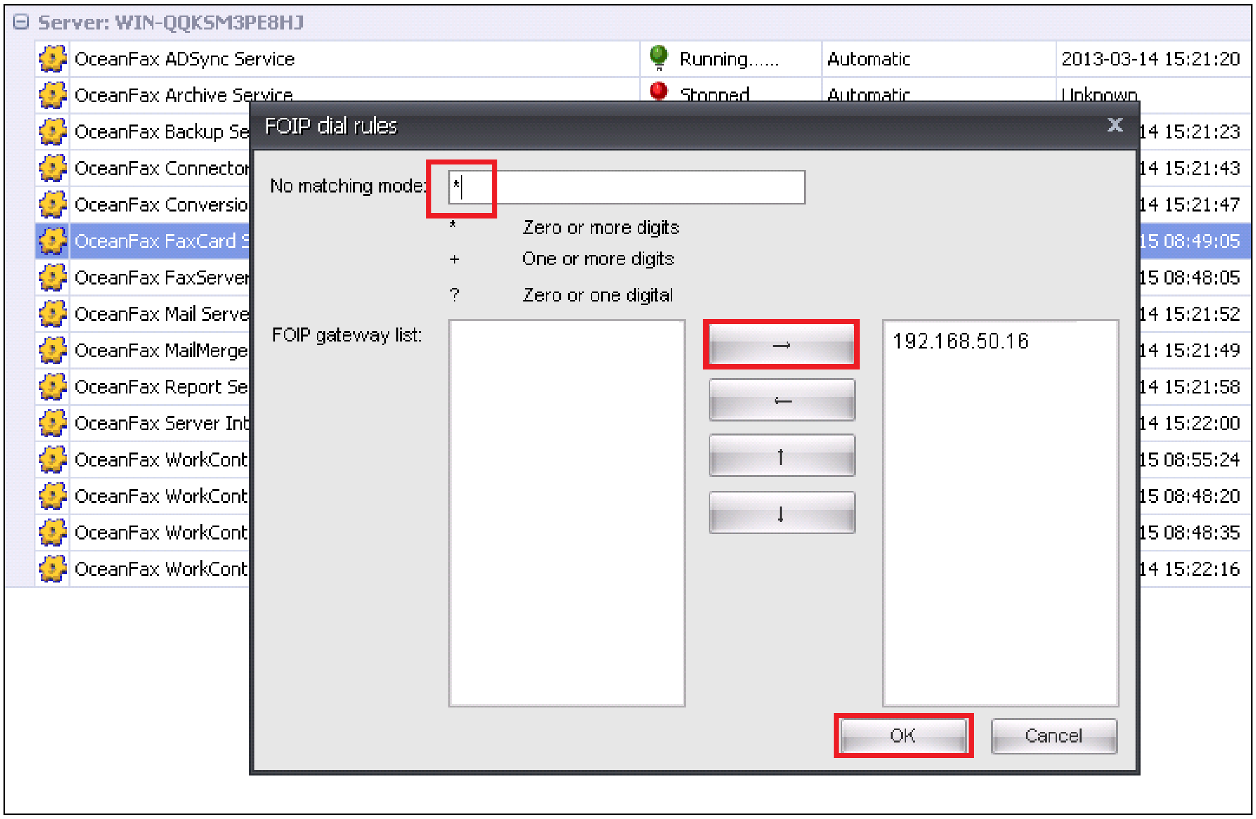
Enter the IP address of Session Manager for the **FOIP gateway**, enter the relevant country and area codes and click on **OK**.



Once **OK** above is clicked in the previous window, **FOIP dial rules** window is shown, click on **Add** at the top right.

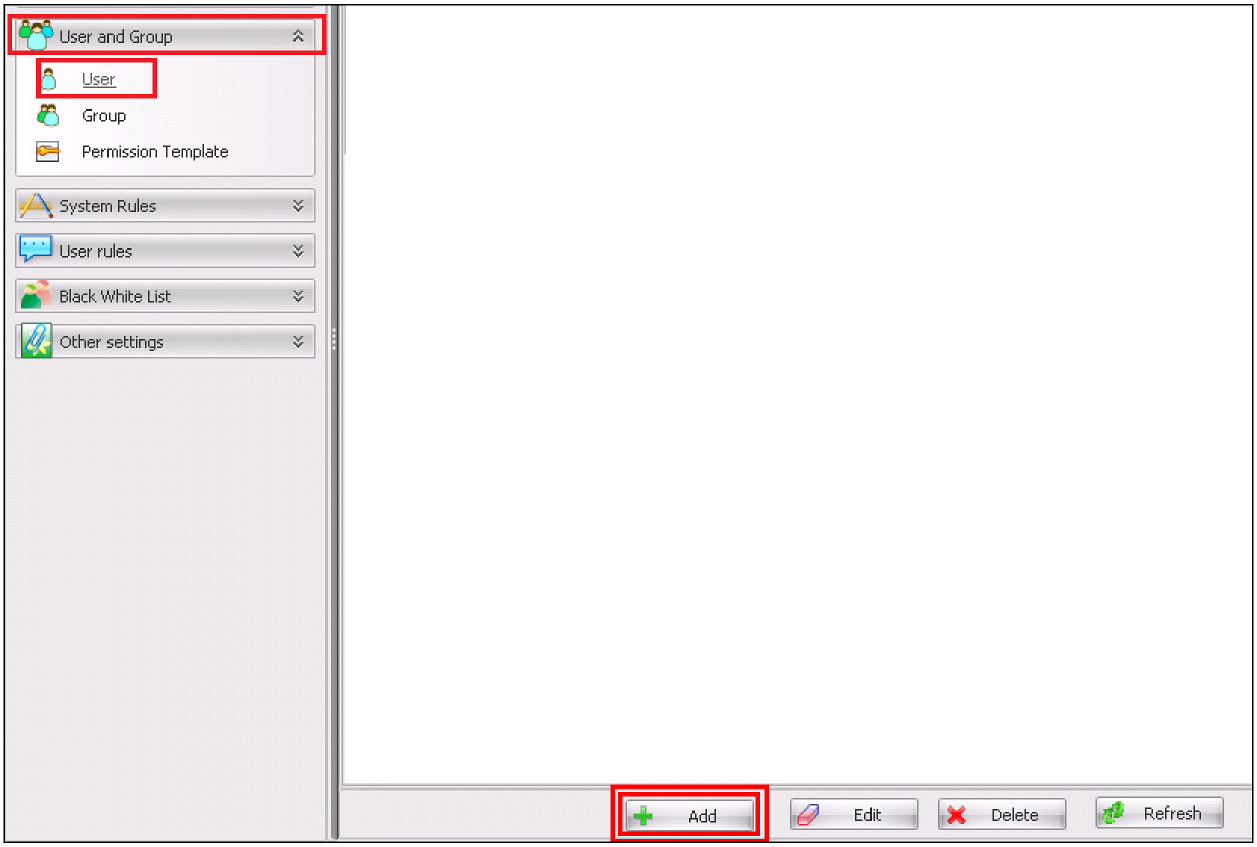


In order to pass all calls to Session Manager * is entered into the **No matching mode** window and Session Manager (**192.168.50.16**) is selected from the **FOIP gateway list**, as shown below. Click on **OK** to complete.

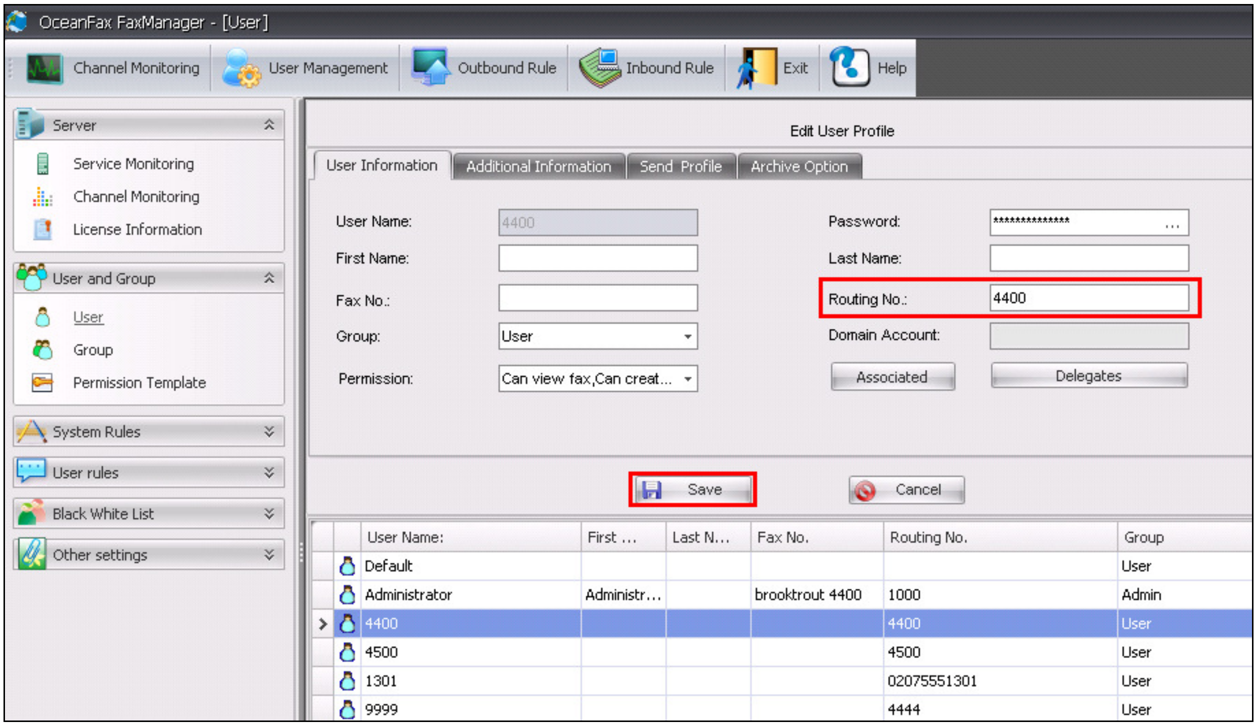


7.3. Adding a user

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 to add a new user.

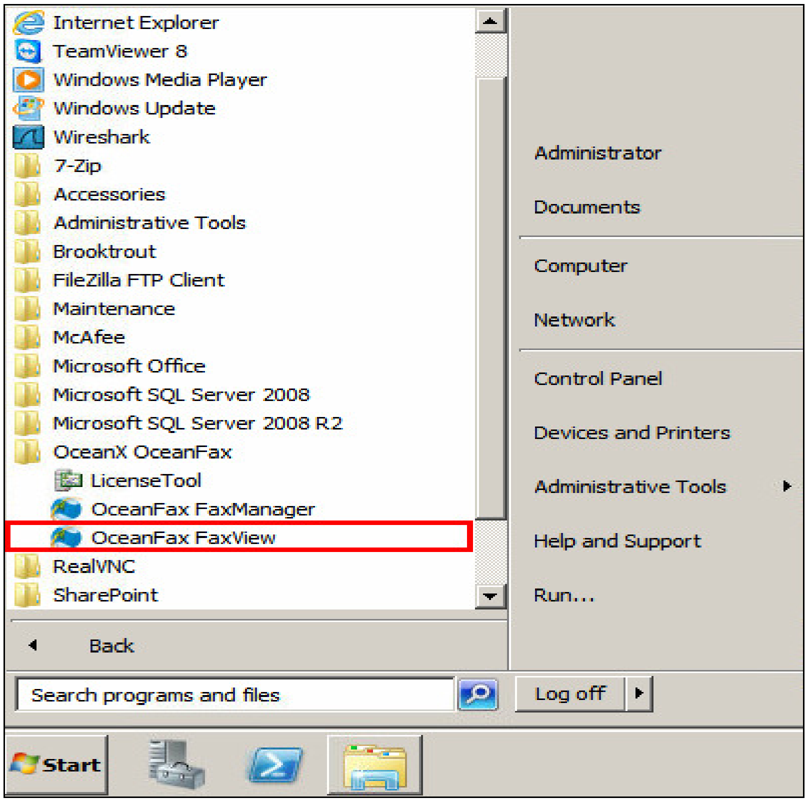


The **User Name** and **Password** entered here will be used to login the user and view the faxes that are being sent/receive to and from this user. The routing number (**Routing No**) associated with the user is the number used to send faxes to the user.

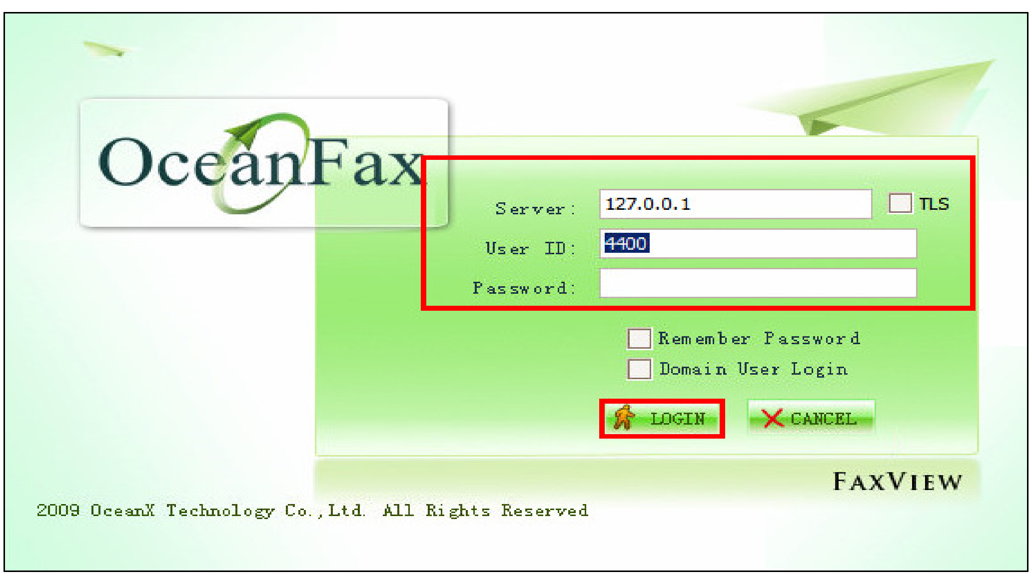


8. Verification Steps

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

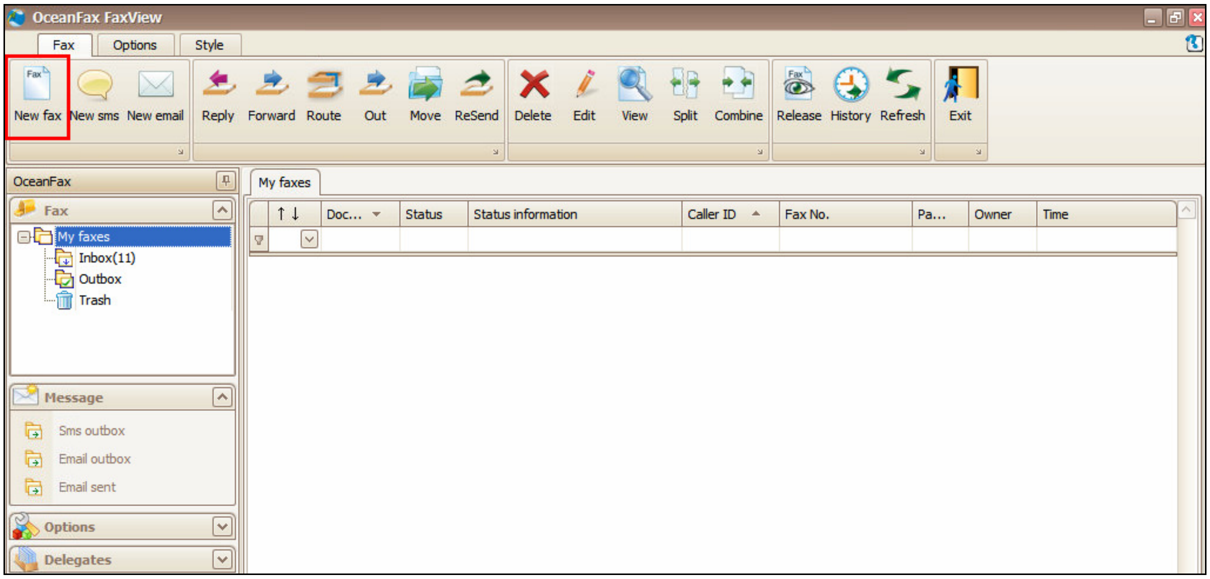


Enter the proper credentials for the required user and click on **LOGIN**.

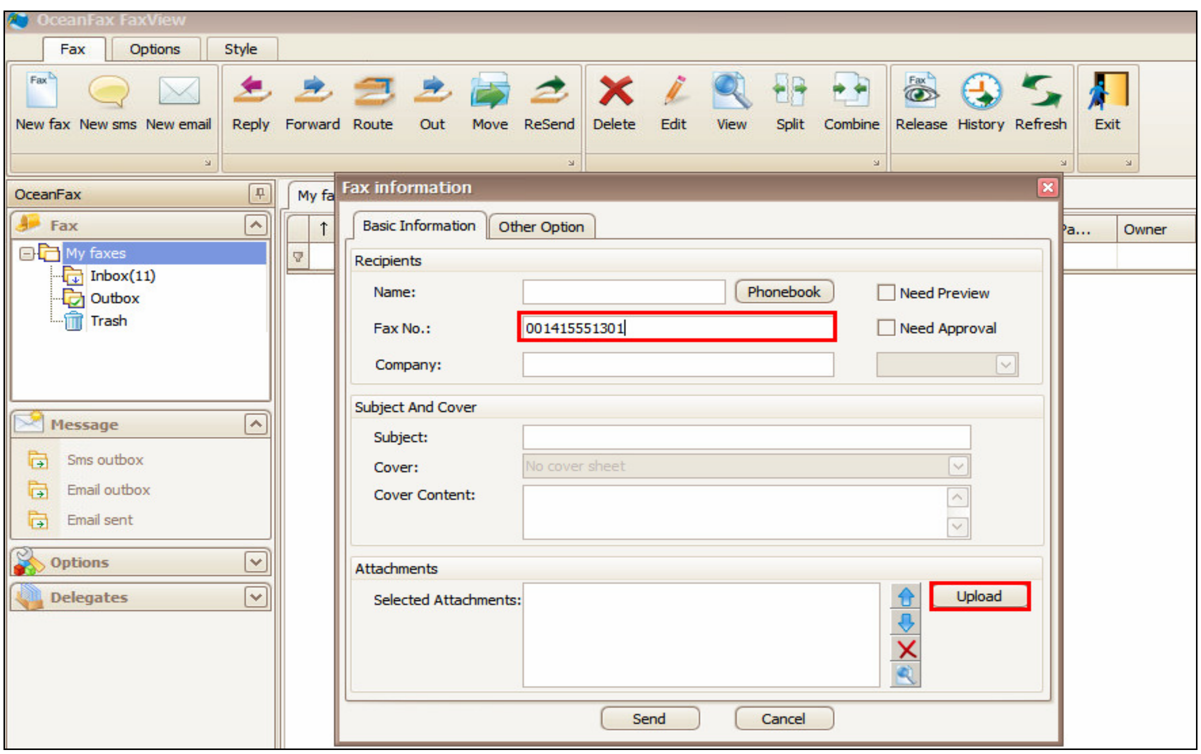


8.1. Sending a FAX to PSTN

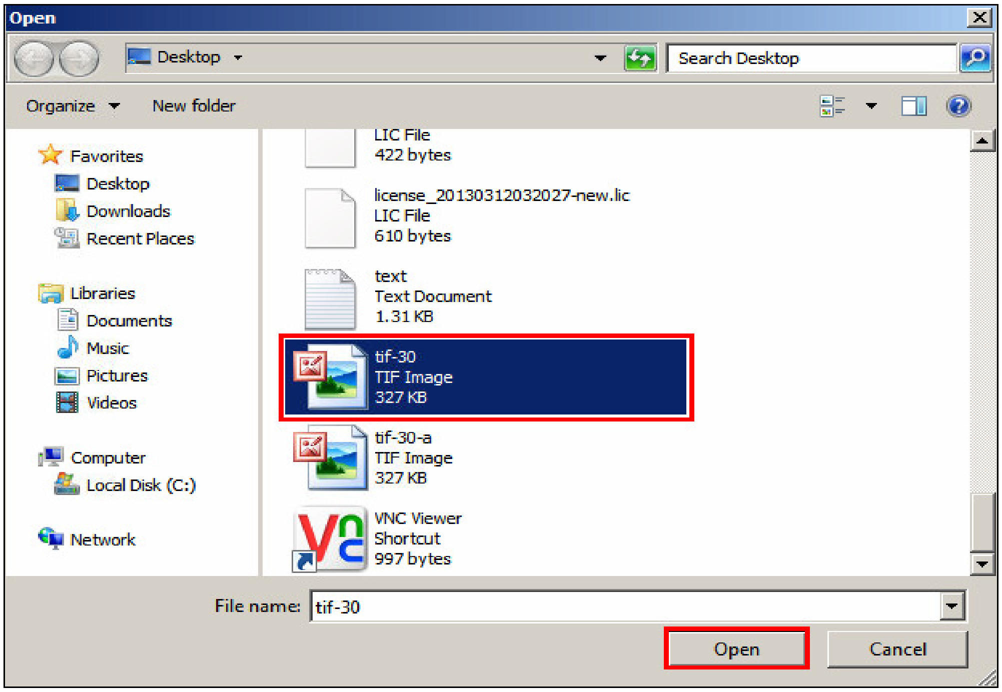
Click on **New Fax** in the top left corner.



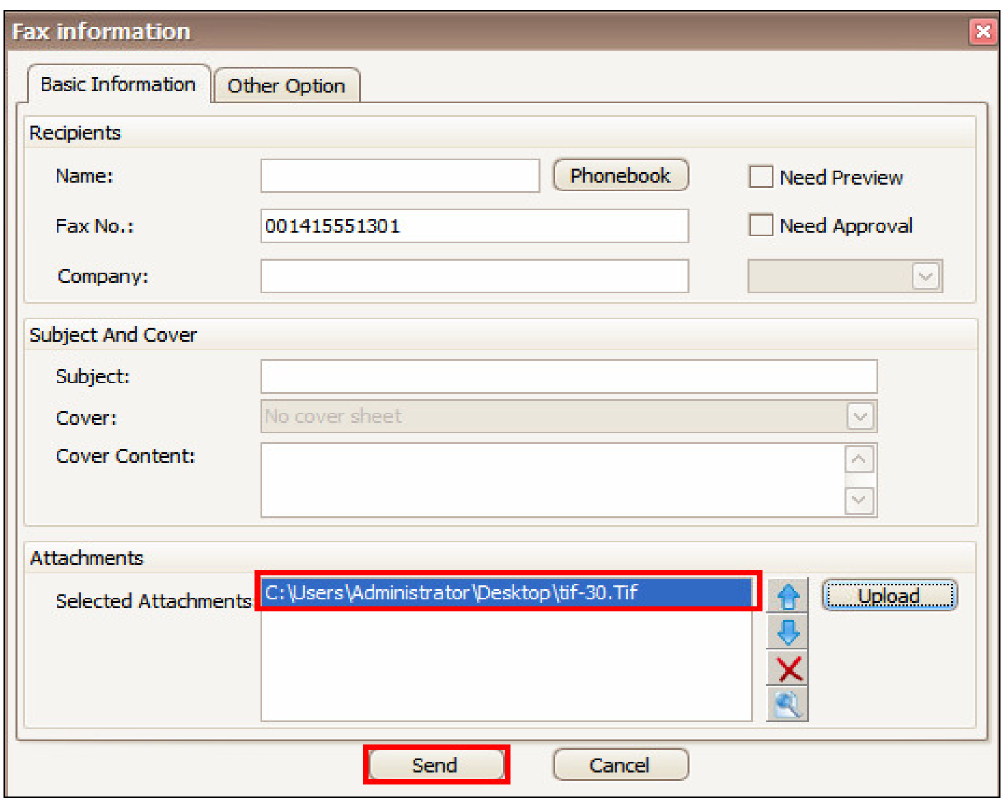
Enter a **Fax No**. to send a fax to PSTN and select **Upload**. In the example below, **001315551301** represents a PSTN fax number.



Browse to the location and select the fax to be sent and click on Open.

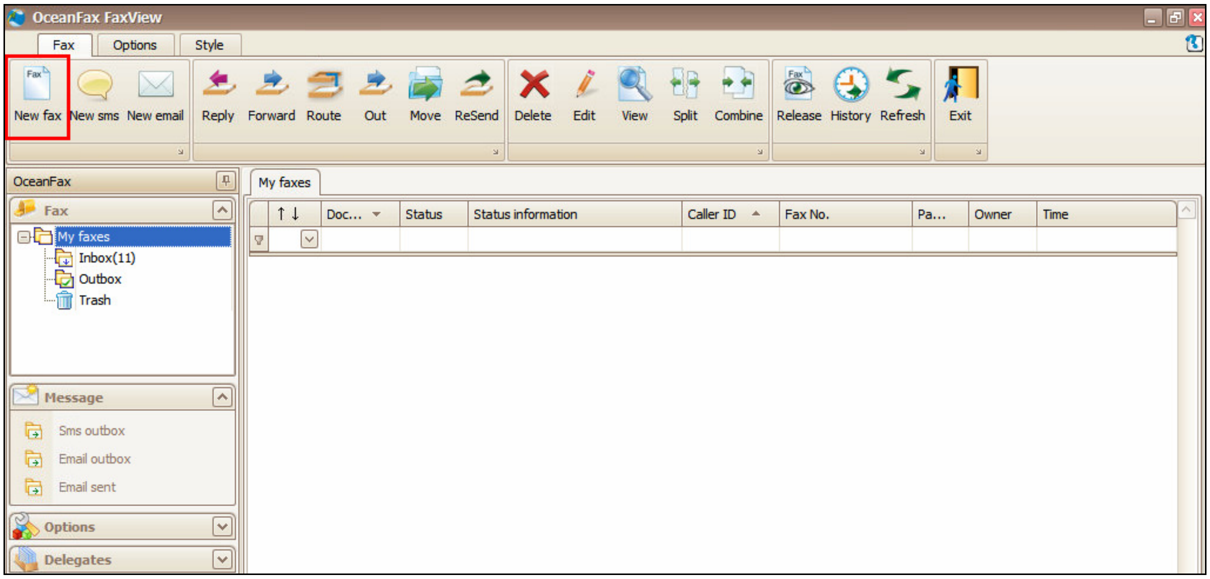


Once the fax has been added, click on **Send** to send the fax.

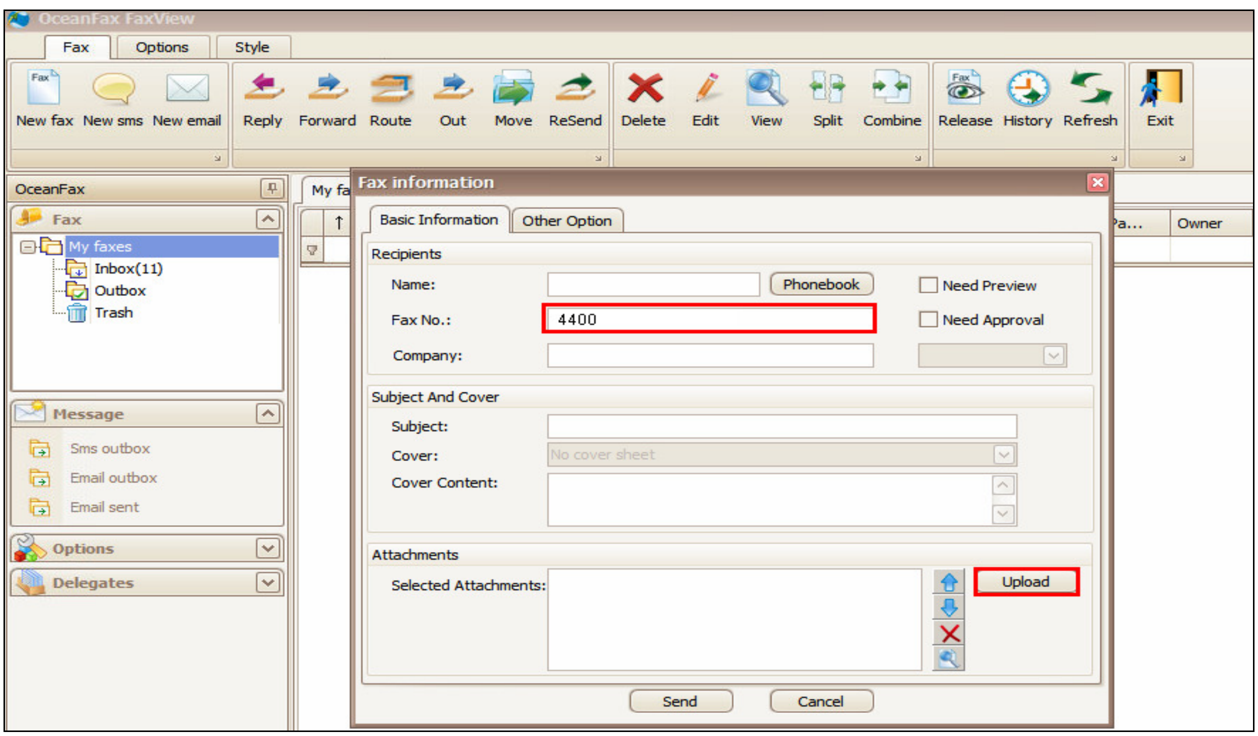


8.2. Sending a FAX Internally

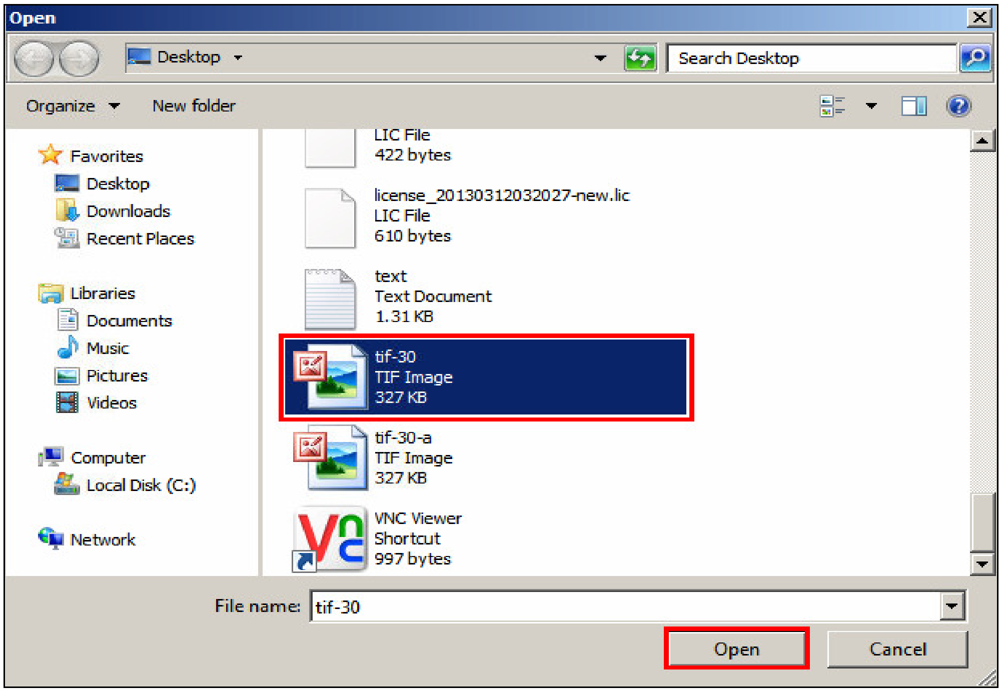
Click on **New Fax** in the top left corner.



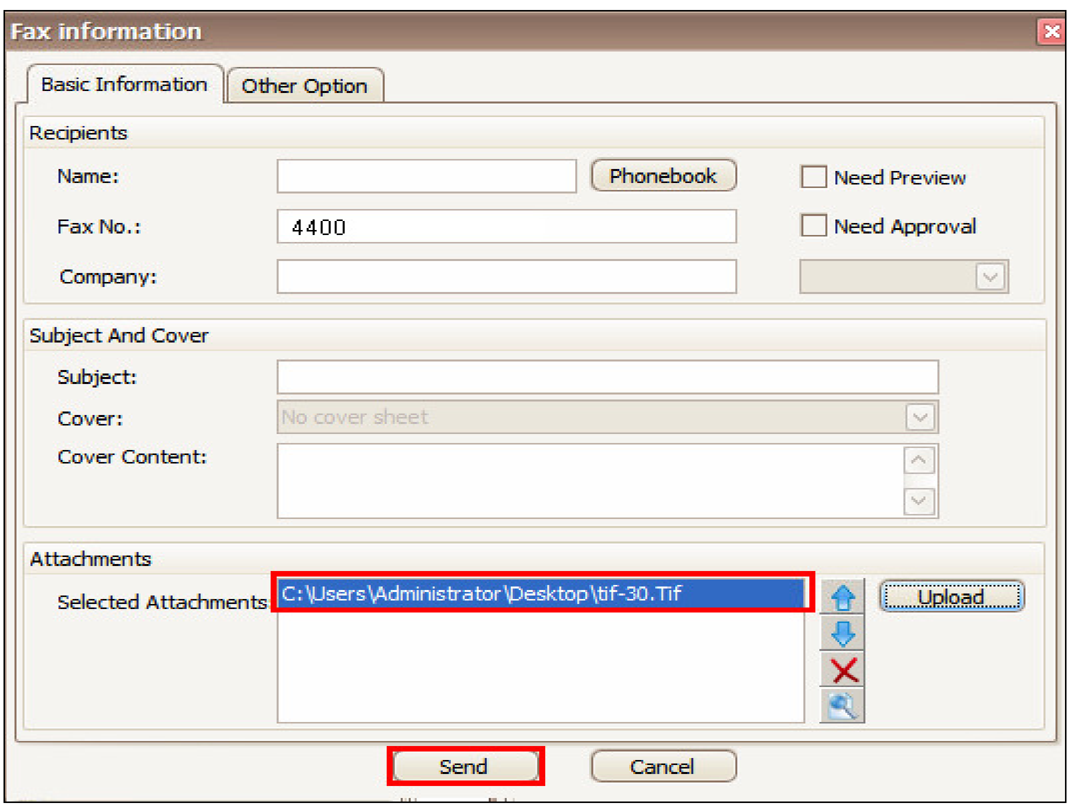
Enter a **Fax No**. to send an internal fax and select **Upload**. In the screen below **4400** represents an example of a fax sent internally.



Browse to the location and select the fax to be sent and click on Open.

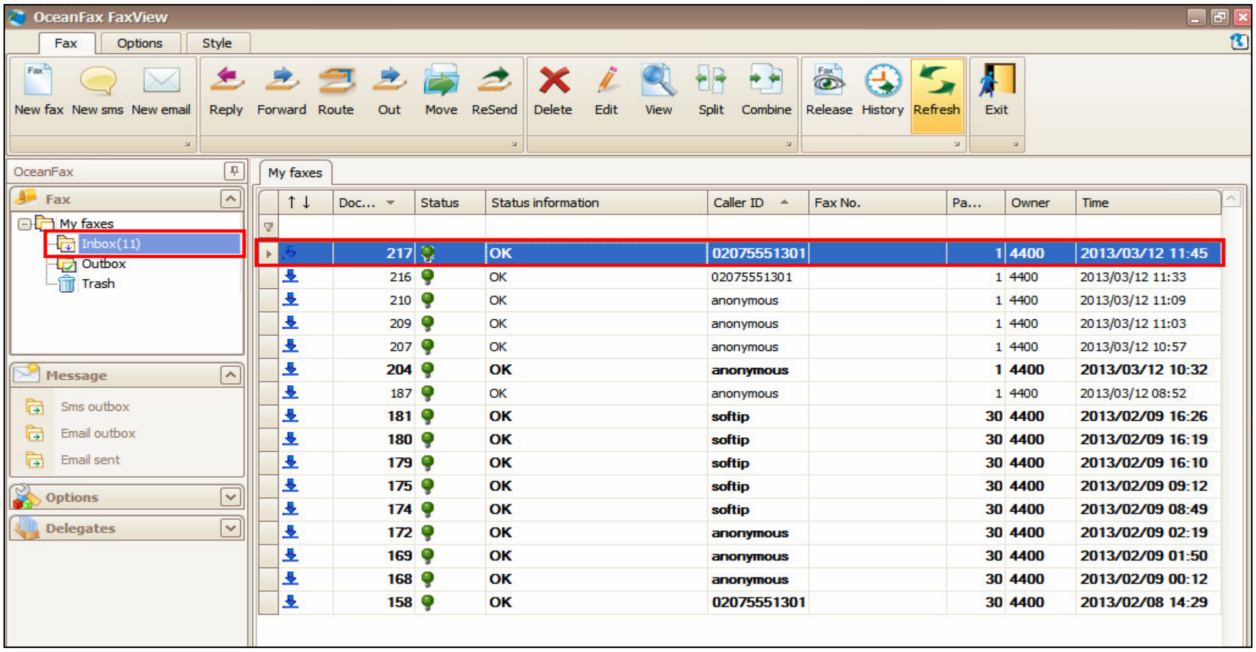


Once the fax has been added, click on **Send** to send the fax.



8.3. Receiving a fax

A received fax message can be found in the inbox as shown below. In order to view a fax double-click on the required message.



9. Conclusion

These Application Notes describe the configuration steps required for OceanFax to successfully interoperate with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.2 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,* Document ID 03-300509 Release 6.2
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205 Release 6.2
[3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473 Release 6.2
[4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324 Release 6.2

Please refer to **Section 2.3** of these Application Notes for information on OceanFax support.

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.