Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a UM-Labs SIP Security Controller with Avaya IP Office, Avaya Communication Manager and Avaya SIP Enablement Services– Issue 1.0

Abstract

These Application Notes describe how to configure UM-Labs SIP Security Controllers RC 2100 and EC 4200 between Avaya IP Office as Branch Office and Avaya Communication Manager and Avaya SIP Enablement Services as Head Office.

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 how to configure UM-Labs SIP Security Controllers (SSC) RC 2100 and EC 4200 between Avaya IP Office as Branch Office and Avaya Communication Manager (CM) and Avaya SIP Enablement Services (SES) as Head Office. The configuration described in these Application Notes focuses on UM-Labs SSC's handling of SIP messages and RTP between Branch Office and Head Office.

The *SIP Security Controllers (SSC)* are security gateways for VoIP and other applications running the Session Initiation Protocol. In addition to providing much needed security features, the UM-Labs SIP Security Controller includes a number of features designed to simplify the interconnection of VoIP Networks and remote SIP users. These functions include local Network Address Translation (NAT) and the ability to handle far-end NAT traversal without the need to manage complex firewall configurations or to use additional protocols. UM-Labs SIP Security Controllers are designed to process all SIP and related traffic crossing a network boundary. In most cases that network boundary is the perimeter of a corporate network where the controller handles VoIP calls between the corporate PBX and other networks. These other networks may include branch offices, remote users and SIP trunk services, or even calls made to and received from other users over the Internet. The SIP Security Controllers may also be used to interconnect network segments within a larger organisation or for service provider deployment where the controllers relay calls between the service provider's core systems and customer connections. The SSC includes a hardened operating system, all necessary security software, and a Web interface for configuration and management. Each model in the range is supplied with multiple network interfaces. The SIP Security Controller implements security controls at three levels: IP Network level, Protocol and Application level, and Content level. The UM-Labs SIP Security Controllers process and validate all SIP messages passing between its connected networks. All subsequent messages in that transaction are then delivered along the same path according to the rules specified in the SIP standard. The SSC applies a standard set of routing rules to direct the calls to the appropriate destination. One of the key functions of the SIP Security Controller is to protect calls by encrypting both the SIP signaling and the RTP media stream using TLS and SRTP. If a connecting phone or other device supports either of these encryption protocols, then the SIP Security Controller automatically encrypts the SIP and RTP messages. This means that if a remote user has a hardware or software phone that supports standards based encryption, the SIP Security Controller will automatically encrypt calls to and from that user. All configuration and management operations are carried out using a simple to use Web GUI.

1.1. Interoperability Compliance Testing

Interoperability compliance testing focused UM-Labs SIP Security Controllers RC 2100 and EC 4200 between Avaya IP Office as Branch Office and Avaya Communication Manager with Avaya SIP Enablement Services as Head Office. Testing verified point to point and conferencing calls and in addition, phone features like hold and transfers with SIP trunking were tested. The transport method used between Avaya and UM-Labs was TCP.

1.2. Support

Technical support can be obtained at http://www.um-labs.com/

2. Reference Configuration

Figure 1 is a high level network diagram of test configuration of UM-Labs SSC and Avaya Solution.

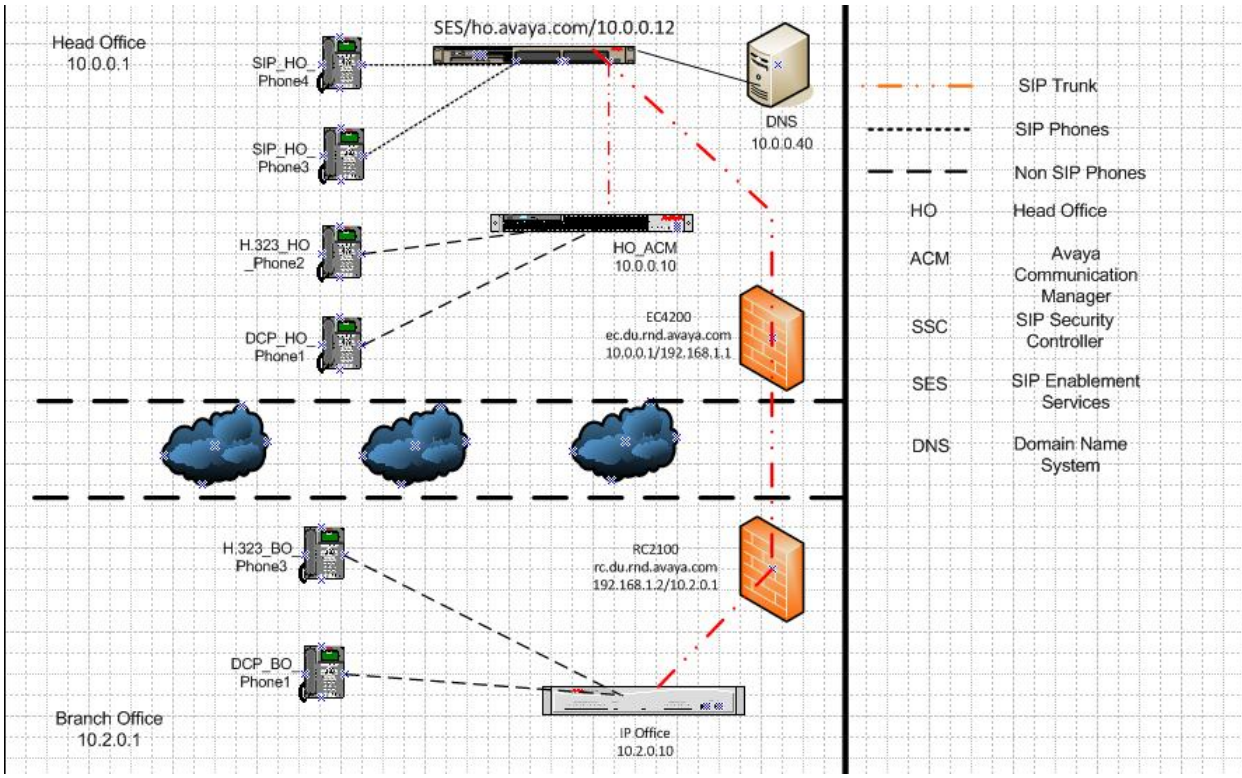


Figure 1: Network Configuration Diagram

3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided.

Equipment	Software
S8300 Server	Avaya Communication Manager 5.1.1 SP1 01.1.415.1-16988
Avaya G350 Media Gateway	28.22.0
Avaya SIP Enablement Services	SES05.1.1-01.1.415.1
Avaya IP Hard Phones (H.323/SIP)	2_9/2_0_4_0
Avaya IP Office 412	4.2(4)
Avaya Softphones (SIP)	SIP R2.1 SP2
Avaya DCP	2.9
UM-Labs SIP Security Controller (RC-2100 and EC-4200)	1.2.1-1435

4. Configure Avaya Communication Manager

This section provides the procedures for configuring Avaya Communication Manager. The configuration page in this section are accessed using Avaya Communication Manager System Access Terminal (SAT). Log in with the appropriate credentials. The procedures include the following areas:

- Verify Avaya Communication Manager License
- Administer IP Node Name for Avaya Communication Manager
- Administer Dial Plan
- Administer Trunk and Signaling
- Administer Routing
- Administer AAR
- Administer Stations Local and OPTIM
- Administer Network Region
- Administer Codec Set

4.1. Verify Avaya Communication Manager License

Verify that the Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. If not, then contact the Avaya sales team or business partner for a proper license file.

Using the SAT, verify that the Off-PBX Telephones (OPS) and SIP Trunks features are enabled on the **System-Parameters Customer-Options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative. On Page 1, verify that the number of OPS stations allowed in the system is sufficient.

```
display system-parameters customer-options                      Page   1 of  10
                                OPTIONAL FEATURES

     G3 Version: V15                             Software Package: Standard
       Location: 1                            RFA System ID (SID): 1
       Platform: 6                            RFA Module ID (MID): 1

                                                               USED
                                Platform Maximum Ports: 44000 141
                                      Maximum Stations: 36000 8
                              Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 100   1
                    Maximum Off-PBX Telephones -   OPS: 100   3
                    Maximum Off-PBX Telephones - PBFMC: 100   0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
        (NOTE: You must logoff & login to effect the permission changes.)
```

On Page 2 of the **System-Parameters Customer-Options** form, verify that the number of SIP trunks supported by the system is sufficient.

```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 2000  0
           Maximum Concurrently Registered IP Stations: 12000 1
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 2000  110
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 0     0
           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: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

4.2. Administer IP Node Name

Enter the **change node-names ip** command and add an entry for the Avaya SES as shown in the sample configuration screen below. The actual node name and IP address may vary. Submit these changes.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Head Office_SES      10.0.0.12
default              0.0.0.0
procr                10.0.0.10

( 3  of 3    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

4.3. Administer Dial Plan

Enter the **change dialplan analysis** command. Add an entry for local **ext** (extension), **dac** (dial access code), and **aar** (automatic alternate routing) as shown in the screen shot below. Submit these changes.

```
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
     1            3    dac
     6            5    ext
     8            4    aar
```

4.4. Administer Trunk and Signaling

Prior to configuring a SIP trunk group for communication with Avaya SIP Enablement Services, a SIP signaling group must be configured. Enter the **add signaling-group 1** command, and add an entry for Avaya SES as shown below. Submit these changes.

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

 Group Number: 1              Group Type: sip
                        Transport Method: tls




   Near-end Node Name: procr                  Far-end Node Name: Head Office_SES
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
       Far-end Domain: ho.avaya.com
                                              Bypass If IP Threshold Exceeded? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
                                                         IP Audio Hairpinning? n
         Enable Layer 3 Test? y
```

Enter the **add trunk-group 1** command and add an entry for Avaya SES as shown below. Submit these changes.

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

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: To_HO_SES                  COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                      Signaling Group: 1
                                                    Number of Members: 10
```

Enter the **add signaling-group 4** command and add an entry for Avaya IP Office as shown below. Submit these changes.

Note: **Far-end Domain** is the IP Address of **Avaya IP Office.**

```
add signaling-group 4                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
                        Transport Method: tls







   Near-end Node Name: procr                  Far-end Node Name: Head Office_SES
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region:1
       Far-end Domain: 10.2.0.10

                                              Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
                                                         IP Audio Hairpinning? n
         Enable Layer 3 Test? n
 Session Establishment Timer(min): 3               Alternate Route Timer(sec): 6
```

Enter the **add trunk-group 4** command and add an entry for Avaya IP Office as shown below. Submit these changes.

```
add trunk-group 4                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 4                  Group Type: sip           CDR Reports: y
  Group Name: To_IPOffice              COR: 1        TN: 1        TAC: 104
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                 Auth Code? n

                                                     Signaling Group: 4
                                                   Number of Members: 10
```

4.5. Administer Routing

Enter the **change route-pattern 1** command and add an entry for Avaya SES as shown. Submit these changes.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: HO_SES
                             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            rest                                        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
```

Enter the **change route-pattern 4** command and add an entry for Avaya IP Office as shown. Submit these changes.

```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name: TO_IPOffice
                             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: 4    0                                                             n   user
```

4.6. Administer AAR

Enter the **change aar analysis 8** command and add an entry for Avaya IP Office as shown. Submit these changes.

```
change aar analysis 8                                           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
    8                     4    4     1         aar          n
    9                     7    7     254       aar          n
                                                            n
                                                            n
                                                            n
```

4.7. Administer Stations Local and OPTIM

To create local or non-sip stations. Enter the **add station 60001** command and add an entry for Local Head Office as shown below. Submit these changes.

```
add station 60001                                           Page   1 of   6
                                     STATION

Extension: 60001                        Lock Messages? n              BCC: 0
     Type: 9650                         Security Code: 60001           TN: 1
     Port: S00004                     Coverage Path 1:                COR: 1
     Name: HO_H.323_Phone1            Coverage Path 2:                COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 60001
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n



                                             Customizable Labels? y
```

To create SIP stations, create a local station as shown above and make this local extension as OPTIM by entering the **change off-pbx-telephone station-mapping 60003** command as shown below and configure it as OPTIM for SIP. Submit these changes

```
change off-pbx-telephone station-mapping 60003                 Page   1 of   2
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station        Application Dial   CC  Phone Number      Trunk        Config
 Extension                  Prefix                       Selection    Set
 60003            OPS            -     60003              1           1
                                 -
                                 -
                                 -
                                 -
                                 -
```

4.8. Administer Network Region

Enter the change **ip-network-region 1** command and add entries as shown below. Submit these changes.

```
change ip-network-region 1                                  Page 1 of 19
                               IP NETWORK REGION
      Region:  1

Location: 1       Authoritative Domain: ho.avaya.com
    Name: Head Office
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                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

4.9. Administer Codec Set

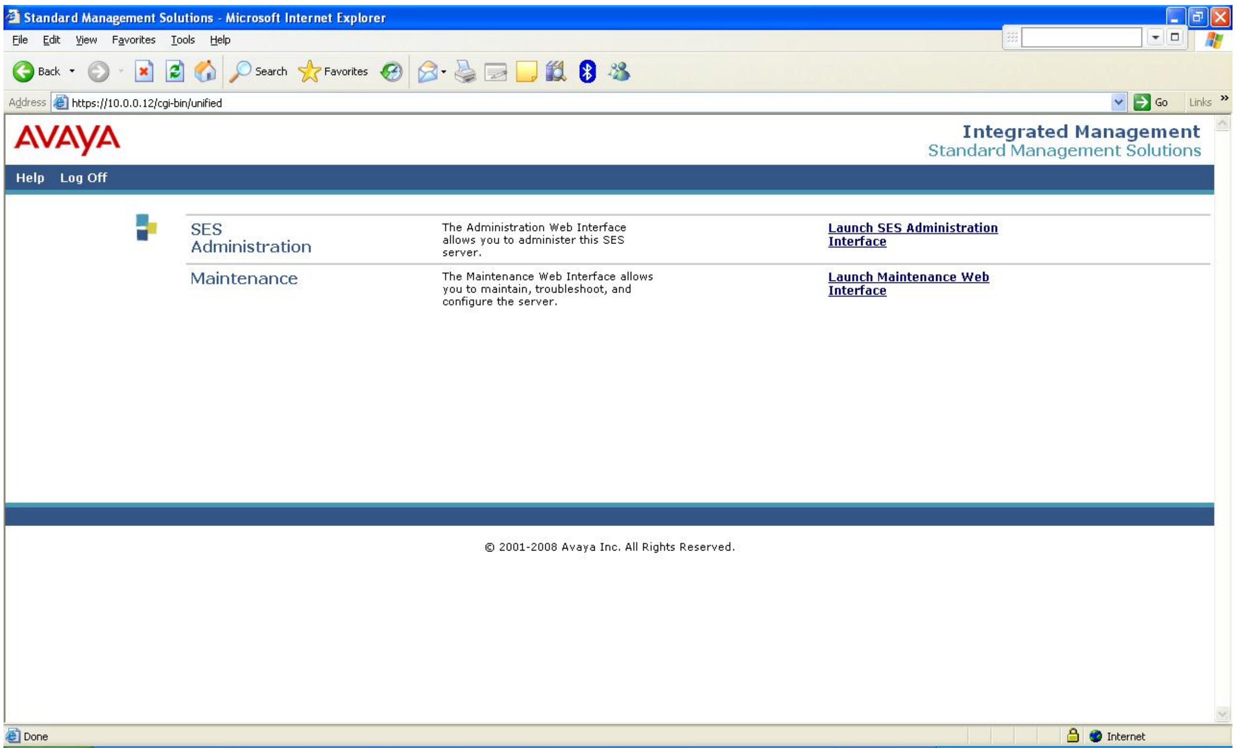
Enter the **change ip-codec-set 1** command and add entries as shown in sample configuration below. Submit these changes.

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

                          IP Codec Set

    Codec Set: 1

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


     Media Encryption
 1: none
 2:
 3:
```

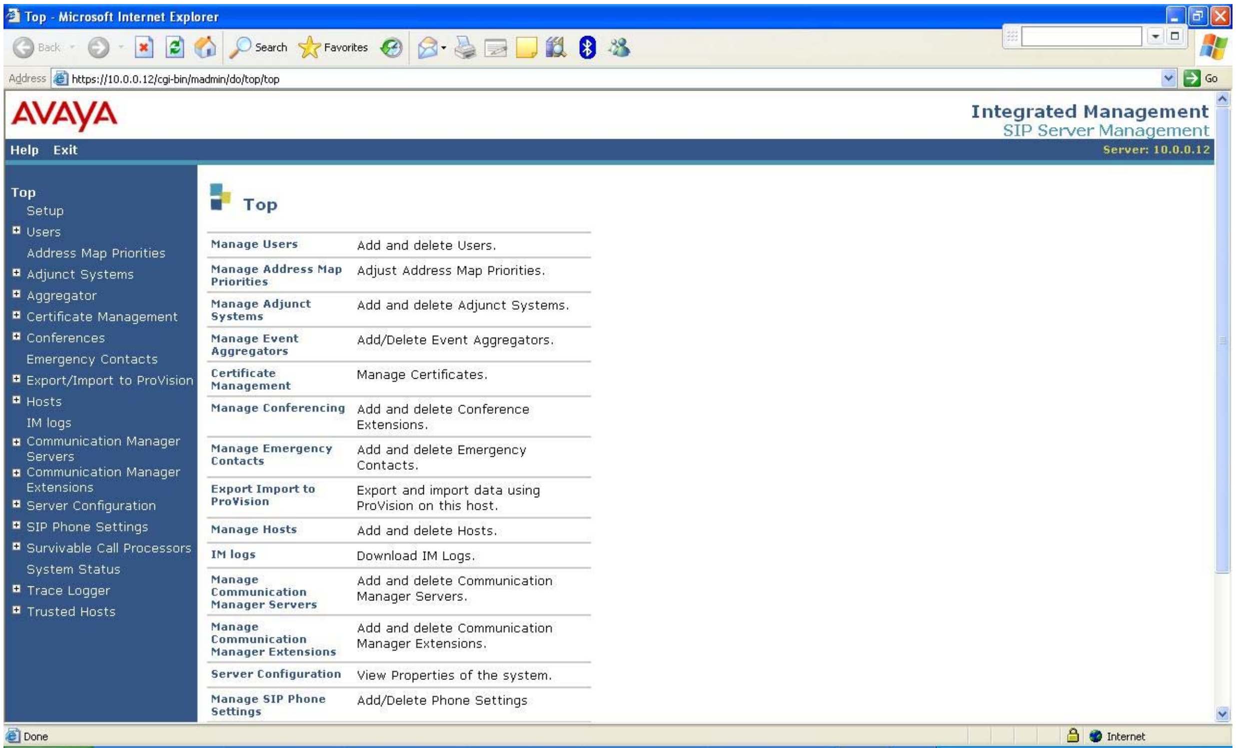
5. Configure Avaya SIP Enablement Services

This section provides the procedures for configuring Avaya SIP Enablement Services. Avaya SES is configured via an Internet browser using the administrator web interface. It is assumed the Avaya SES software and the license file have already been installed on the server.

Access the Avaya SES administration web interface by entering **http://<SES-ip-addr>/admin** as the URL in an Internet browser. Log in with the appropriate credentials and then select the Launch SES Administration Interface link from the main page.



From the main page click on **Launch SES Administration Interface**. The Avaya SES Administration Home Page is displayed as show below.



The administration procedures include the following areas:

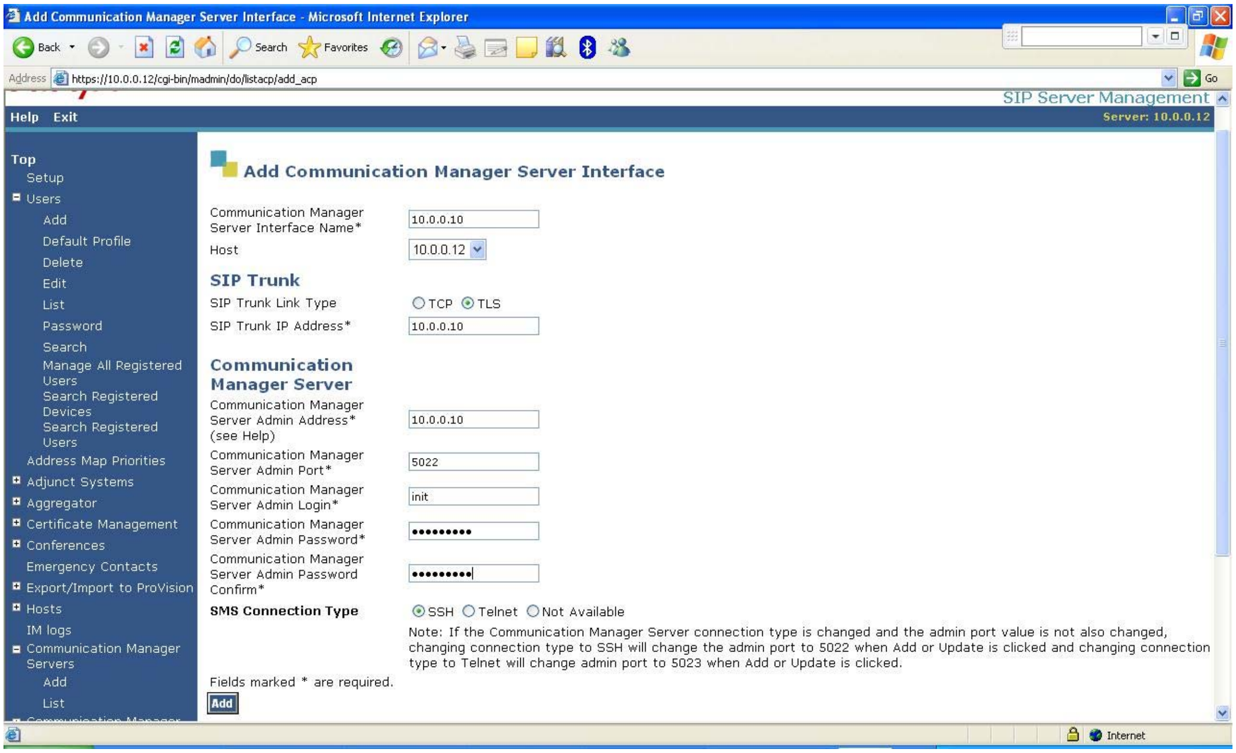
- Administer Avaya Communication Manager
- Administer Mapping
- Administer Trusted Hosts
- Administer SIP End Points

5.1. Administer Avaya Communication Manager

From the home page on the left panel expand **Communication Manager Servers→Add** (Not Shown)

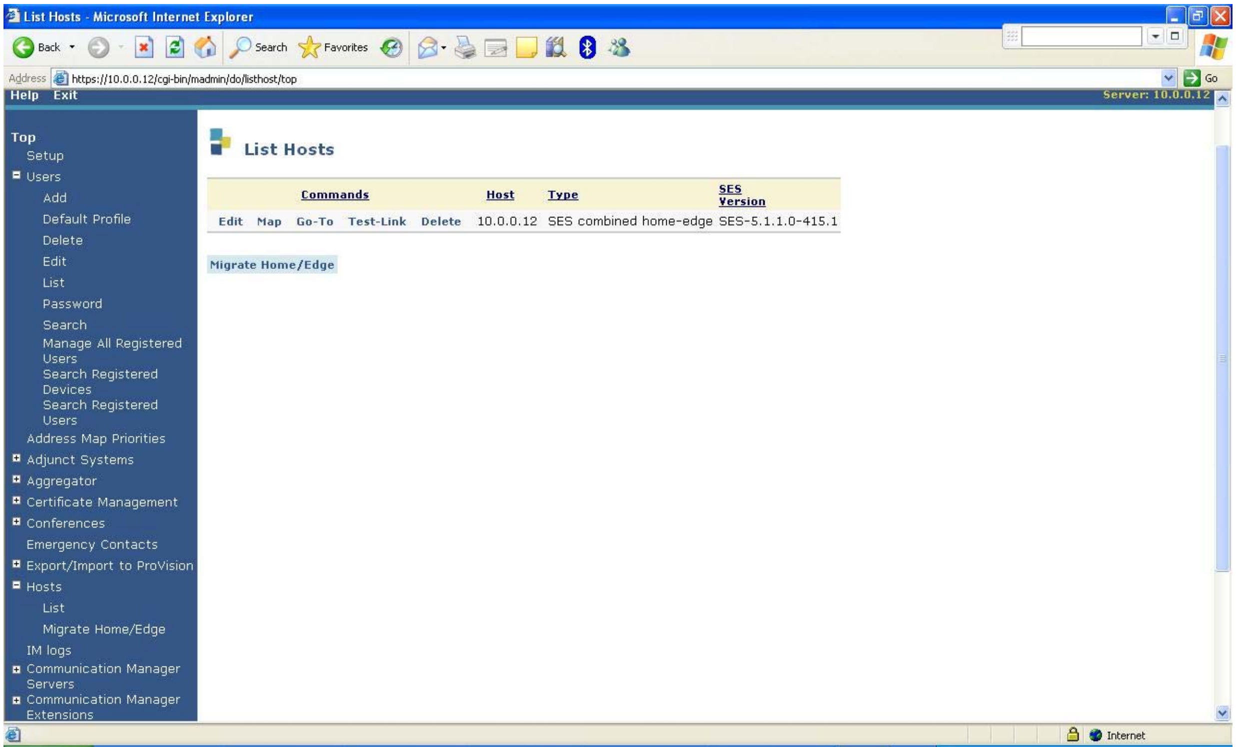
Enter the required details as show in the sample configuration and Click **Add** and **Continue**.

- **Communication Manager Server Interface Name** = **<10.0.0.10>**
- **SIP Trunk Link Type** = **<TLS>**
- **SIP Trunk IP Address** = **<10.0.0.10>**
- **Communication Manager Server Admin Address** = **<10.0.0.10>**
- **Communication Manager Server Admin Port** is the default value
- **Communication Manager Server Admin Login** = **<init>**
- **Communication Manager Server Admin Password** as previously defined for <init>
- **SMS Connection Type** = **<ssh>**

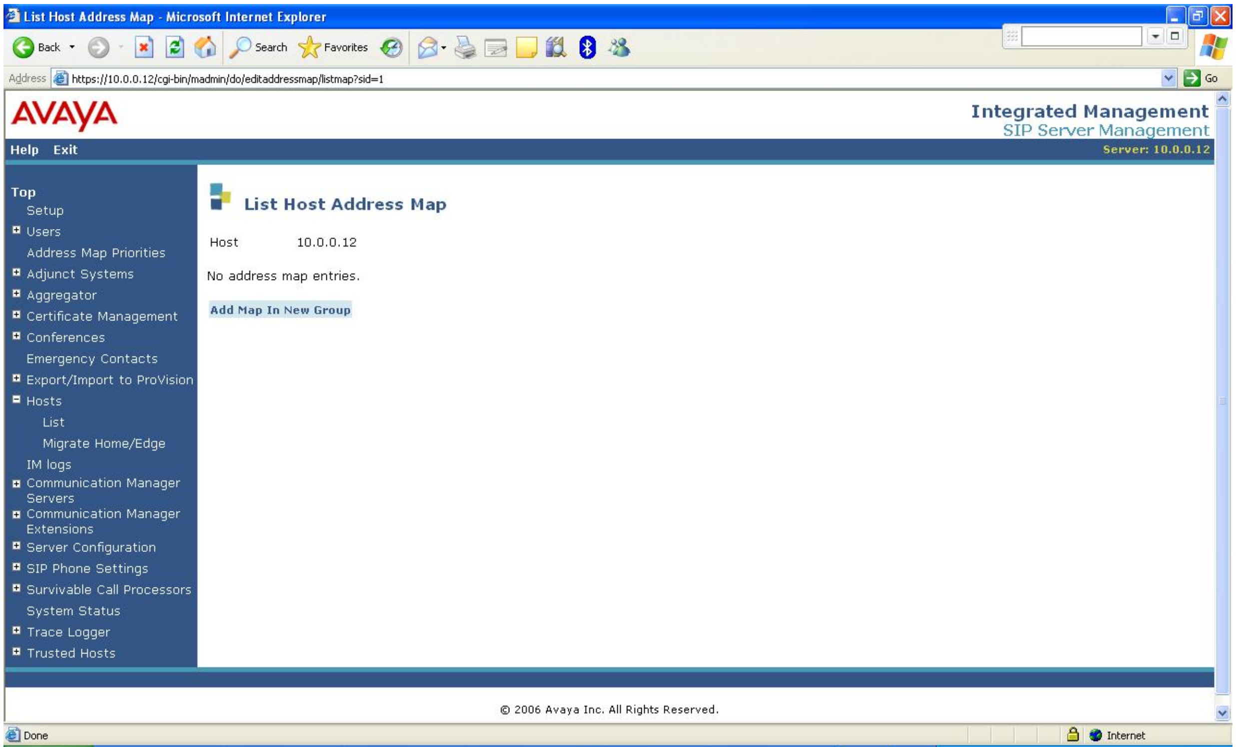


5.2. Administer Mapping

Configure Avaya IP Office as a host on Avaya SES. From home page expand **Host**. Click on **List** to display **List Hosts** page. Select the **Map** link for Avaya SES to display the **List Host Address Map** page.

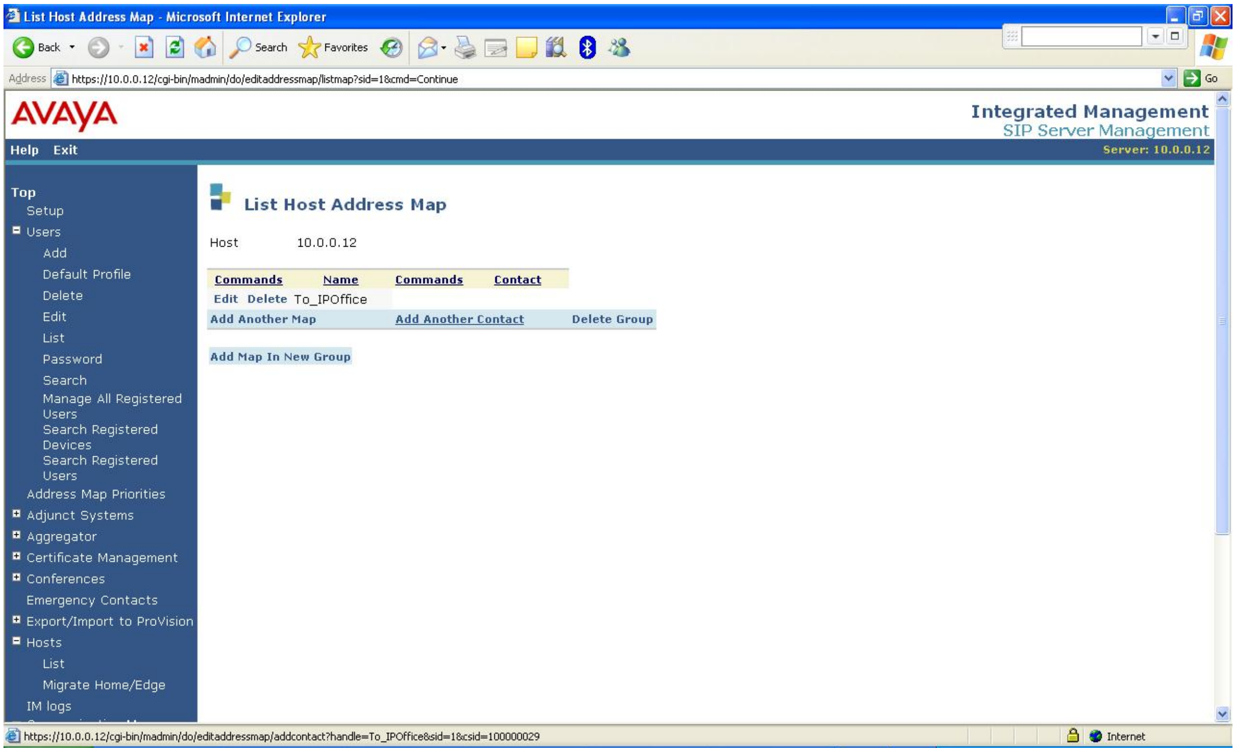


Add a Host Address Map entry for calls to Avaya IP Office. Click on **Add Map In New Group**.



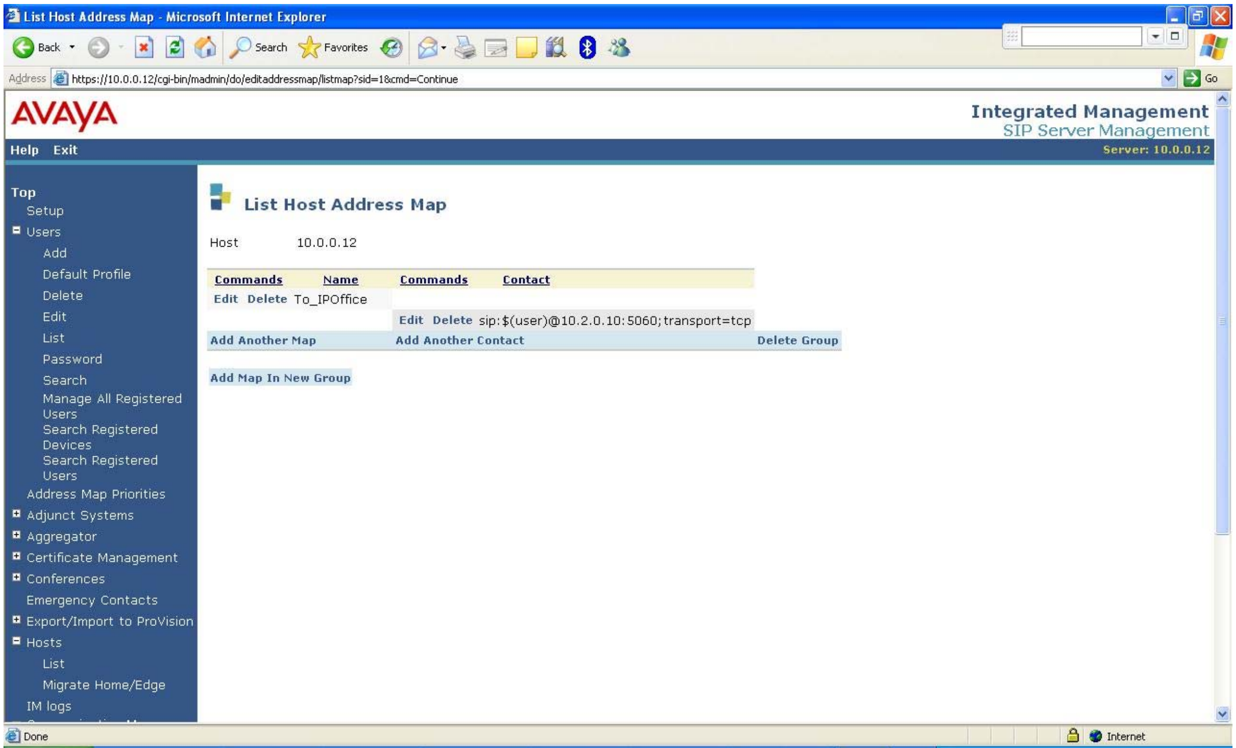
Enter a descriptive name in the **Name** field. In the **Pattern** field, enter the regular expression to pattern match for extensions on Avaya IP Office. In this configuration, extensions begin with **8**. Verify the **Replace URI** checkbox is ticked. Click the **Add** button once the form is completed. On the confirmation screen (not shown), click **Continue.**

Add a Contact entry for calls to Avaya IP Office. Click on **Add Another Contact**.



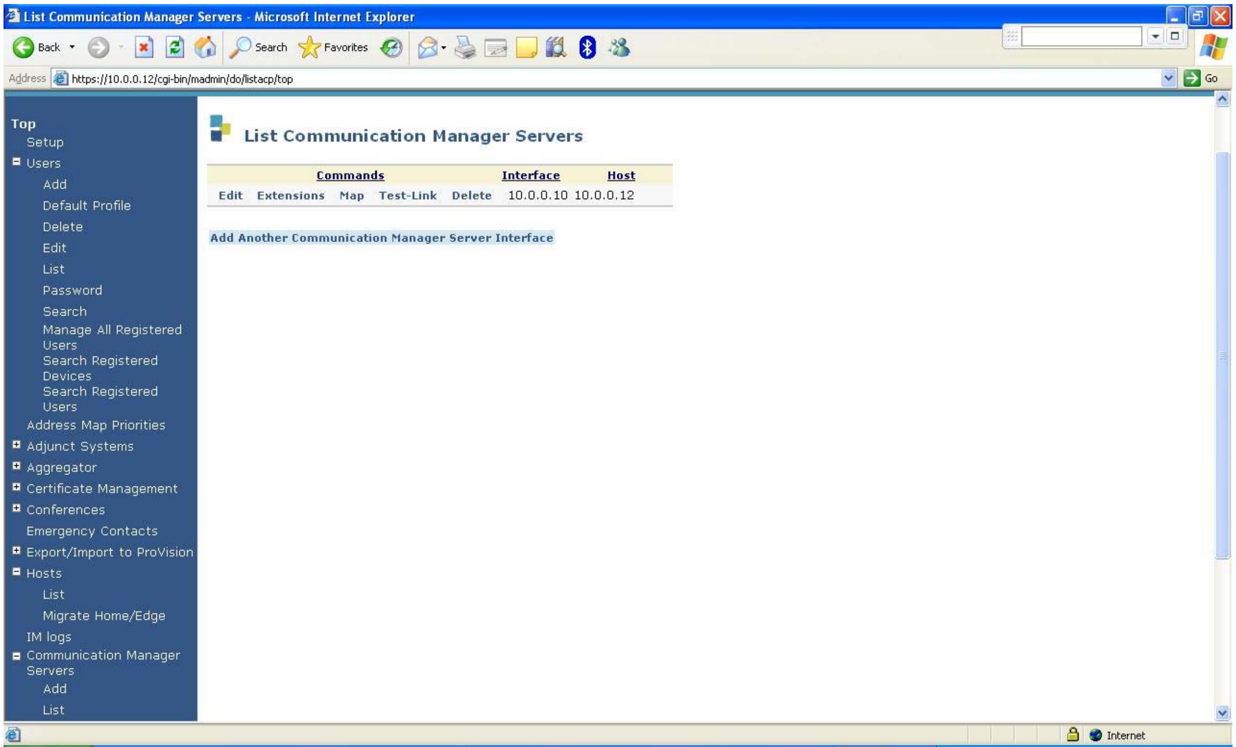
Enter a descriptive name in the **Name** field. In the **Contact** field enter **sip:$(user)@10.2.0.10:5060;transport=tcp**. The IP address is the Avaya IP Office LAN2 IP address. Transport is TCP as show in the sample configuration and click **Add**.

(Not Shown) On the confirmation screen, click **Continue.** Below is the configured Host mapping.

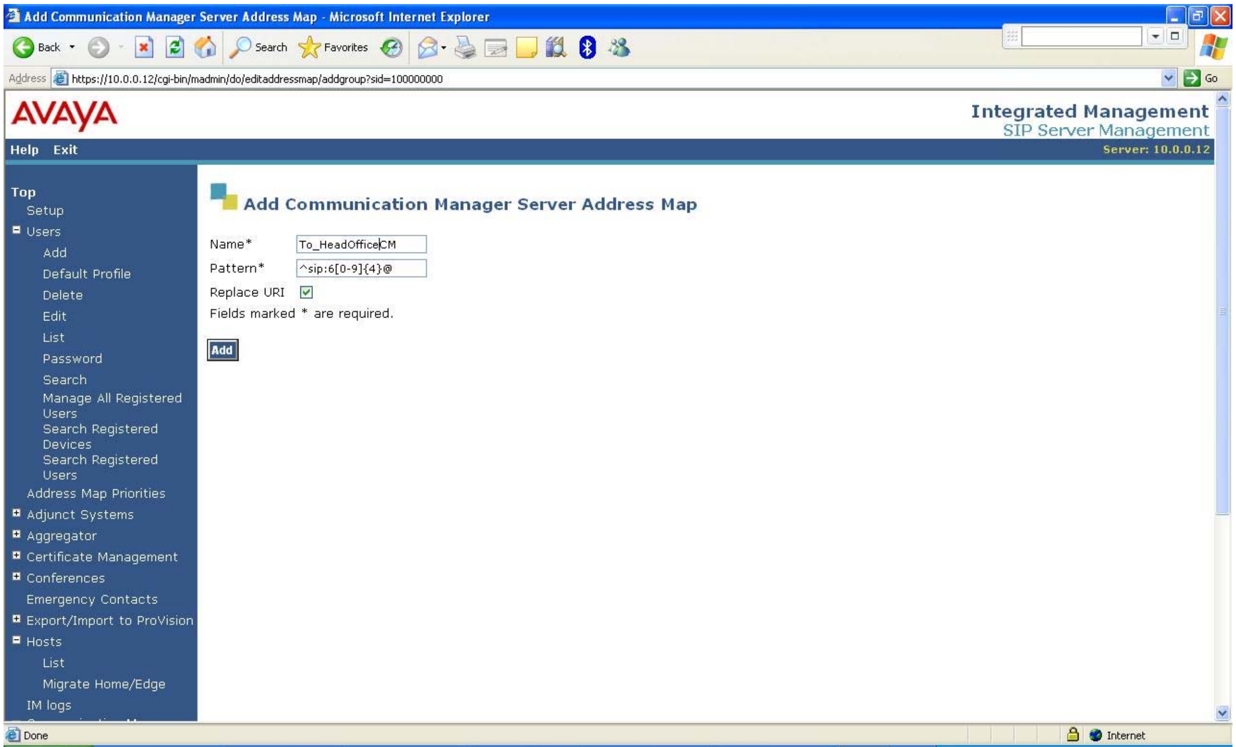


Configure Avaya Communication Manager as a Host on Avaya SES. From the home page, expand **Communication Manager Servers** and select **List**. This will display **List Communication Managers Servers** as shown below.

On the **List Communication Managers Servers** page, select the **Map** link for Avaya SES to display the **List Communication Manager Server Address Map** (not shown).

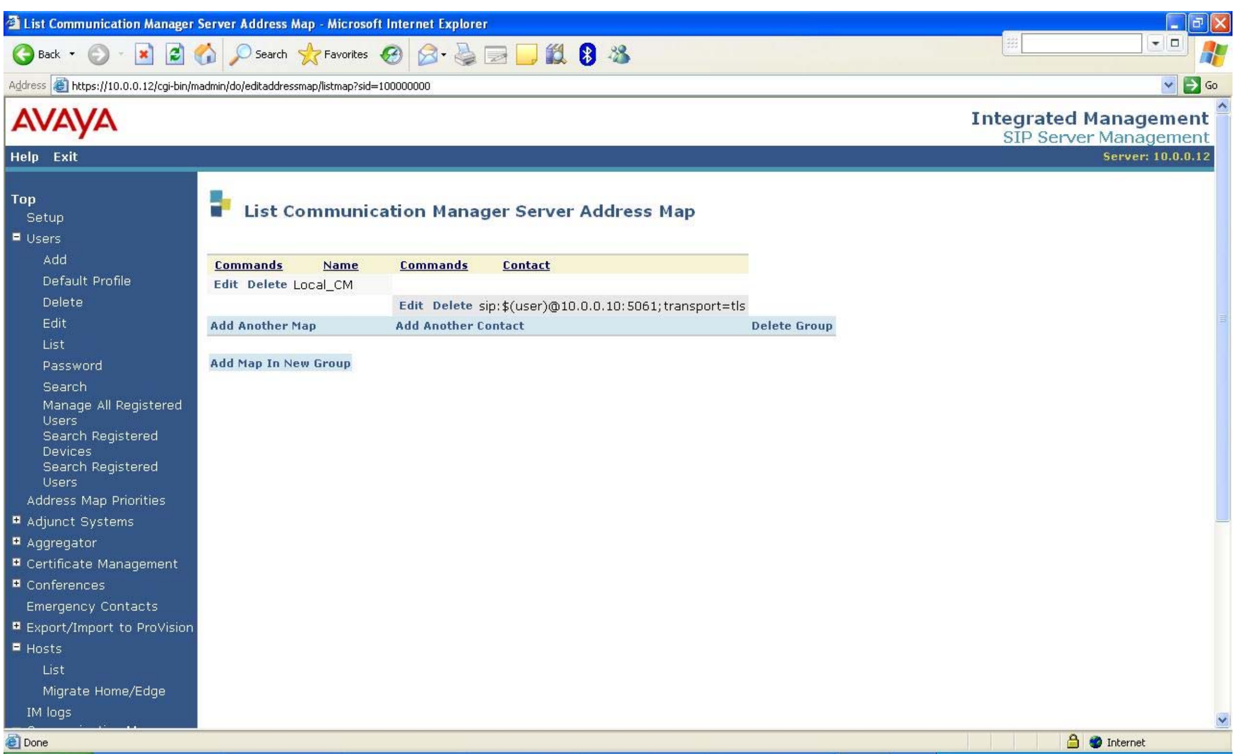


Click on **Add Map In New Group** (Not Shown) and enter a descriptive name in the **Name** field. In the **Pattern** field, enter the regular expression to pattern match for extensions on Avaya Communication. In this configuration, extensions begin with **6**. Ensure the **Replace URI** checkbox is ticked. Click the **Add** button once the form is completed. On the confirmation screen, click **Continue** (not shown)**.**



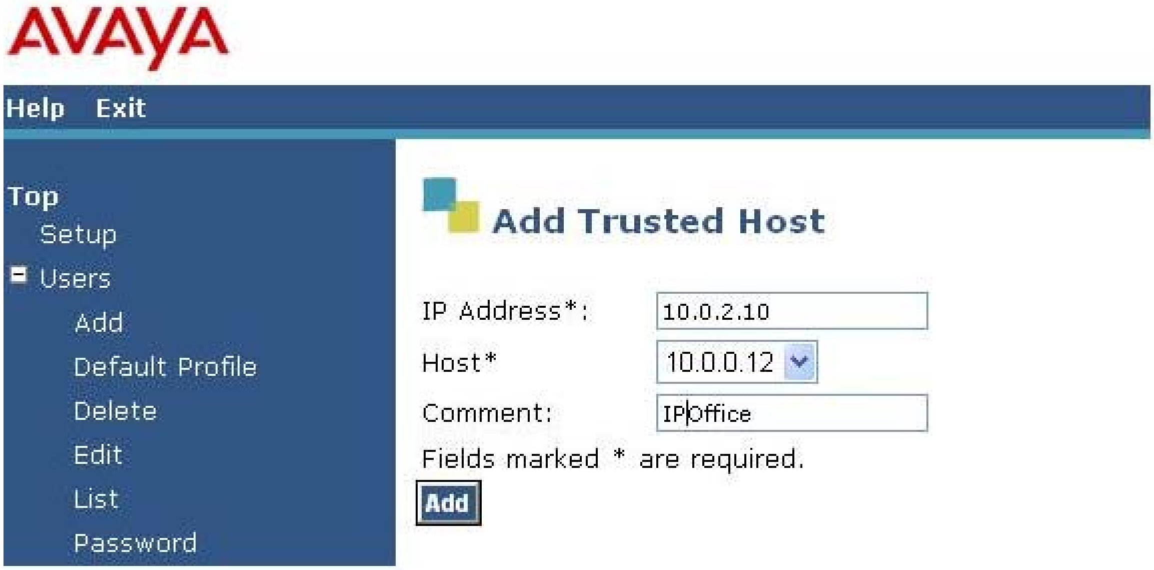
Add a Contact entry for calls to Avaya Communication Manager. Click on **Add another Contact** (not shown). Enter a descriptive name in the **Handle** field. In the **Contact** field, enter **sip:$(user)@10.0.0.10:5061;transport=tls**. The IP address is the Avaya Communication Manager IP address. Transport is TLS as shown in the sample configuration below. Click **Add**.

On the confirmation screen, click **Continue** (not shown). Below is the configured Host mapping.



5.3. Administer Trusted Hosts

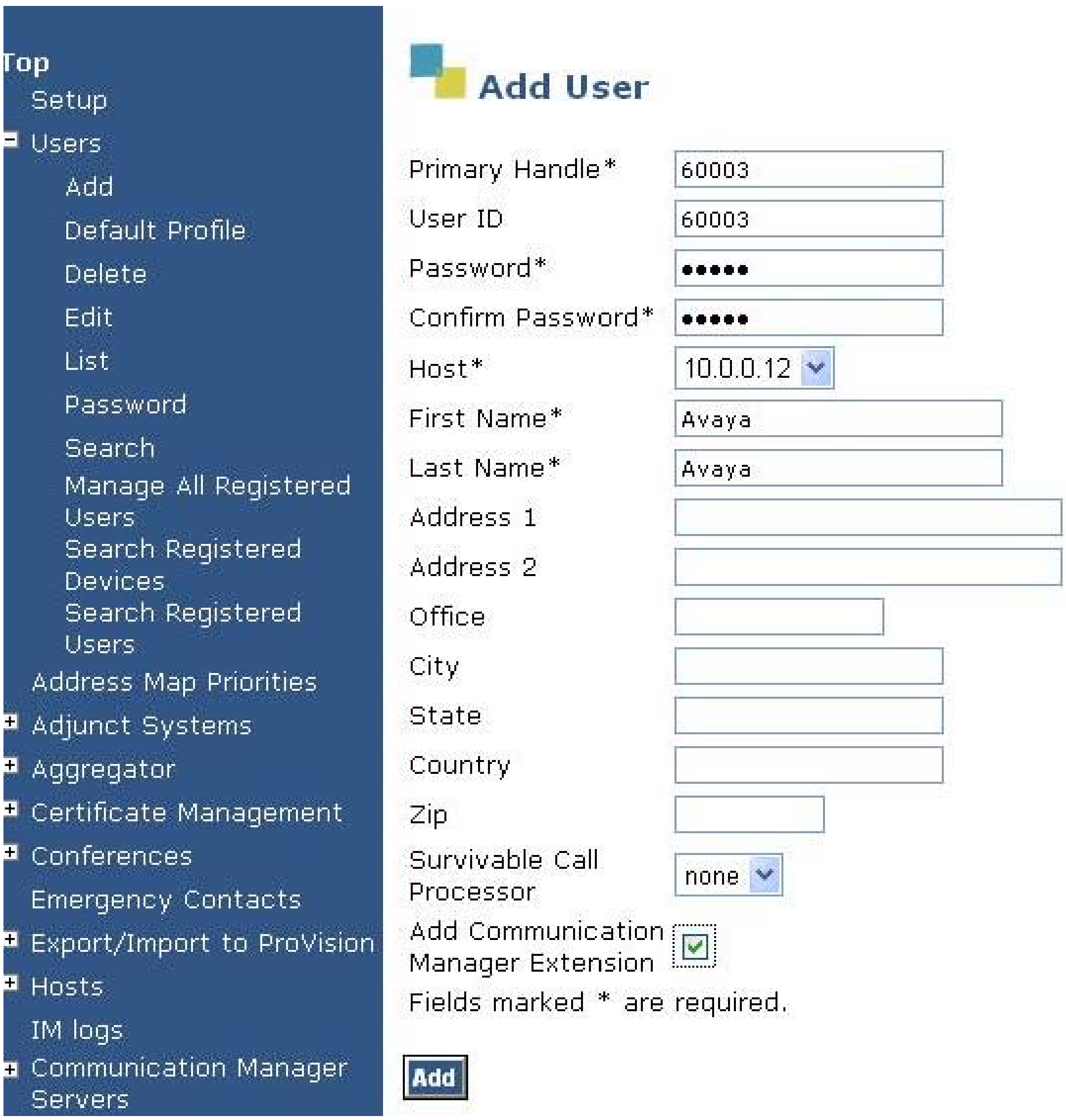
From the home page on the left panel, click on **Trusted Hosts→Add** and enter the details of IP Office and click on **Add (Not Shown)**. Repeat the same steps for adding SSC RC2100 Gateway.



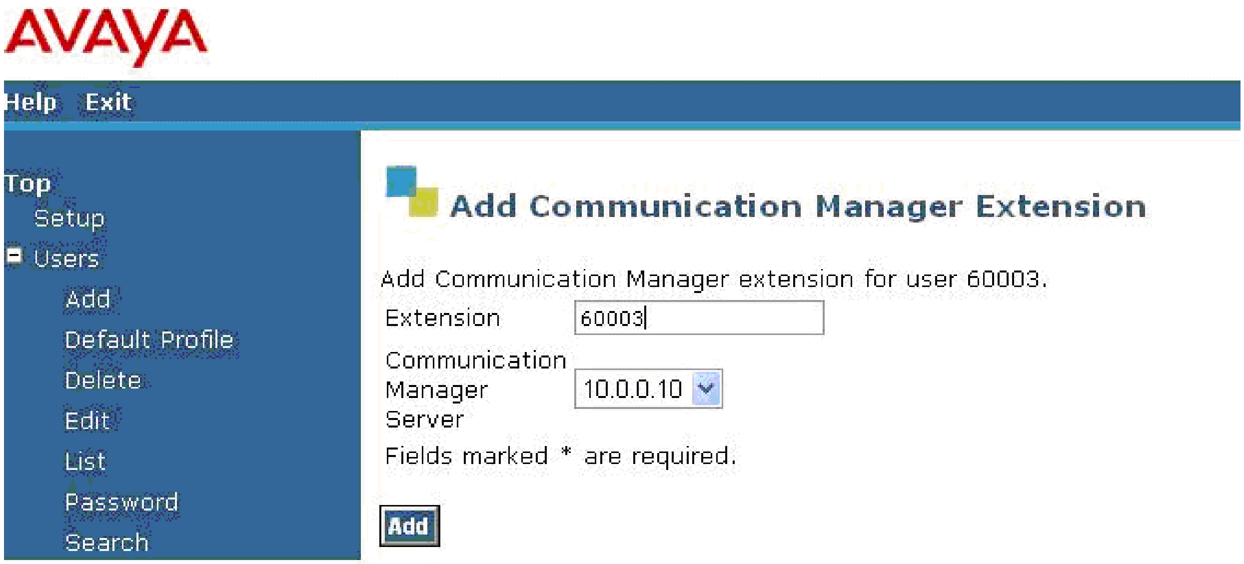
5.4. Administer SIP End points

Expand **Users** on the left panel and click **Add**. Enter the required details as show in the sample configuration below and click **Add**. Repeat the same steps for other SIP OPTIM Endpoints

- **Primary Handle = 60003**
- **UserId = 60003**
- **Password = xxxxxx**
- **Confirm Password = xxxxxx**
- Enter **First Name**
- Enter **Last Name**
- Tick the **Add Communication Manager Extension**



Click Continue on subsequent screen (not shown). The screen below appears and enters the extension as show in sample screen shot and click **Add**.



6. Configure Avaya IP Office

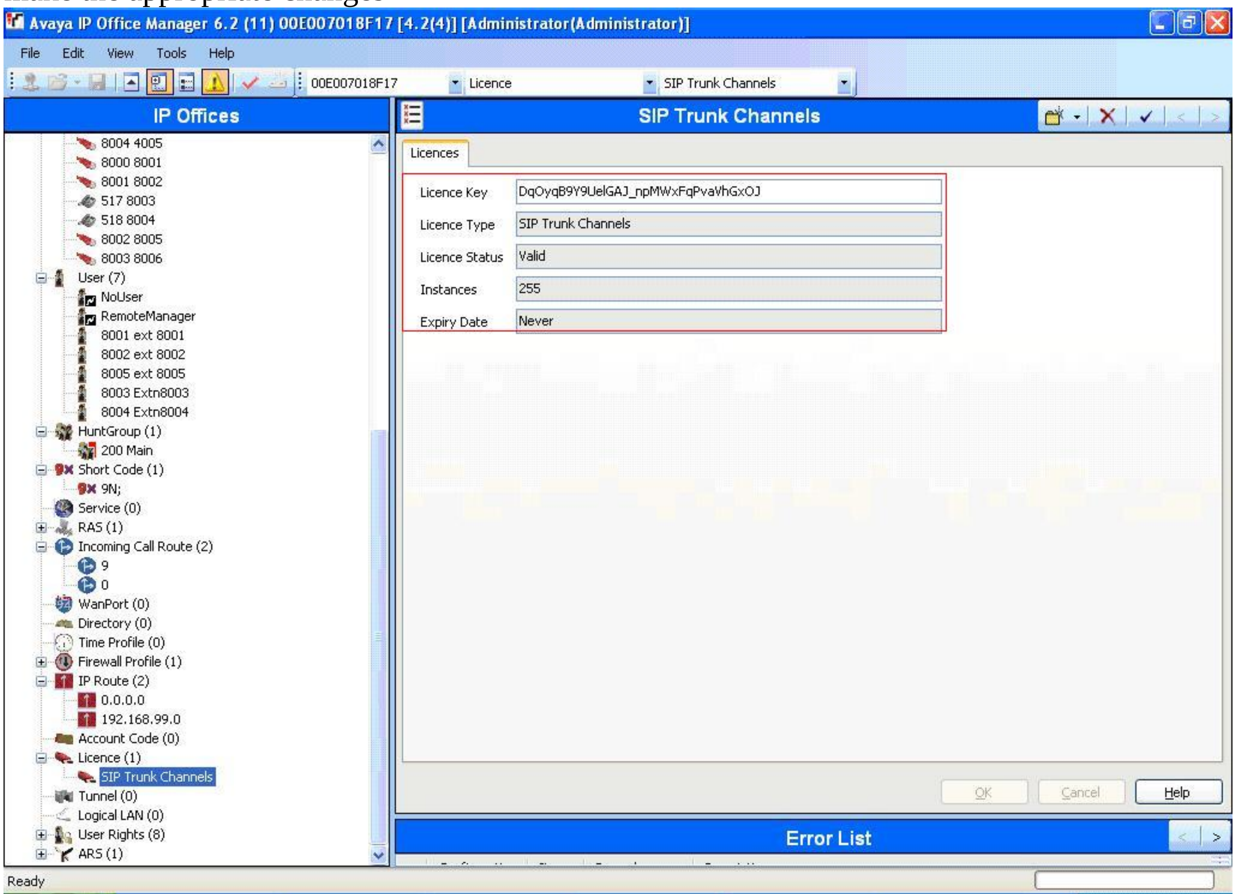
This section provides the procedures for configuring Avaya IP Office. The procedures include the following areas:

- Administer SIP Trunk License
- Administer Firewall
- Administer SIP Trunk
- Administer Users
- Administer Incoming Routing
- Administer Short Code and Gateway

IP Office is configured via the IP Office Manager program. Log into the IP Office Manager PC and select **Start →Programs→IP Office→Manager** to launch the Manager application. Log in to the Manager application using the appropriate credentials.

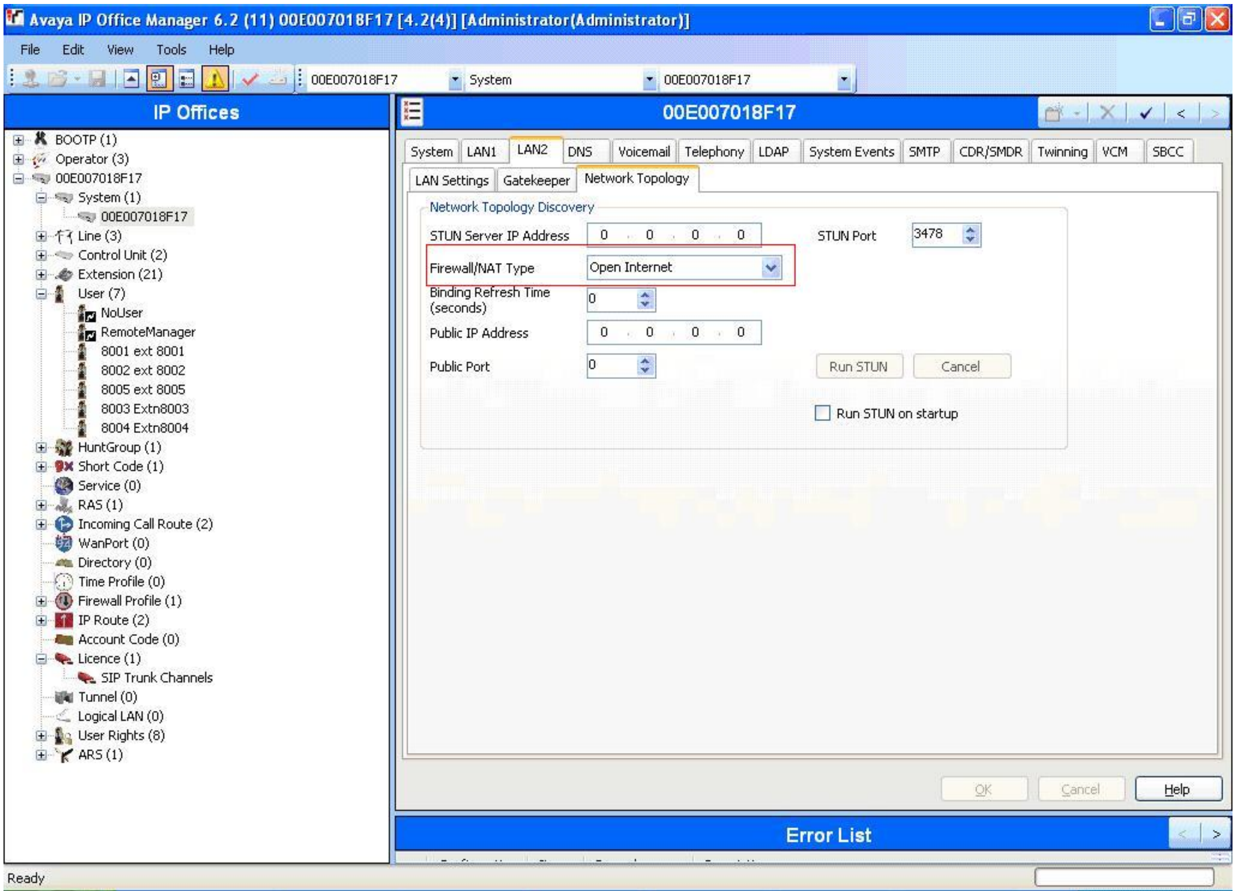
6.1. Administer SIP Trunk License

Verify that there is a SIP Trunk Channels License. Double-click on **Licence** in the left panel. Verify that there is a SIP Trunk Channels entry. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative or Business Partner to make the appropriate changes



6.2. Administer Firewall

In this sample configuration, **LAN2** is configured as IP Office IP Address. From the left panel click **System → LAN2 →** Network Topology select **Firewall=Open Internet**.

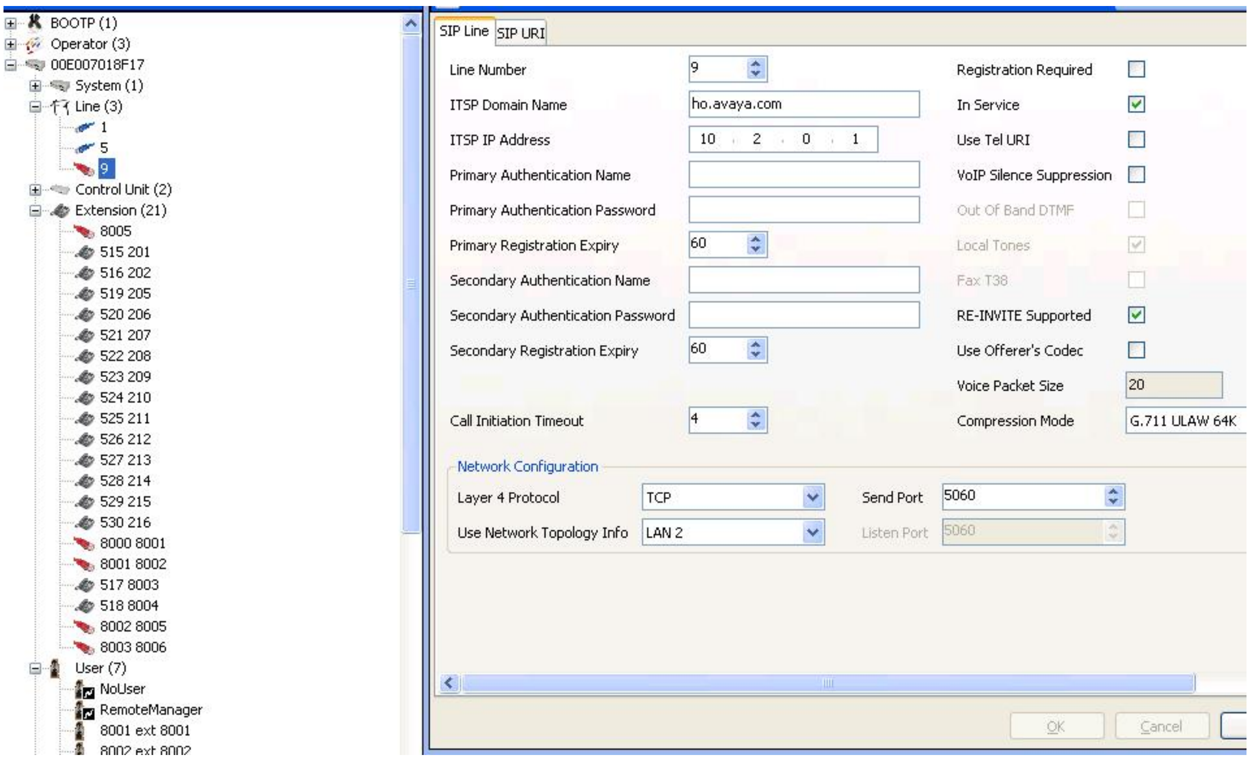


6.3. Administer SIP Trunk

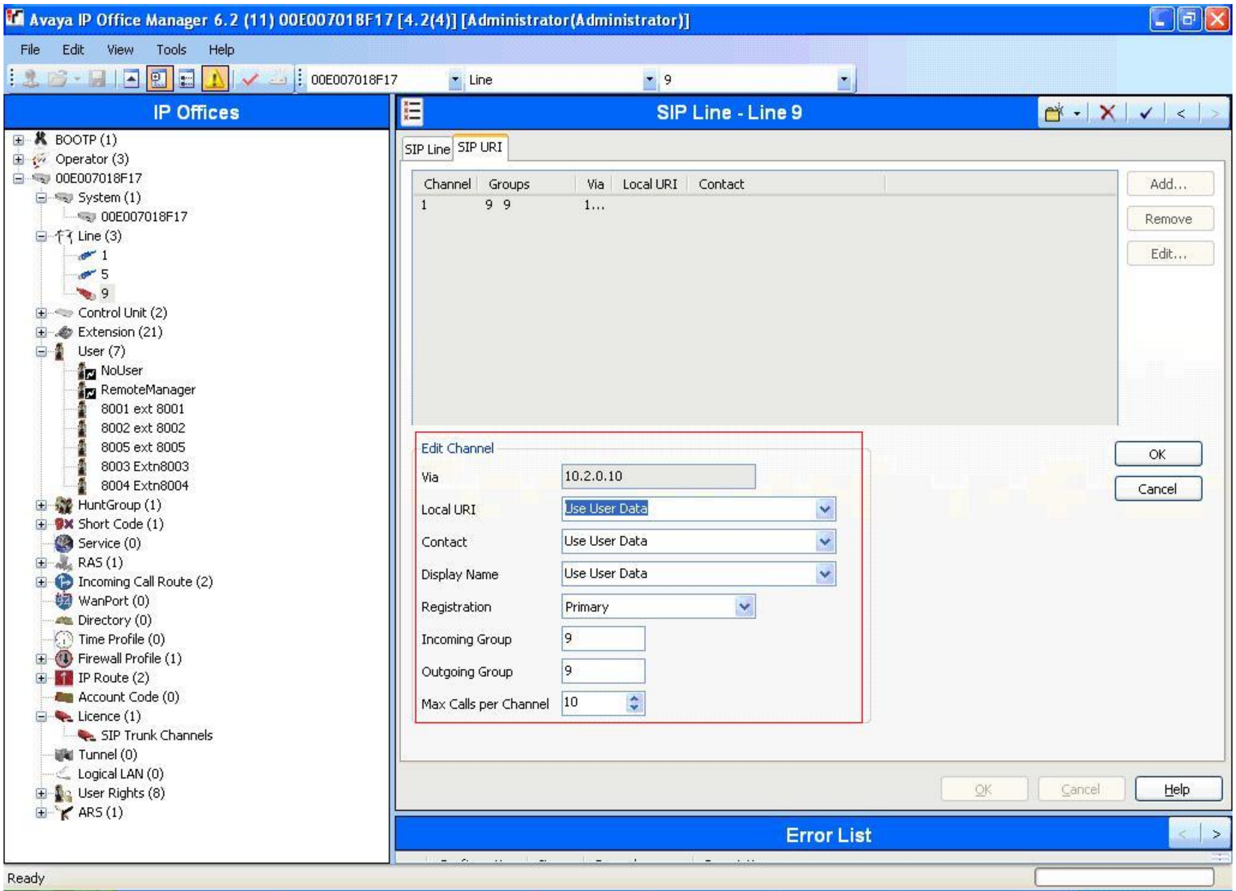
Create the SIP line for Avaya SES. Select **Line** in the left panel. Right-click and select **New →SIP Line** (Not shown). Enter the SIP Domain Name of Avaya SES in the **ITSP Domain Name** field. Enter the UM-Labs SSC RC 2100 Gateway IP Address in the **ITSP IP Address** field. In the Network Configuration section, select the following:

- **Layer 4 Protocol**, use **TCP**
- **Send Port**, use **5060**
- **Line Network Topology Info** use **LAN2**

The above values must match what is administered on Avaya SES. Select the appropriate **Compression Mode** to **G711 ULAW 64K**. This is required to match what was configured for the Codec Set in Avaya Communication Manager. Use default values for other fields.

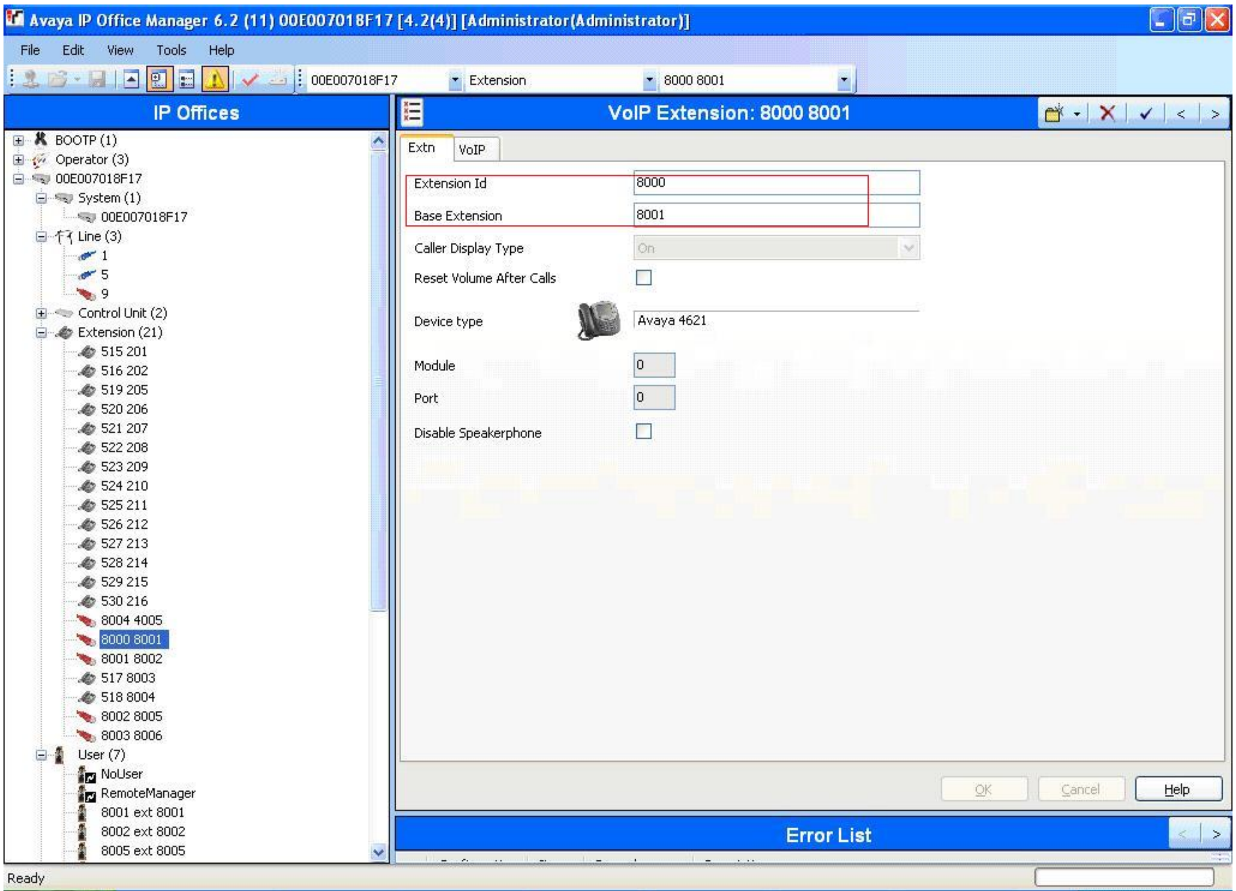


To configure URI parameters for the line, click on **Line** select the **SIP URI** Tab. Press the **Add** button. Select **Use User Data** for **Local URI**, **Contact,** and **Display Name.** Enter a unique number for the **Incoming Group** and **Outgoing Group** fields. Use default values for all other fields. Press the **OK** button.

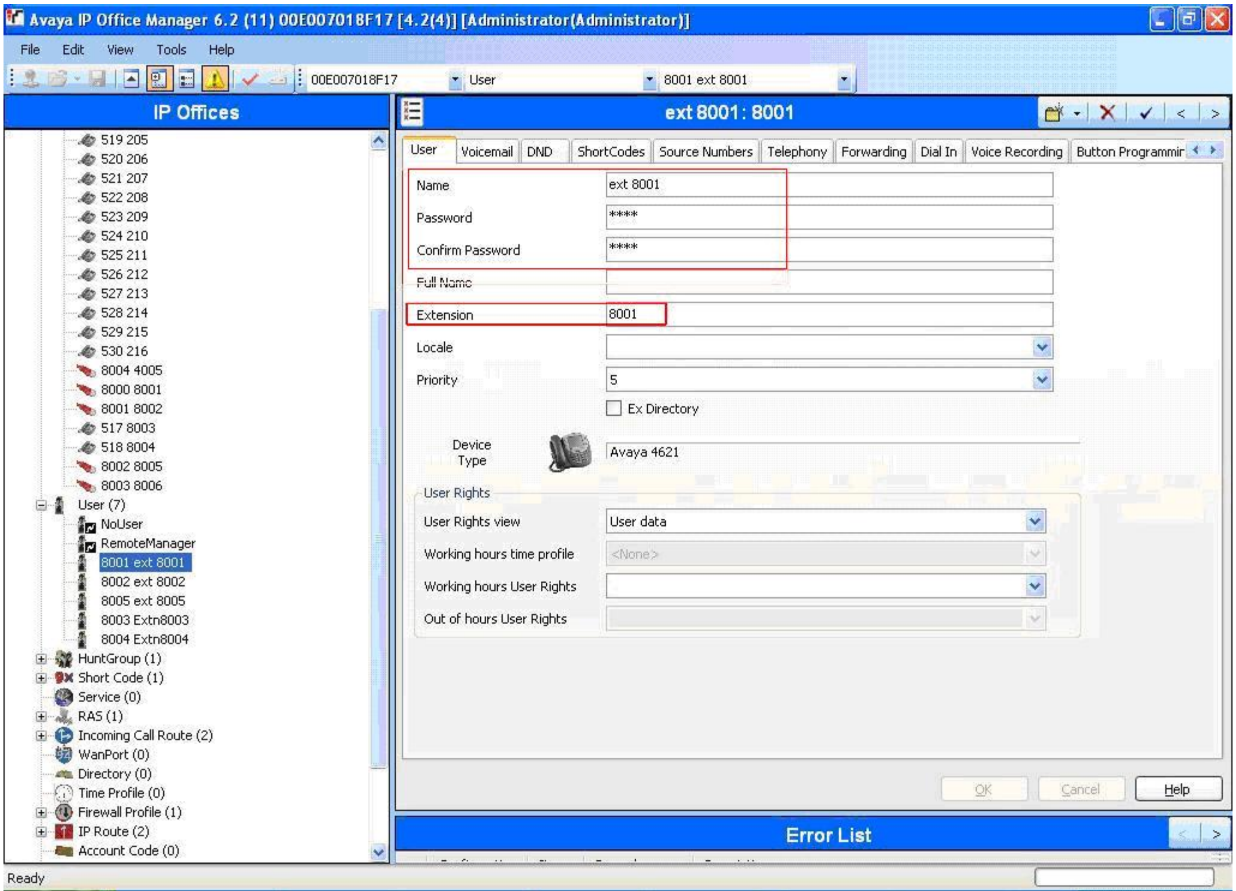


6.4. Administer Users

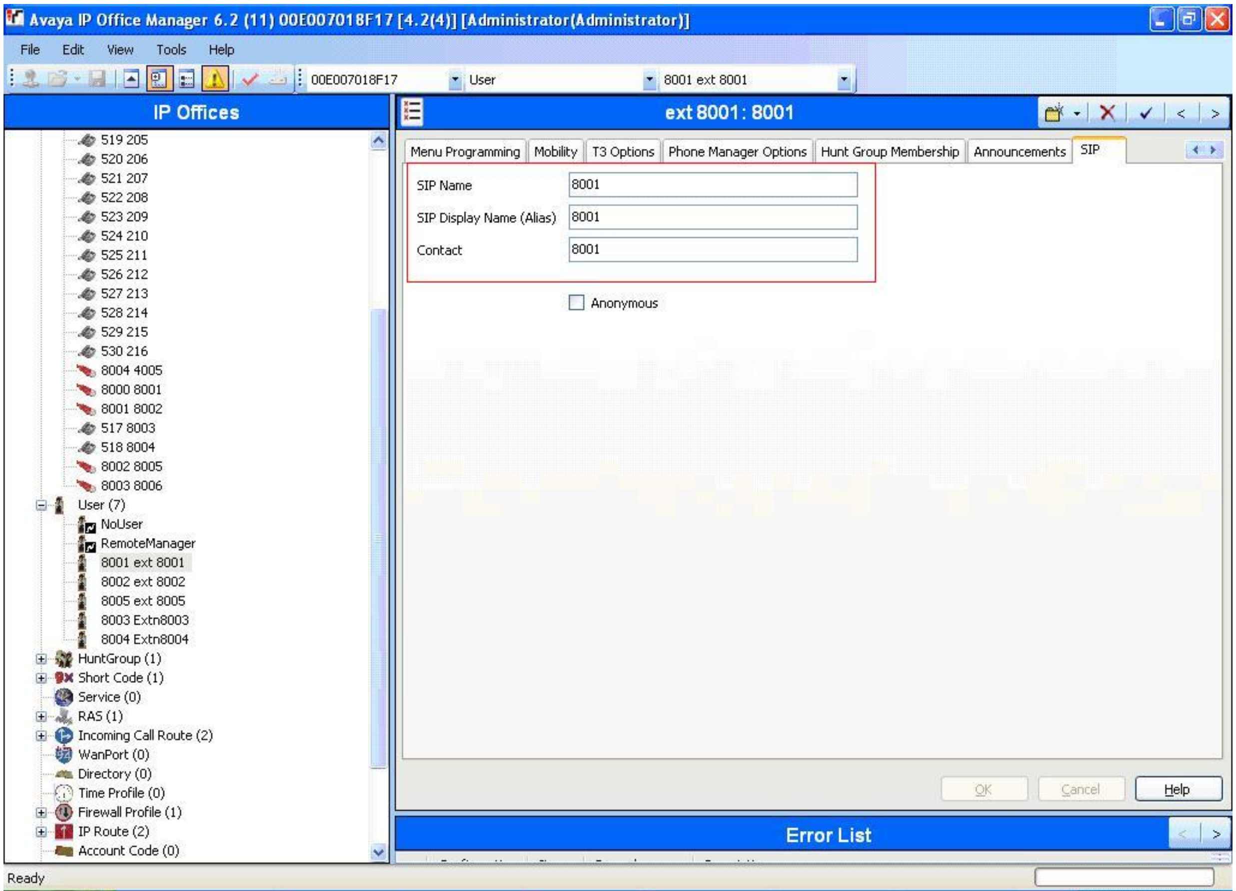
Create the VOIP Extensions to connect a H.323 end point to IP Office. Right click on the **Extension** and select **New →VOIP Extension**. Enter the details as shown in the sample configuration.



Create new user to connect a H.323 End Point to IP Office. Right click on **User** in the left panel, and select **New →User**. Enter the details as show in the sample configuration. Note this is a VOIP user.

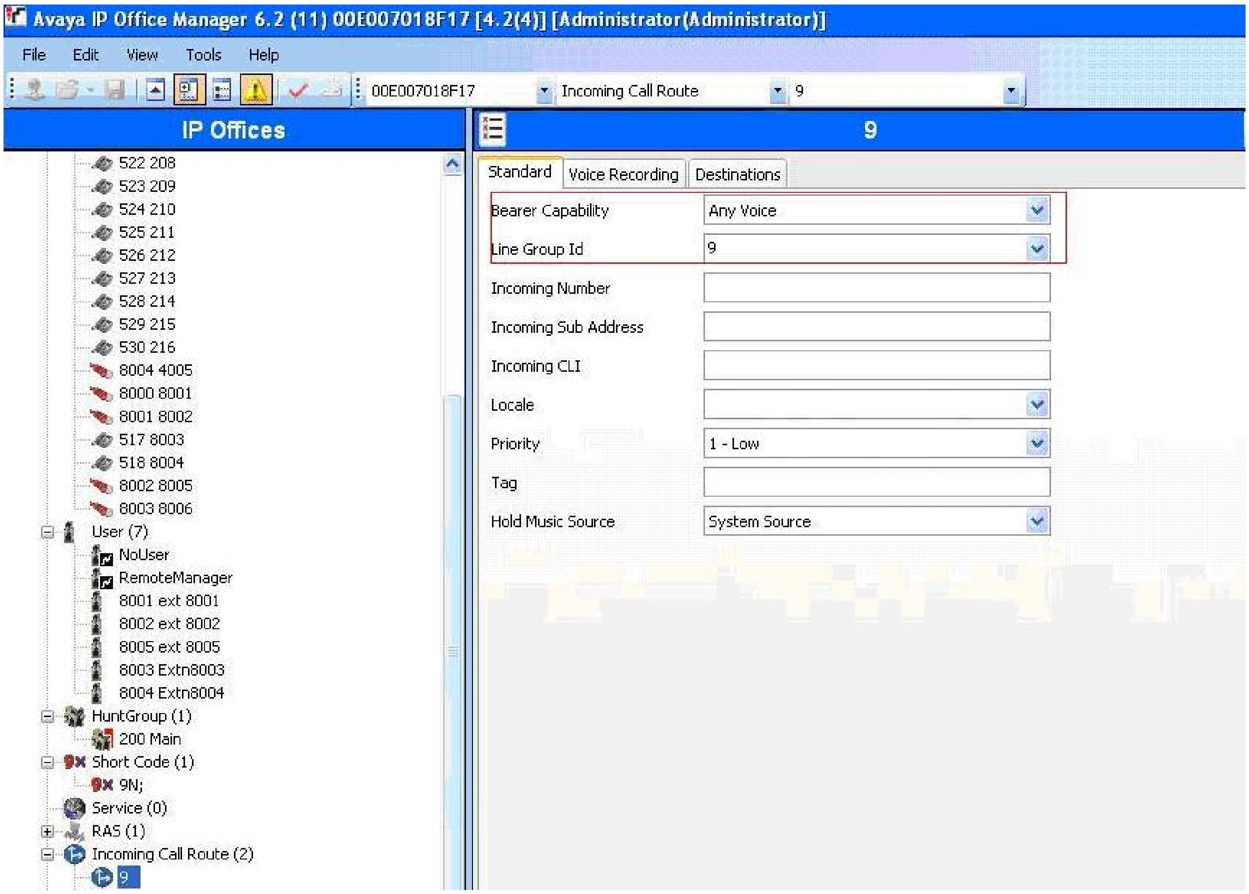


Navigate to the **SIP** tab for the user and enter the details as show in the sample configuration. This is for the VOIP user.

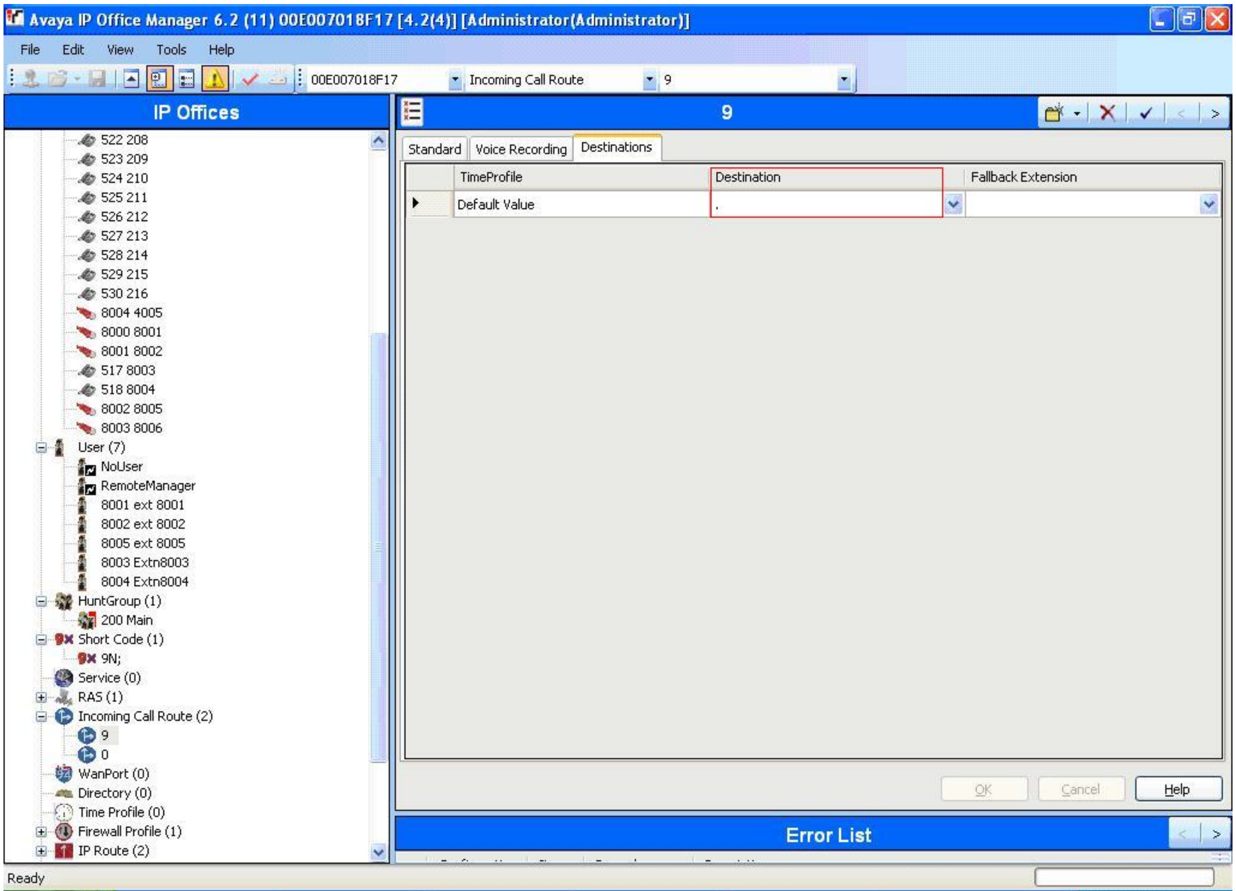


6.5. Administer Incoming Routing

Create an Incoming Call Route for the SIP calls. Select **Incoming Call Route** in the left panel. **Right-click** and select **New**. Click on the **Standard** tab, select **Any Voice** under **Bearer Capability** and enter the Incoming Group created for the URI in the **Line Group Id** field. Use default values for all other fields. Press the **OK** button (Not Shown).

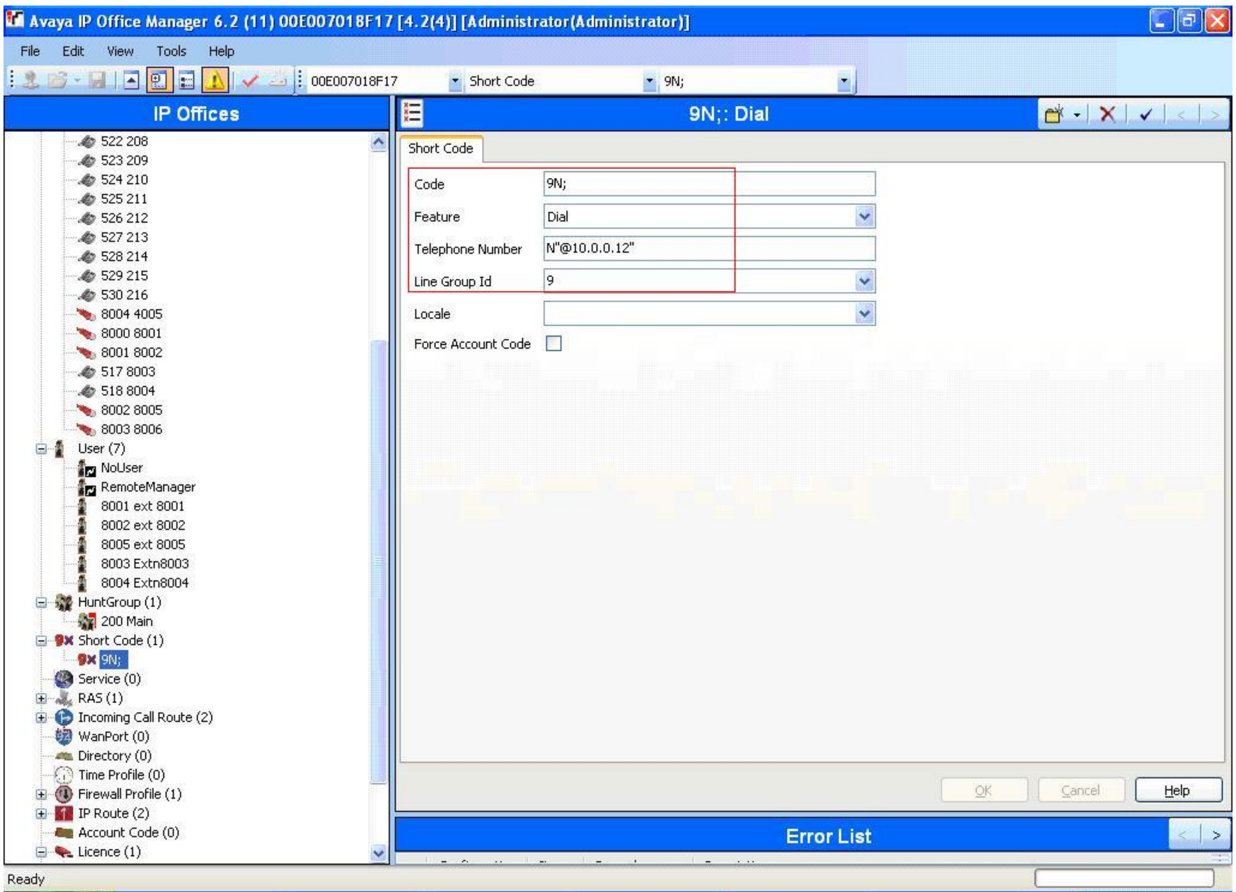


Select the Destination tab for the Incoming Call Route, and enter "." in the **Destination** field. Press the **OK** button (Not Shown).

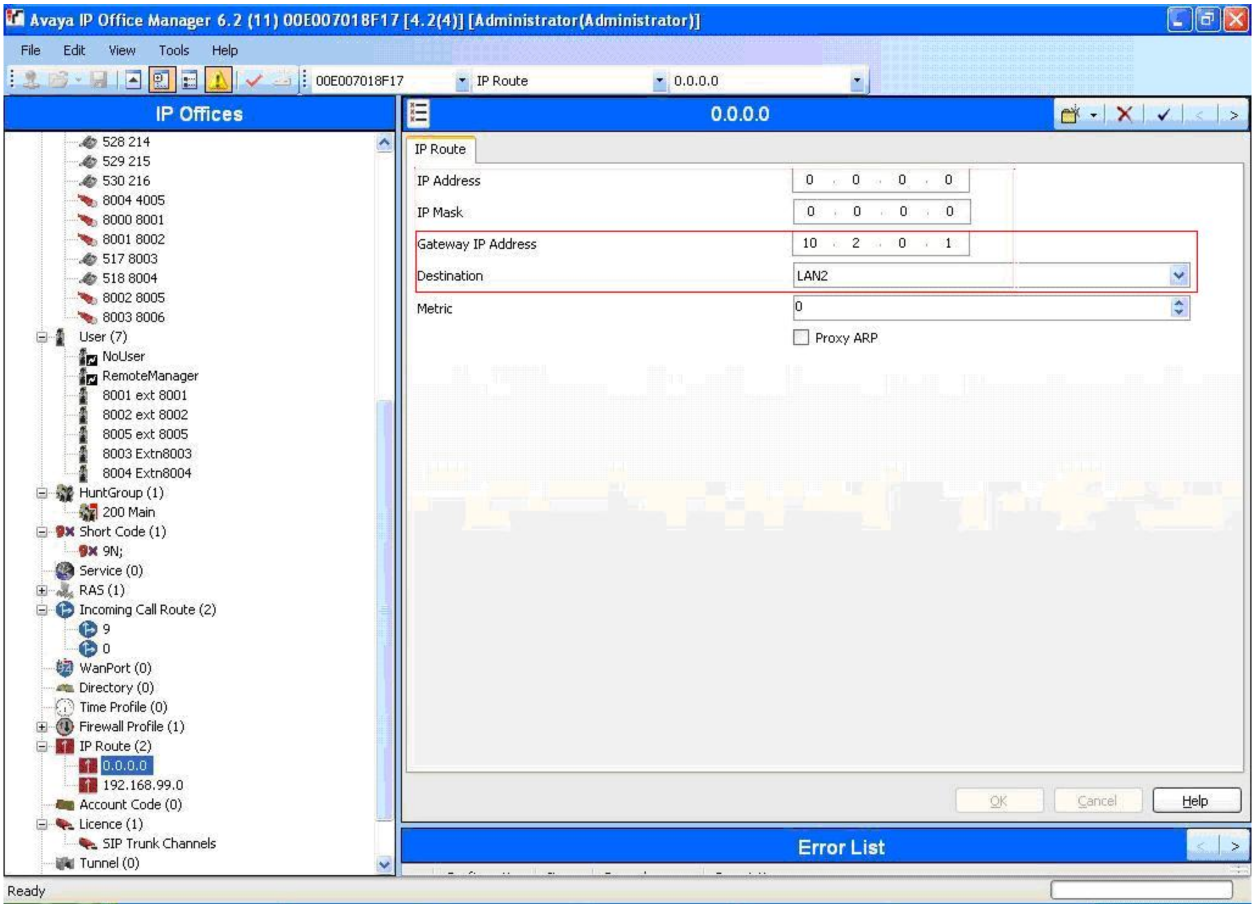


6.6. Administer Short Code and Gateway

Create a short code to route calls to Avaya Communication Manager via Avaya SES. Select **Short Code** in the left panel. **Right-click** and select **New**. Enter a unique code that ends with **9N;** for the **Code** field. Select **Dial** for the **Feature**. Enter the dialed number followed by (**N“@<ip address of SES server>**) for the Telephone Number field. This corresponds to the extension numbers that are administered on Avaya Communication Manager followed by 9. Enter the SIP line Outgoing Group ID created previously for the **Line Group Id**. Use default values for all other fields. Press the OK button.



Configure the Default Gateway on the IP Office by clicking **IP Route** in left panel and selecting the IP address of 0.0.0.0. Enter the gateway IP address in **Gateway IP Address** and select **LAN2** from the pull down menu for **Destination** as shown.



7. Configure the UM-Labs SSC EC4200 in Head Office

This section provides the procedures for configuring the EC4200 in the Head Office. The procedures include the following areas:

- Administer Initial Setup
- Administer License
- Administer Basic Configuration
- Administer SIP Routes
- Administer Save Configuration
- Verify Software Version

7.1. Administer Initial Setup

The EC4200 ships with a default IP address on interface eth0 of 192.168.1.1. For the purposes of this test, this default address was left unchanged. Other installations may choose to change this default to simplify subsequent configuration. Refer to the UM-Labs documentation for details.

For the purposes of the certification test, the RC2100 and EC4200 were linked on a test network using a private IP address. To simplify subsequent configuration the default IP address of interface eth0 on the RC2100 was changed to a different value from that of the EC4200. Other installations may pick a different default IP address.

Follow the quick start guide (Refer UM-Labs Website) to change the default IP of the EC4200 (192.168.1.1.) Configure the EC4200 from the GUI, connect to http://192.168.1.1, log in and change the password.

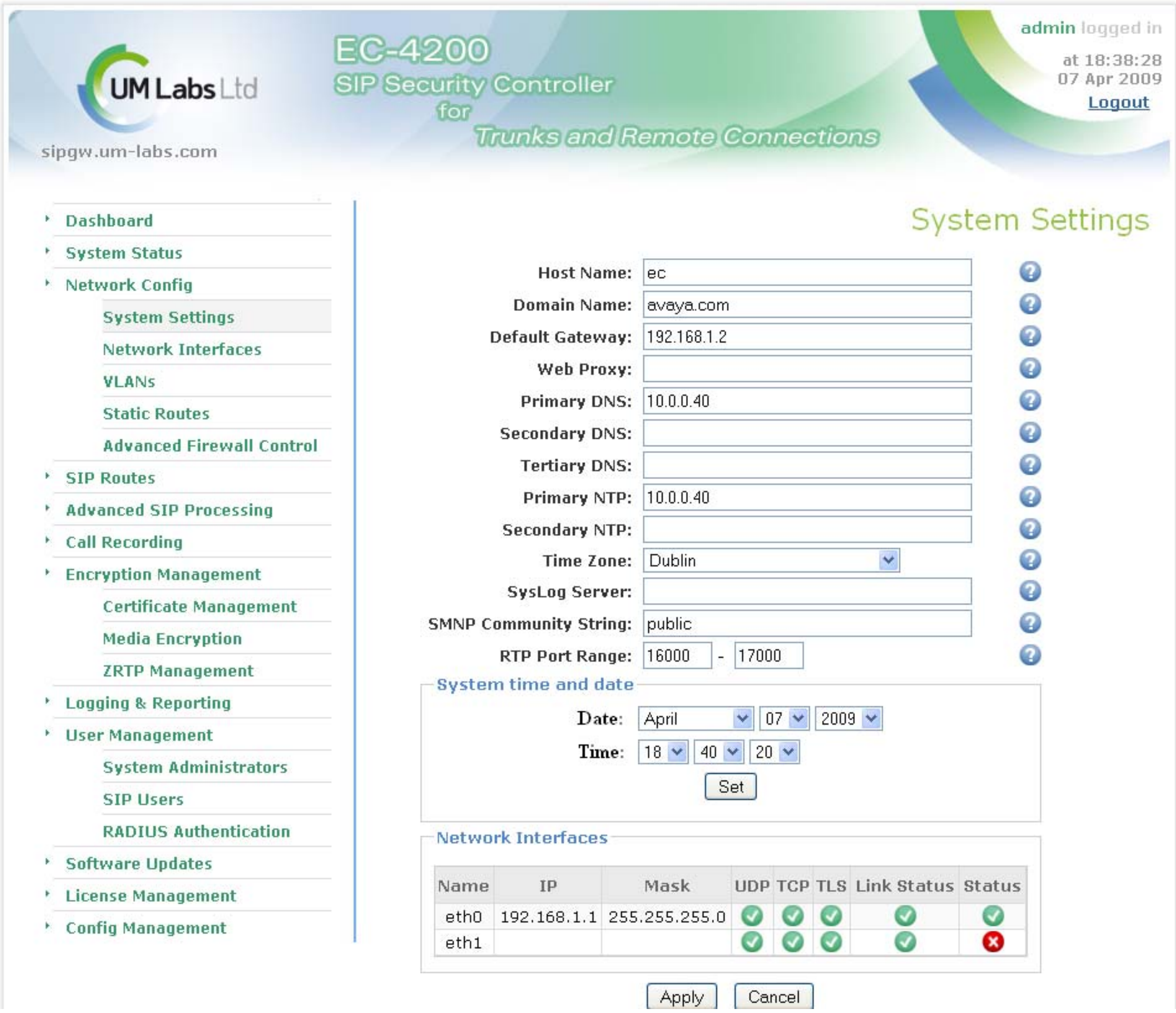
7.2. Administer License

For the very first time, log in using the above URL. Users need to Accept the license and change **admin password**, click on **Save**.

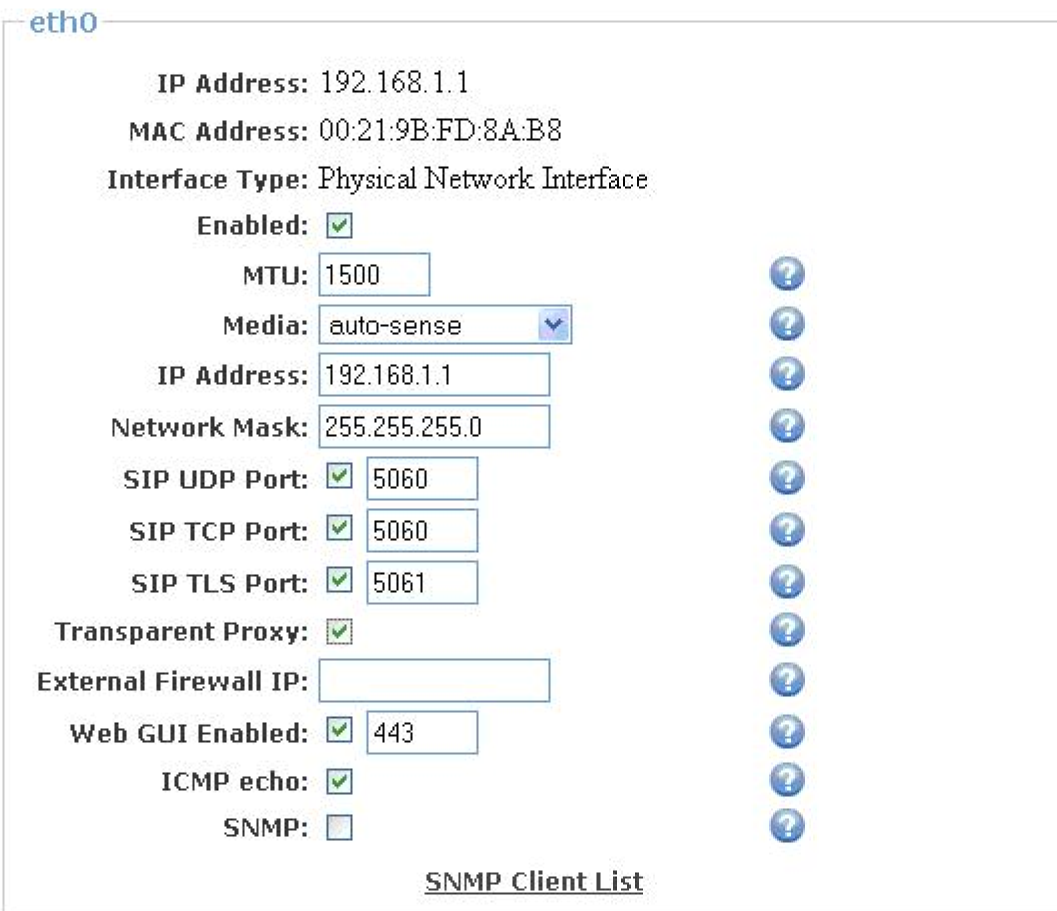
7.3. Administer Basic Configuration

From the left panel, click on **Network Config →System Settings**, enter the details for **Host Name, Domain Name, Default Gateway, Primary DNS,** and **Time Zone** as shown in the sample configuration.

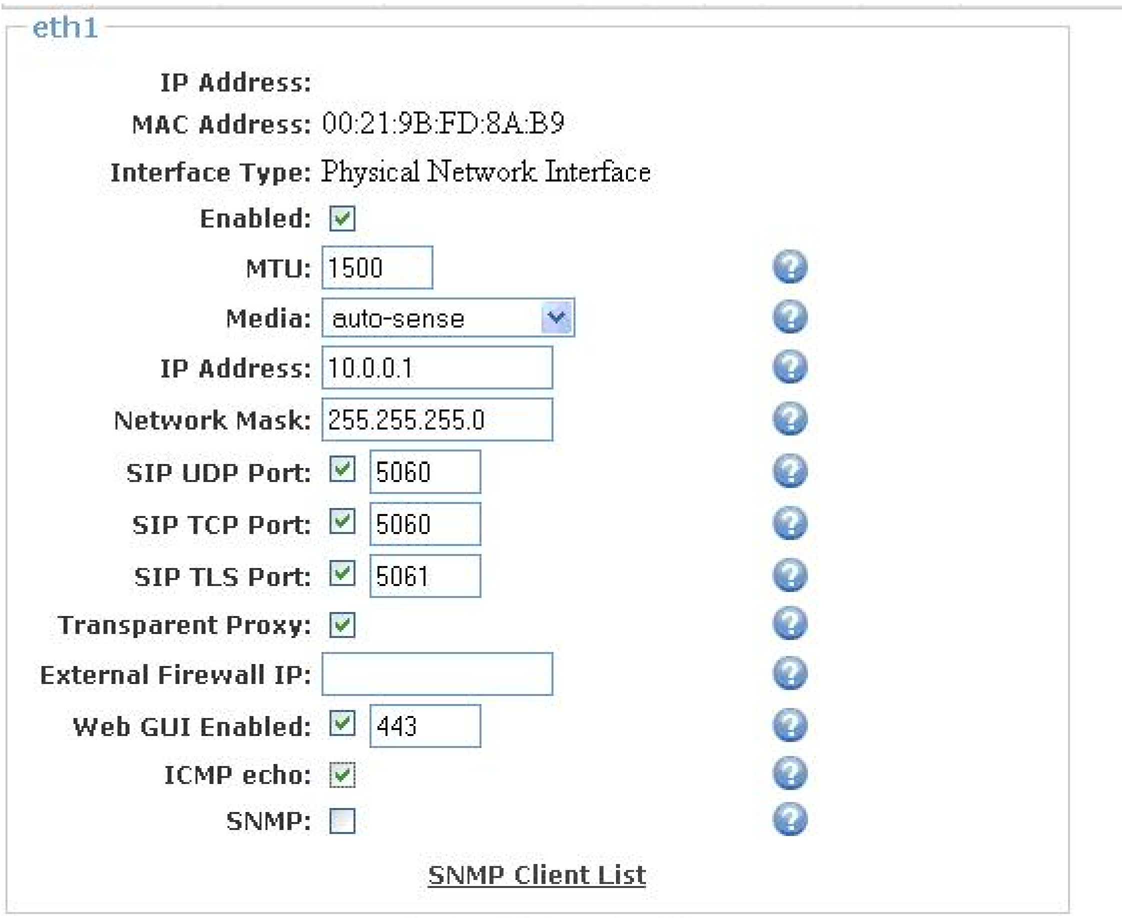
For the purposes of these tests, there was no operational NTP server on the test network and the Head Office Primary DNS was used as the NTP server. For live installations it is strongly recommended that at least one valid NTP server is configured. Refer to the UM-Labs documentation for details. To save these changes, click on **Apply**.



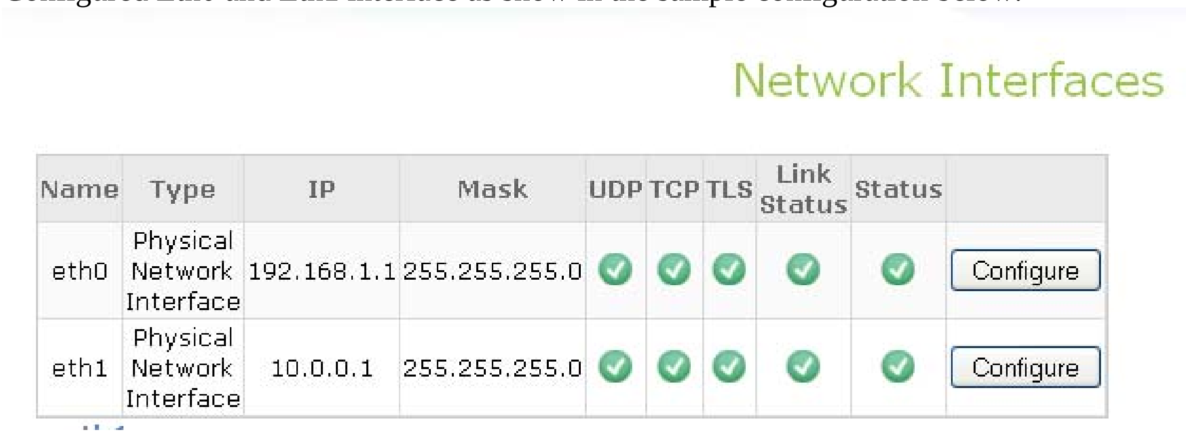
From the left panel, choose **Network Config** and click on **Network Interfaces and select Eth0.** Configure the IP Address as **192.168.1.1** (Link to HO). Set each Interface to **Transparent Proxy.** Enable **Ping and Web Admin (Not Shown)**. Click Apply.



To configure the IP Address for the **eth1**, click on **Network Interfaces** configure **eth1 10.0.0.1**(Head Office). Set each Interface to **Transparent Proxy.** Enable **Ping** and **Web Admin** (Not Shown). To save these changes, click on **Apply** not shown in this screen shot.



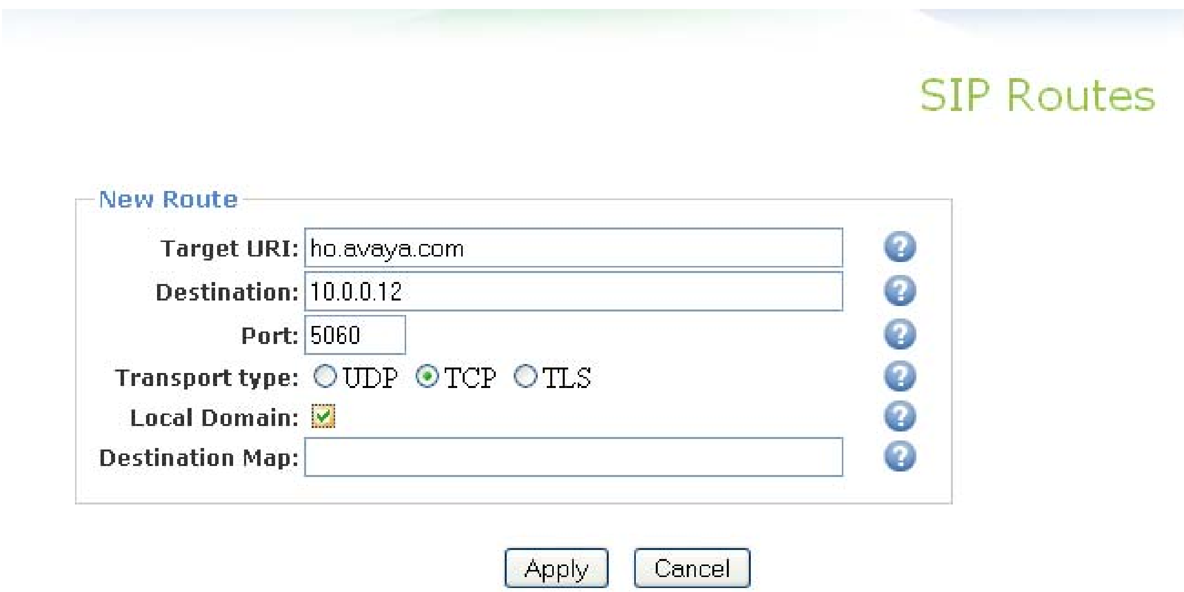
Configured Eth0 and Eth1 interface as show in the sample configuration below.


Network Interfaces

Name	Type	IP	Mask	UDP	TCP	TLS	Link Status	Status	
eth0	Physical Network Interface	192.168.1.1	255.255.255.0						Configure
eth1	Physical Network Interface	10.0.0.1	255.255.255.0						Configure

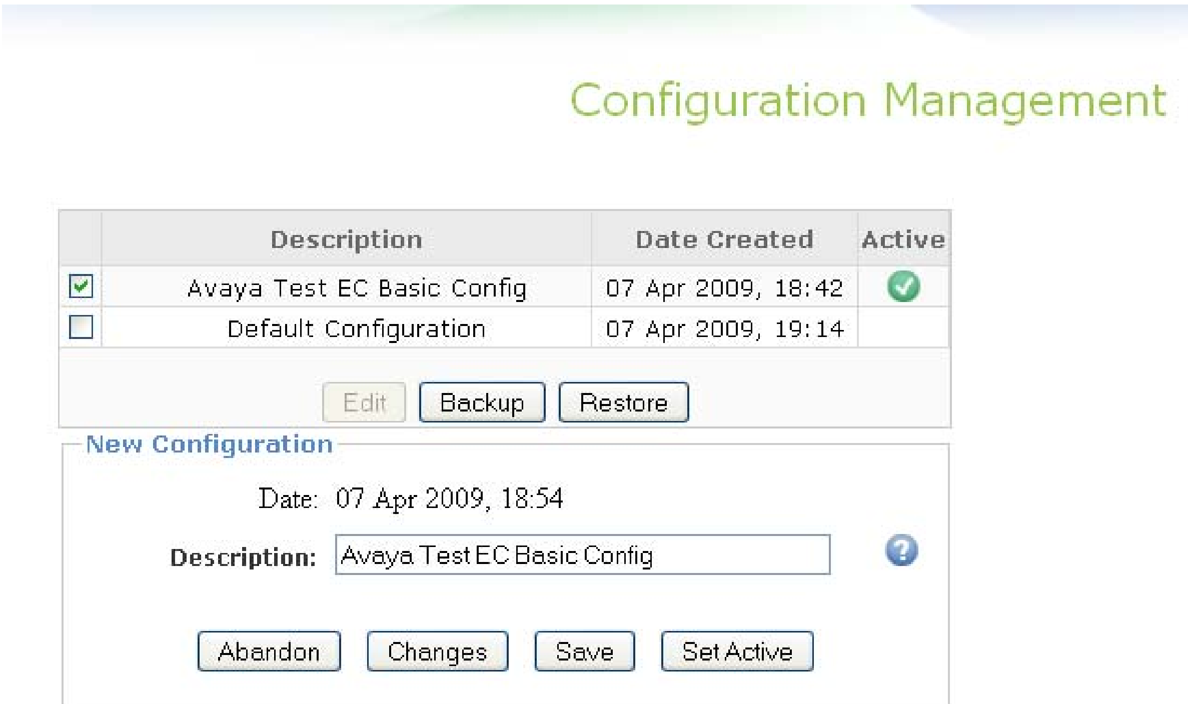
7.4. Administer SIP Routes

Click on **SIP Routes** in the left hand panel, add routes for Head Office. Make all routes local domain by enabling **Local Domain**. Set **Transport Type** between Avaya systems and EC4200 as TCP. UDP was used in tests to enable local diagnostics. Note that setting the domains as local in each SIP route ensures that there are no restrictions on the call flow between the two test sites. Other installations may require a more restrictive call flow policy. Refer to the UM-Labs documentation for more information (Refer Section 1.2).



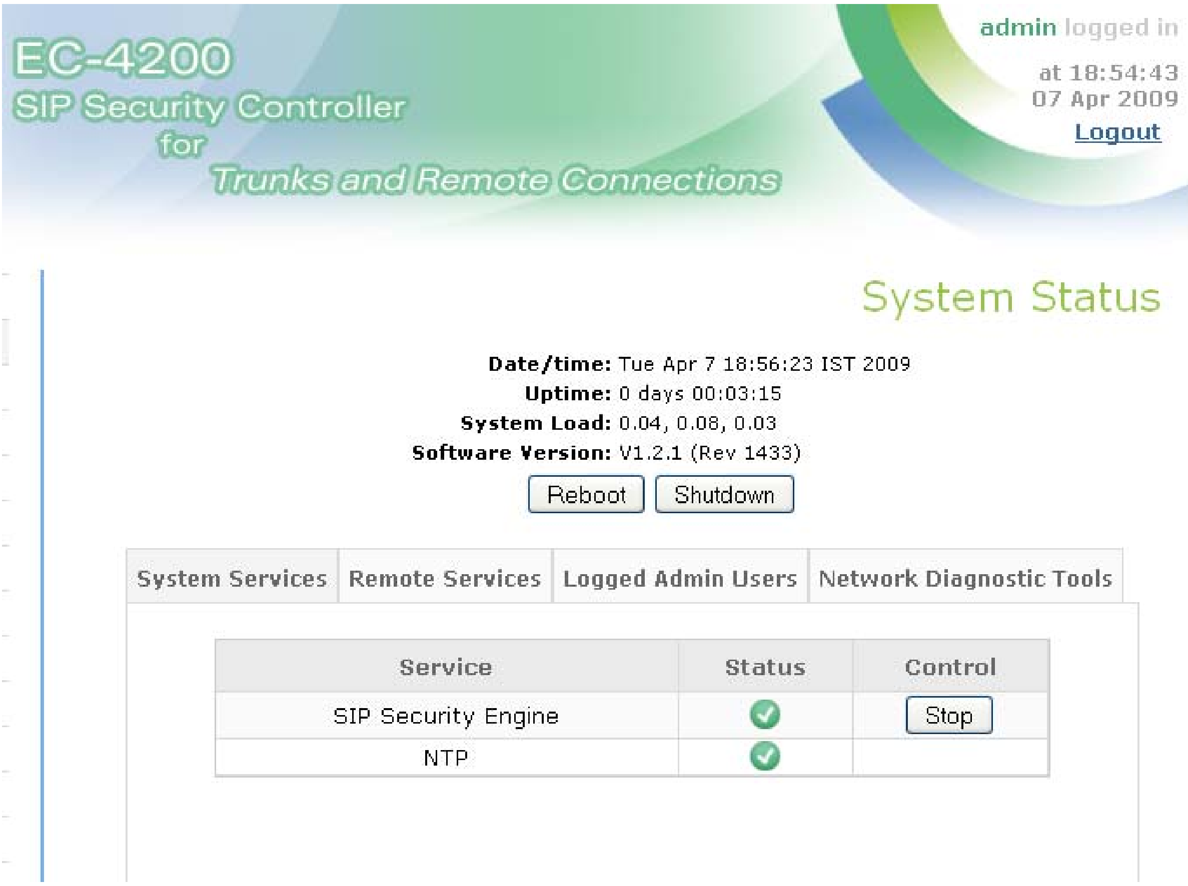
7.5. Administer Save Configuration

To save the above configuration, click on the **Configuration Management** from Home Page and enter **Description** of the configuration. Click **Save** and then click on **Set Active**. Next, a Reboot page is displayed. Click **Reboot** to make the configuration active (not shown).



7.6. Verify Software Version

To verify Software version, click on **System Status**.



8. Configure the UM-Labs RC2100

This section provides the procedures for configuring RC2100 in Branch Office. The procedures include the following areas:

- Administer Initial Setup
- Administer License
- Administer Basic Configuration
- Administer SIP Routes
- Administer Save Configuration
- Verify Software Version

8.1. Administer Initial Setup

For the purposes of the certification test, the RC2100 and EC4200 were linked on a test network using a private IP address. To simplify subsequent configuration the default IP address of interface eth0 on the RC2100 was changed to a different value from that of the EC4200. Other installations may pick a different default IP address.

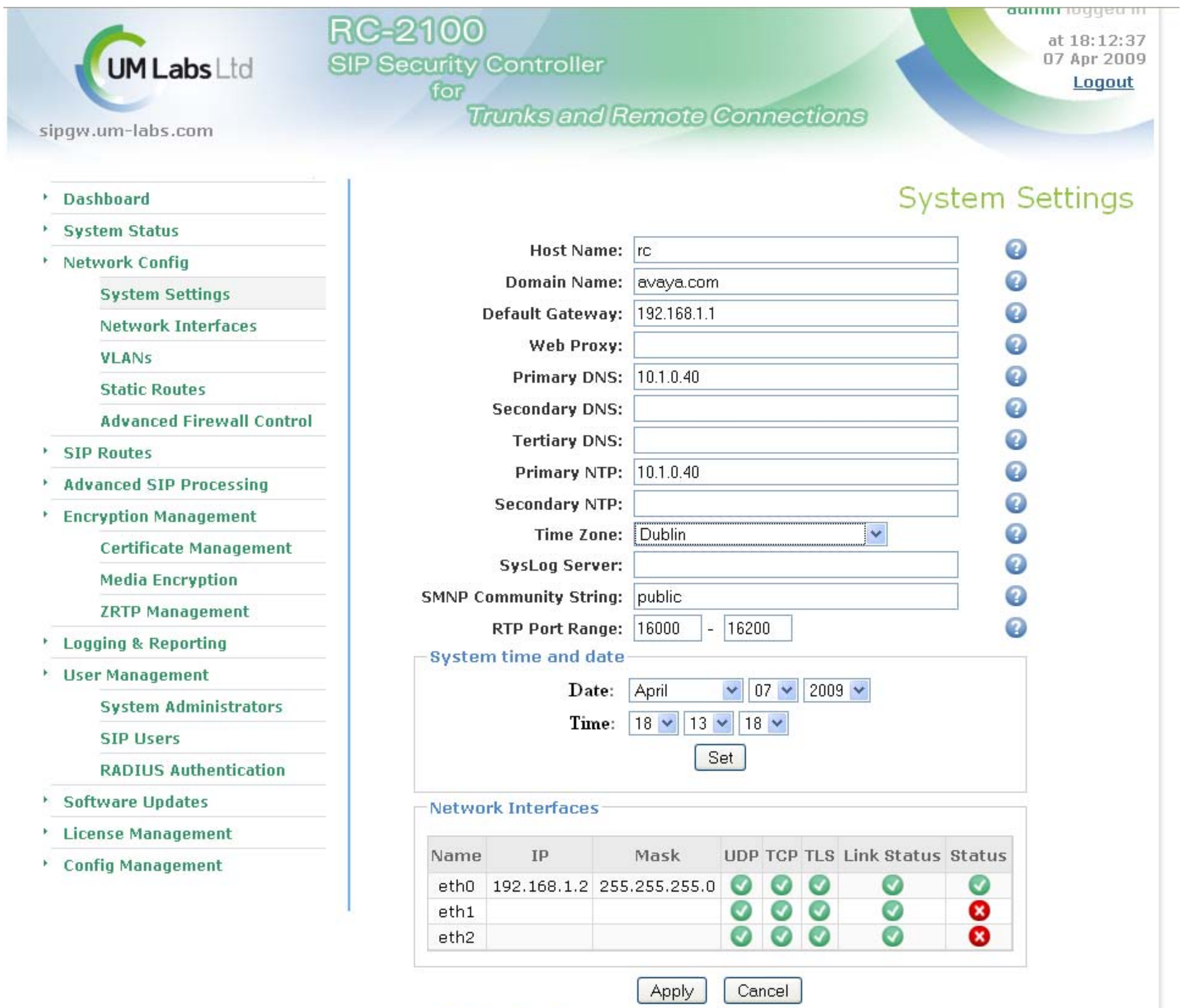
Follow the quick start guide (refer UM-Labs Website at http://www.um-labs.com/documentation.php) to change the default IP of the RC2100 (192.168.1.2.) To configure the RC2100 from the GUI, connect to http://192.168.1.2 and log in with the appropriate login credentials.

8.2. Administer License

For the very first time, log in using the above URL. Users need to Accept license and change **admin password**, click on **Save**

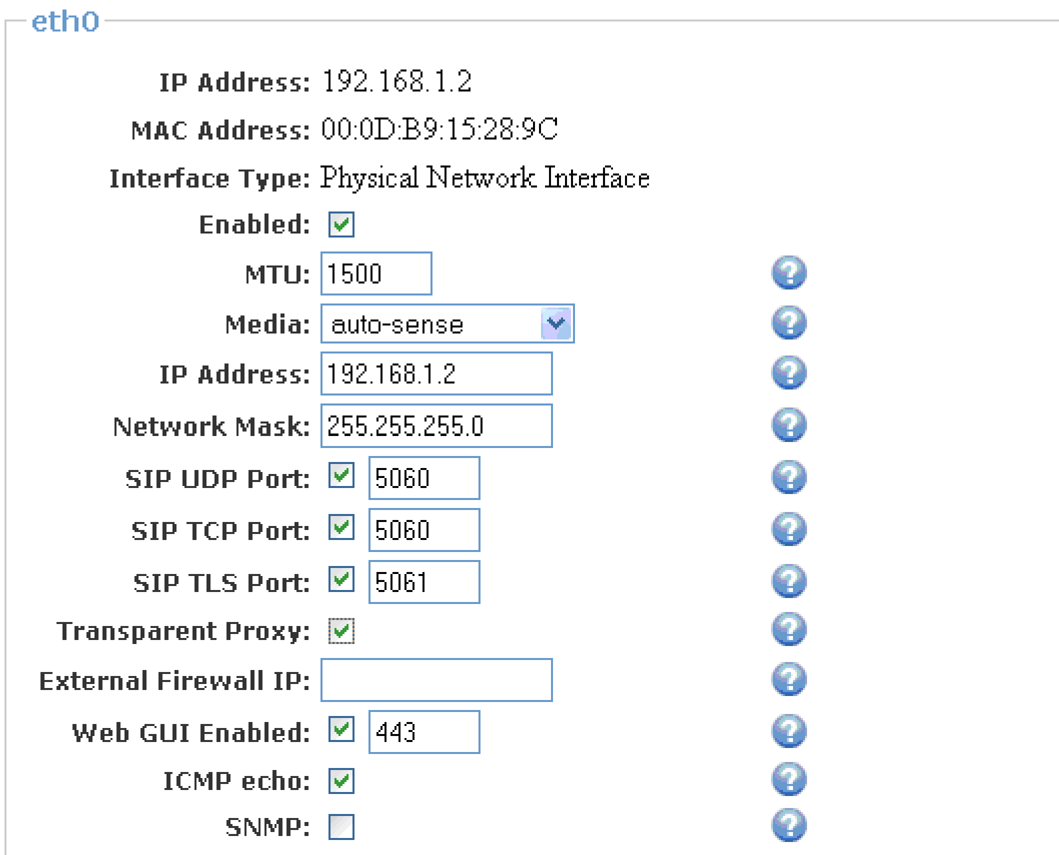
8.3. Administer Basic Configuration

From the left panel click **Network Config →System Settings**, enter the details for **Host Name, Domain Name, Default Gateway, Primary DNS,** and **TimeZone** as show in the sample configuration. For the purposes of these tests, default Branch Office Primary DNS was NTP server in this configuration as there was no operational NTP server on the test network. For live installations it is strongly recommended that at least one valid NTP server is configured. Refer to the UM-Labs documentation for details.

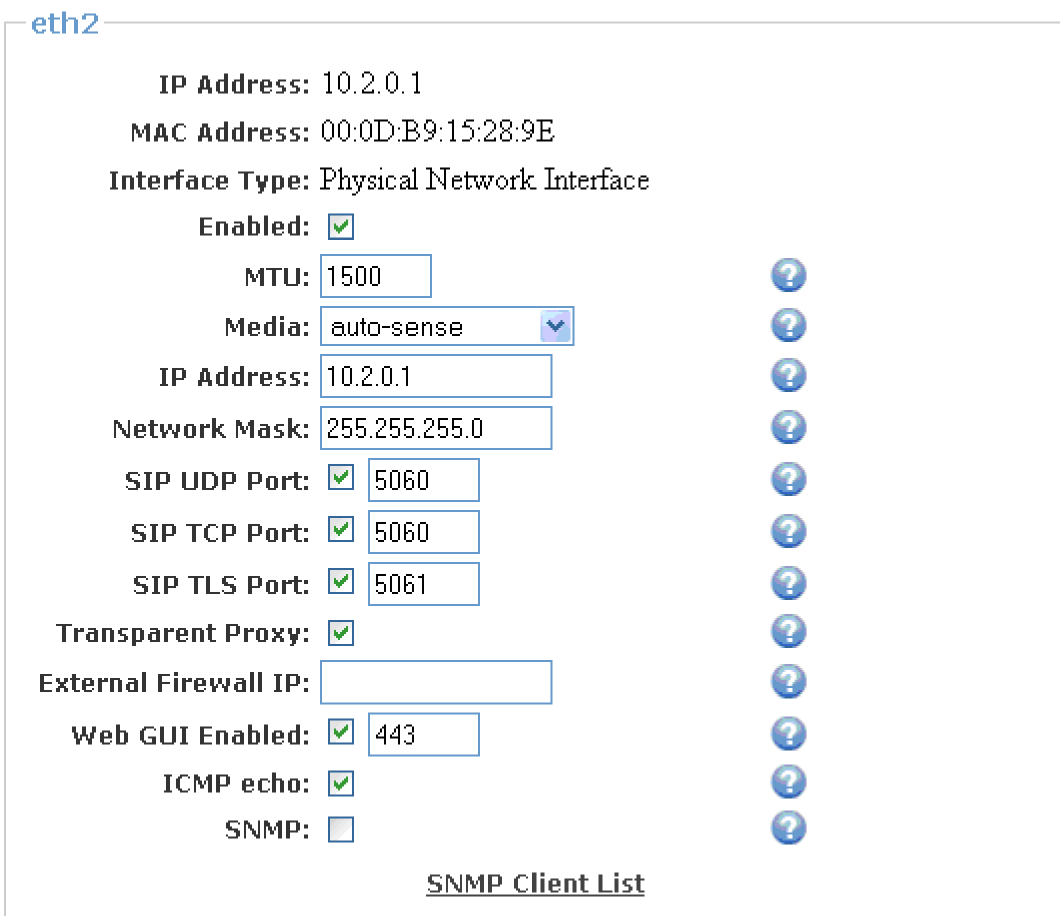


Click on **Apply**.

Click **Network Config →Network Interfaces,** and configure the IP Addresses of **eth0** as **192.168.1.2** (Link to Head Office). Set each Interface to **Transparent Proxy.** Enable **Ping** and **Web Admin** as needed (Not Shown).

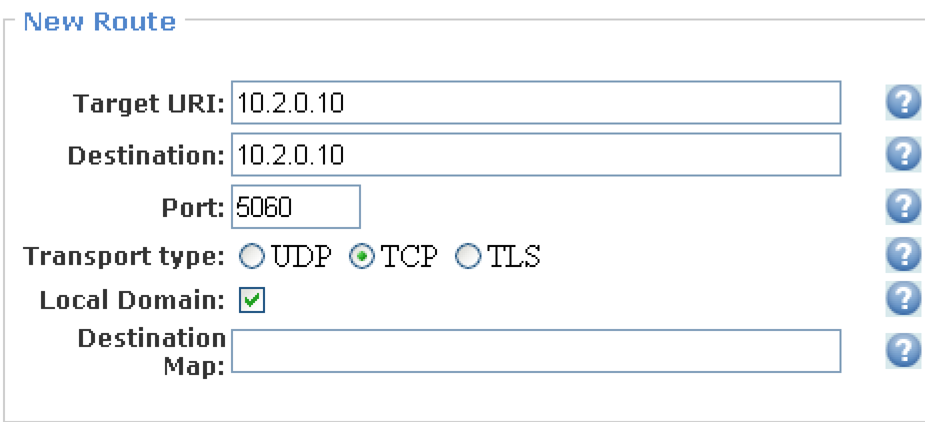


Select **Network Interfaces**, configure IP Address of **eth2 as 10.2.0.1** (Interface to IP Office). Set each Interface to **Transparent Proxy.** Enable **Ping** and **Web Admin** as needed (Not Shown). Click Apply.



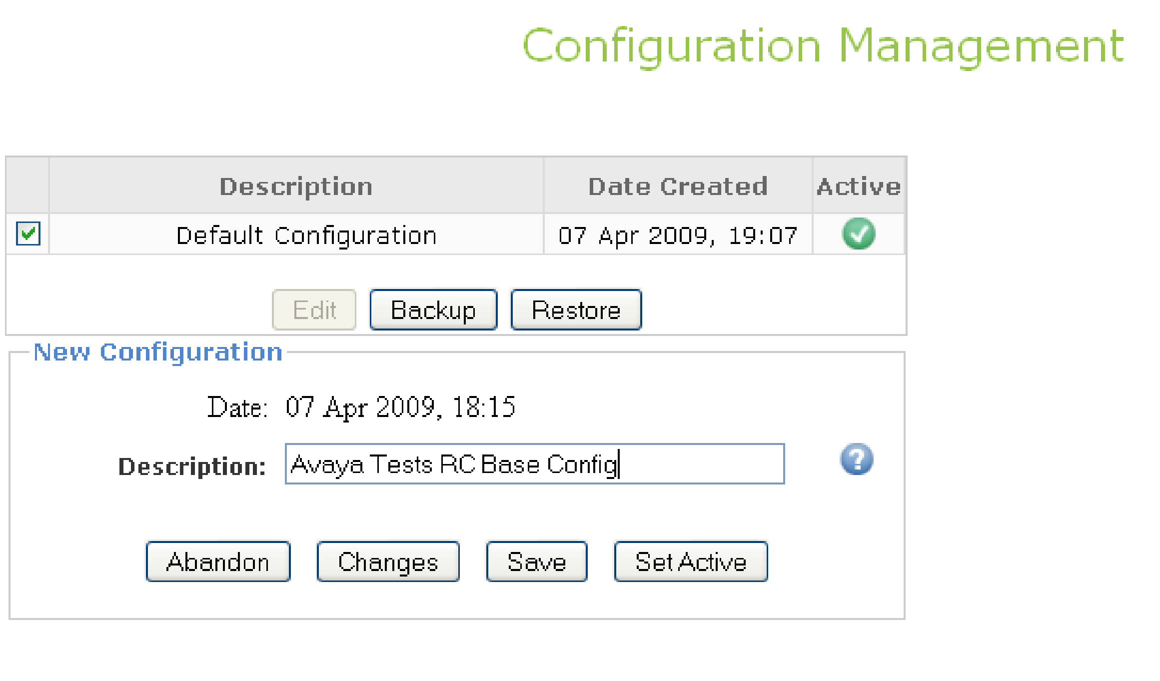
8.4. Administer SIP Routes

Click on **SIP Routes** in the left hand panel, add routes for IP Office. Make all routes local domain by enabling **Local Domain**. Use TCP transport between Avaya systems and RC2100. Note that setting the domains as local in each SIP route ensures that there are no restrictions on the call flow between the two test sites. Other installations may require a more restrictive call flow policy. Refer to the UM-Labs documentation for more information.
Click on **Apply** for each route.



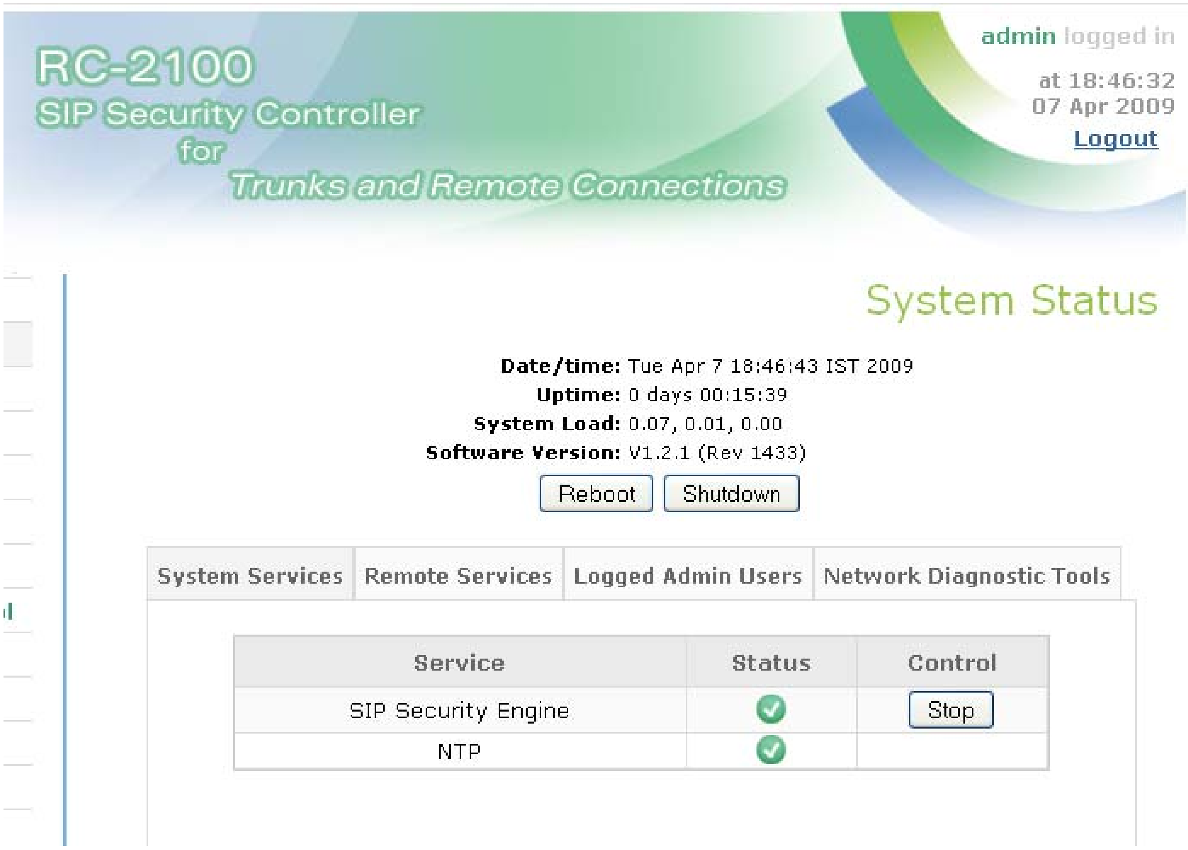
8.5. Administer Save Configuration

To save the above configuration, click on the **Configuration Management.** Enter a configuration **Description. C**lick **Save** and then click on **Set Active**. Next, a Reboot page is displayed. Click **Reboot** to make the configuration active (not shown).



8.6. Verify Software Version

To verify the software version, click on **System Status** in the left panel.



9. General Test Approach and Test Results

In this test configuration, a real time deployment scenario was simulated with UM–Labs SSC sitting on each office. All the signaling and RTP was through SSC using TCP.

10. Verification Steps

Verification and troubleshooting steps between UM-Labs SSC, Avaya IP Office, Avaya Communication Manager and Avaya SIP Enablement Services.

- Place a call from an extension on the Avaya IP Office to an extension on Avaya Communication Manger. Answer the call and verify talk path.
- Repeat previous case in the opposite direction.
- Verify that calls can be transferred from an extension on Avaya IP Office to an extension on Avaya Communication Manager.
- Verify that calls can be transferred from an extension on Avaya Communication Manager to an extension on Avaya IP Office.
- Verify that extensions on Avaya IP Office can conference in extensions on Avaya Communication Manager.
- Verify that extensions on Avaya Communication Manager can conference in extensions on Avaya IP Office.
- To verify Home Page →SIP routes page shows status (UDP links only, i.e. between RC2100 and EC4200.)
- To verify UM-Labs SSC logs, go to Home Page→ **Logging and Reporting** to view logs. To enable full packet trace (for diagnostics only), check **Enable SIP Packet Trace**, click **Apply**, save **Config** and **Reboot.**
- To verify logs from Avaya Communication Manager, use **SAT**, enter **list trace tac n**, where TAC is used for the trunk group created on the Avaya Communication Manger to Avaya SES and IP Office **.**
- Verify logs from Avaya IP Office. Avaya IP Office can be traced with **System Status Application**. Log into the IP Office Administration PC and select **Start→Programs → IP Office→System** Status to launch the application. In this tool, double click on **Trunks** entry and select trunk created and Press **Trace All** button. The messages on the line are displayed.
- To verify logs on Avaya SES, use command line trace called **traceSES**.

11. Conclusion

The Interop between UM-Labs SSC RC2100 and EC4200 and Avaya Communication Manager, IP Office and SIP Enablement Services has passed.

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.