Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a UM Labs SIP Security Controller EC-4200 with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe how to configure a UM Labs SIP Security Controller EC 4200 between an Avaya Head Office and Branch Office. Each site has an Avaya Communication Manager and Avaya SIP Enablement Services, and all communication between the sites passes through the UM Labs EC-4200.

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 a UM Labs SIP Security Controller (SSC) EC 4200 between a Head Office and a Branch Office. The configuration described in these Application Notes focuses on UM Labs SSC's handling of SIP messages and RTP between the Branch Office and Head Office.

The *SIP Security Controller (SSC)* is a security gateway 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 controller will relay calls between the service provider's core systems and customer connections.

The shipped appliance 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 Security Controller 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 signalling 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 will automatically encrypt the SIP. 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 on UM Labs SIP Security Controller EC 4200 between an Avaya Head Office and Branch Office. Testing verified Point–to-Point calls and telephony feature like hold, transfer and conferencing. The transport method used between Avaya and UM Labs was UDP.

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 the test configuration of UM Labs SSC and Avaya Solution.

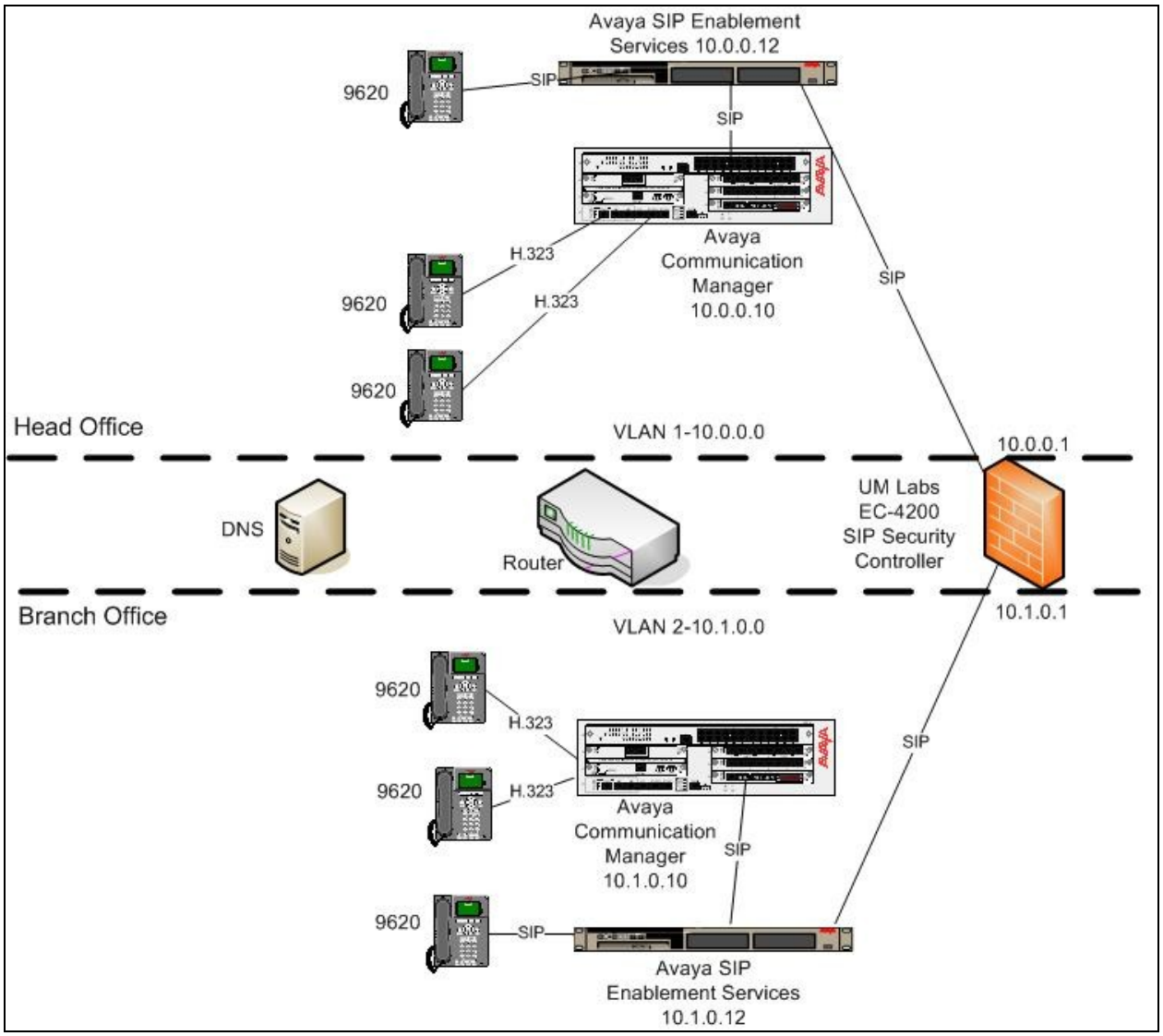


Figure 1: Network Configuration Diagram

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8300 Server Avaya G350 Media Gateway	Avaya Communication Manager 5.1.1 SP1 01.1.415.1-16988 28.22.0
Avaya S8300 Server Avaya G350 Media Gateway	Avaya Communication Manager 5.1.1 SP1 01.1.415.1-16988 28.22.0
Avaya SIP Enablement Services S8500B	SES05.1.1-01.1.415.1
Avaya one-X® Deskphone 9600-Series Phones (H.323)	2_9
Avaya one-X® Deskphone 9600-Series Phones (SIP)	2_0_4_0
UM Labs SIP Security Controller (EC-4200)	1.4 -1887

4. Configure Avaya Communication Manager

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

- Verify Communication Manager License
- Administer IP Node Name for 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 Communication Manager license has proper permissions for features illustrated in these Application Notes. If not, contact the Avaya sales team or business partner for a proper license file.

Using the SAT, verify that the Off-PBX Telephones (OPTIM) 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 OPTIM 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
HeadOffice_SES          10.0.0.12
default                 0.0.0.0
procr                   10.0.0.10

( 4  of 4    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 Head Office and Branch Office Dial Plan

Enter the **change dialplan analysis** command. Add an entry for local **ext** (extension), **dac** and **aar** 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
    7            5    aar
```

Enter the **change dialplan analysis** command on Branch Office Communication Manager. Add an entry for local **ext** (extension), **dac** and **aar** 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    aar
    7            5    ext
```

4.4. Administer Trunk and Signaling

Enter the **add signaling-group 3** command and add an entry for Avaya SES as shown in the sample configuration. Submit these changes.

- Group Type = sip
- Transport Method = tls
- Near-end Node Name = procr
- Far-end Node Name = HeadOffice_SES
- Near-end Listen Port = 5061
- Far-end Network Region = 1
- Direct IP-IP Audio Connections = N

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

 Group Number: 3              Group Type: sip
                        Transport Method: tls




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

Enter the **add trunk-group 3** command and add an entry for Avaya SES as shown in the sample configuration. Submit these changes.

```
add trunk-group 3                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 3                     Group Type: sip           CDR Reports: y
  Group Name: HO_SES                          COR: 1        TN: 1        TAC: 103
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                       Signaling Group: 3
                                                     Number of Members: 10
```

4.5. Administer Routing

Enter the **change route-pattern 3** command and add an entry for Avaya SES as shown in the sample configuration. Submit these changes.

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

4.6. Administer Stations SIP and Non-SIP

To create local or non-SIP stations, enter the **add station 60001** command and add an entry for Local Head Office as shown in the sample configuration. 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_SIP_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. Make this local extension as OPTIM by entering the **change off-pbx-telephone station-mapping 60003** command as shown below. 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              3          1
                                -
```

4.7. Administer Network Region

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

- **Region = 1**
- **Authoritative Domain = ho.avaya.com**
- **Name = HeadOffice**
- **Intra-region IP-IP Direct Audio = no**
- **Inter-region IP-IP Direct Audio = no**

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

Location: 1       Authoritative Domain: ho.avaya.com
    Name: HeadOffice
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   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
```

4.8. Administer Codec Set

Enter the **change ip-codec-set 1** command and add entries as shown in the sample configuration. 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:
```

Repeat the configuration procedures in Section 4.1 to Section 4.8 to configure the Branch Office Communication Manager.

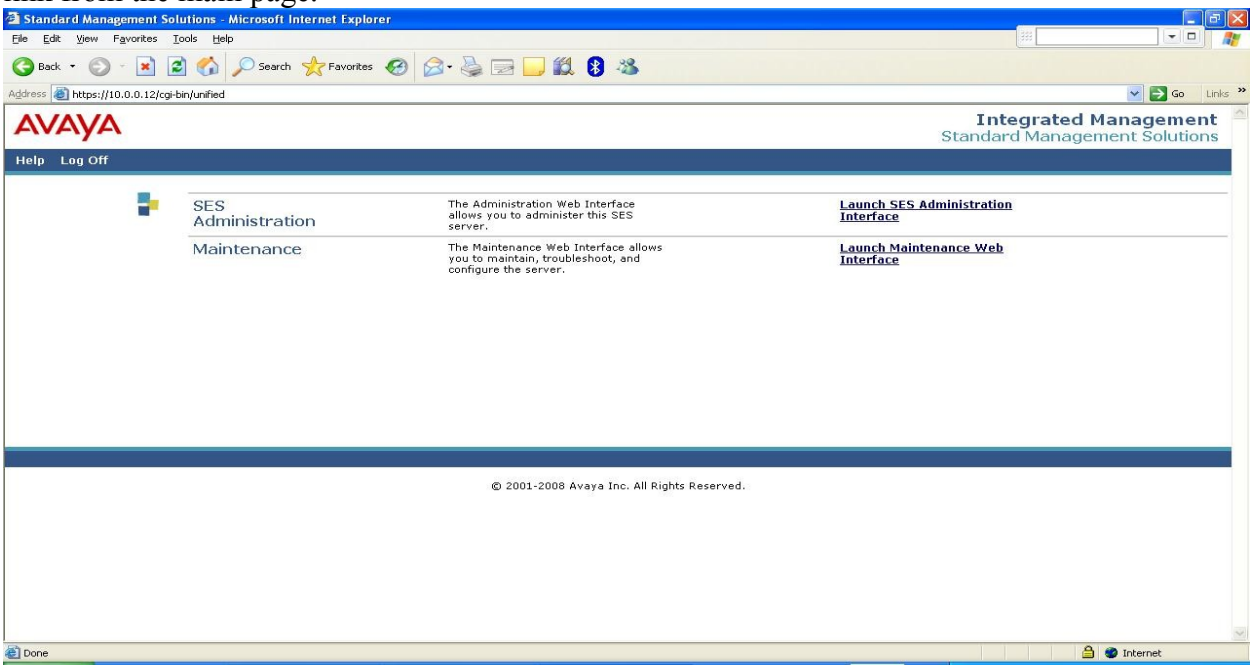
5. Configure Avaya SIP Enablement Services

This section provides the procedures for configuring SIP Enablement Services (SES) at the Head Office. Avaya SES is configured via an Internet browser using the administrator web interface. It is assumed that 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.

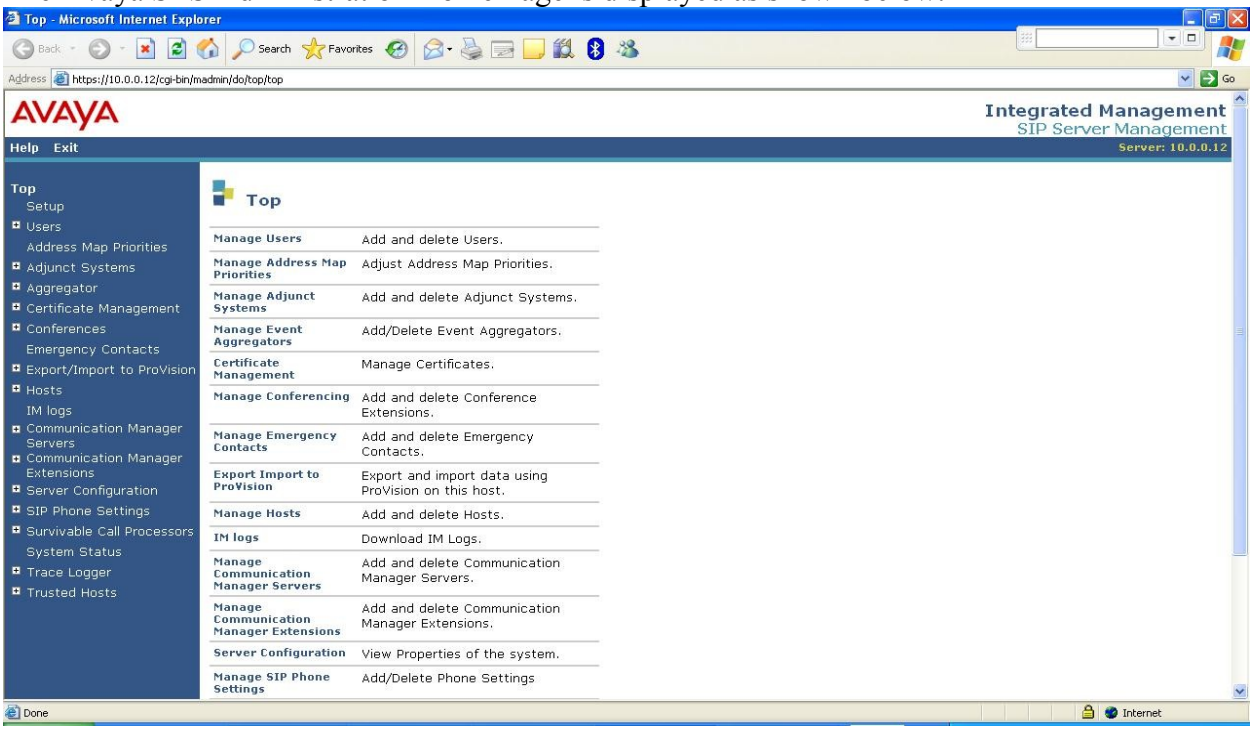
- Administer SIP OPTIM Users
- Administer Communication Manager Server Interface
- Administer Mapping in Host and on Communication Manager
- Administer Trusted Hosts

5.1. Administer SIP OPTIM Users

Log in with appropriate credentials and then select the **Launch SES Administration Interface** link from the main page.

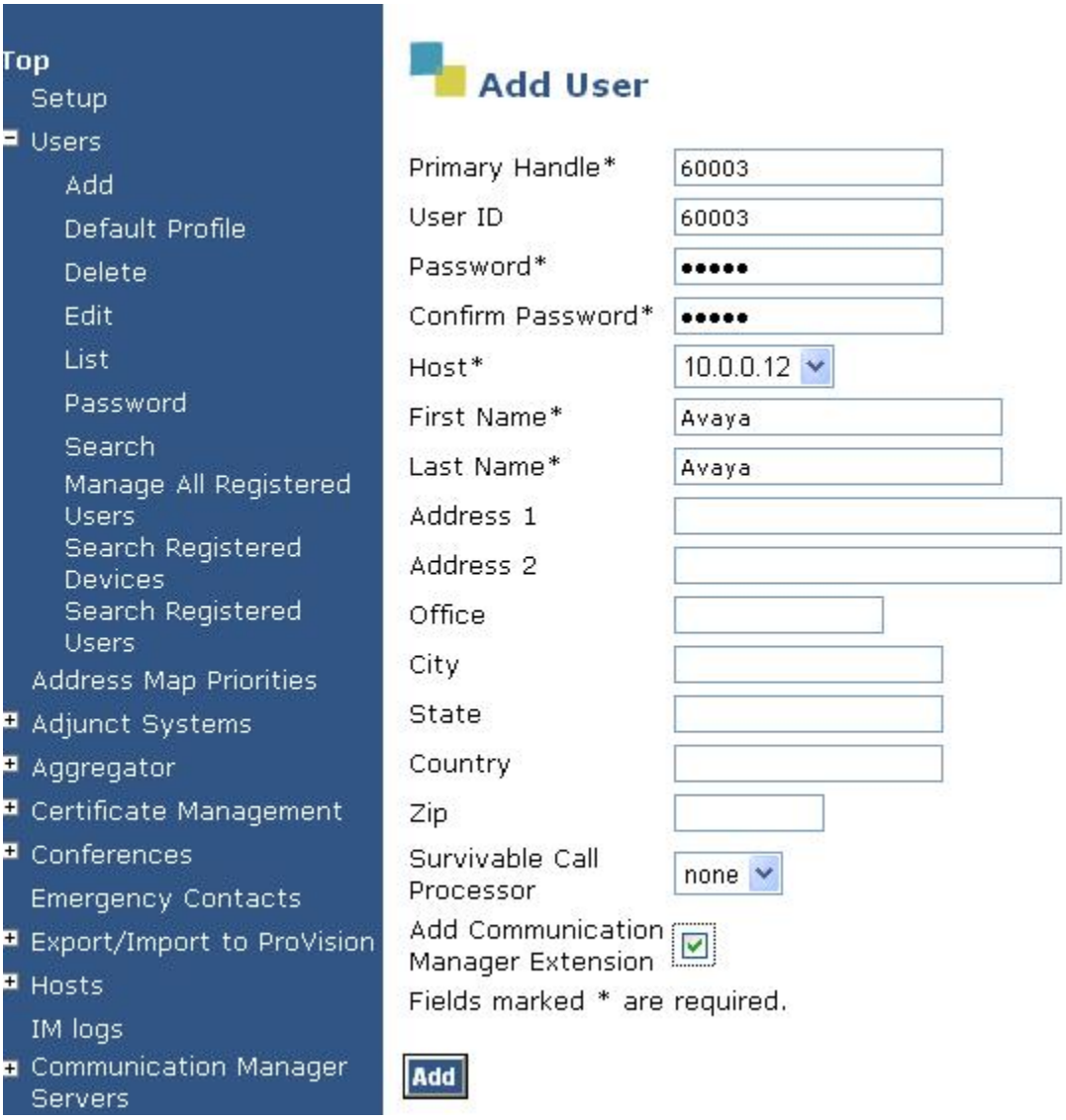


The Avaya SES Administration Home Page is displayed as shown below.

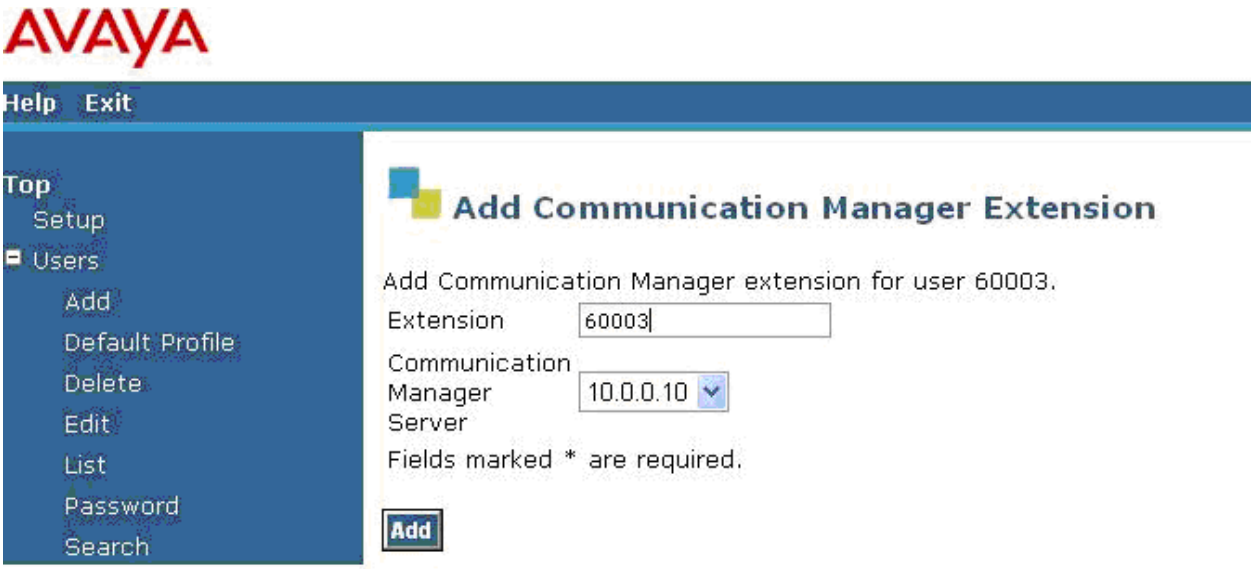


On the left panel expand **Users.** From **Users** click **Add**. Enter the required details as shown in the sample configuration below and click **Add**. Repeat the same steps for other SIP OPTIM users.

- **Primary Handle = 60003**
- **User ID = 60003**
- **Password = xxxxxx**
- **Confirm Password = xxxxxx**
- Tick the **Add Communication Manager Extension**



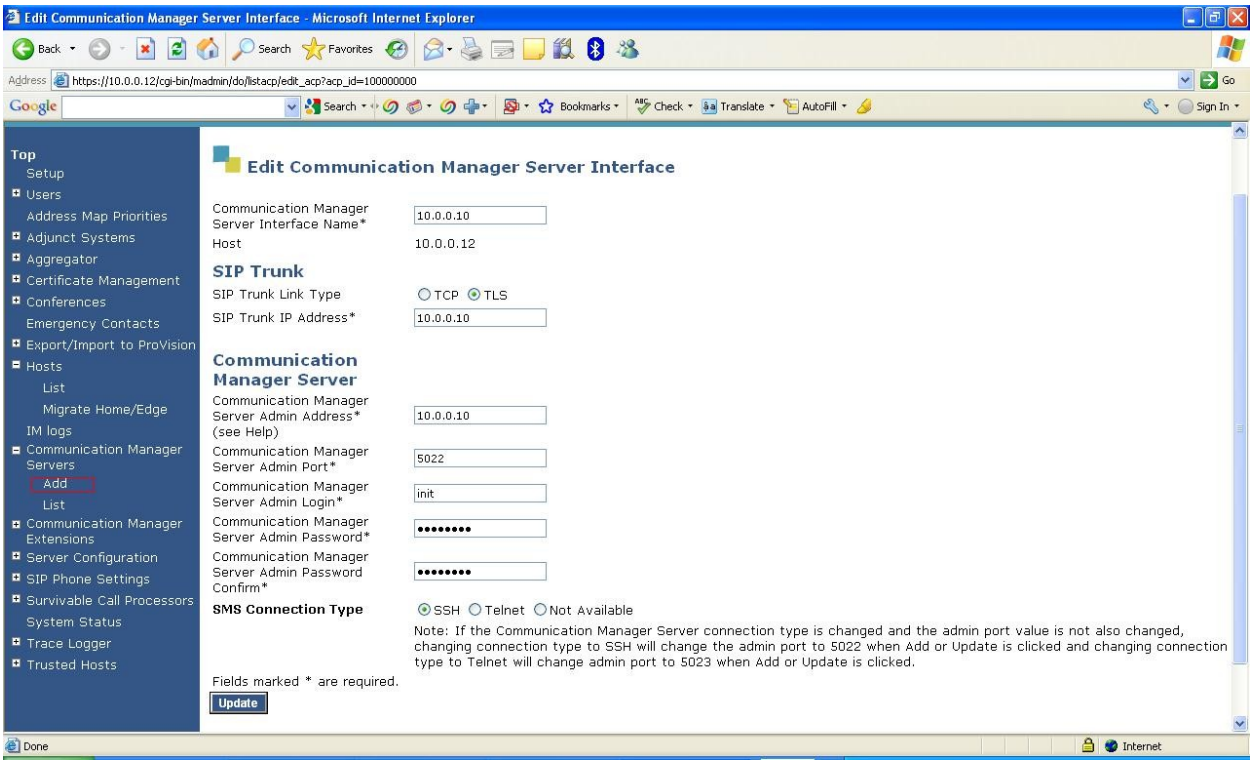
Click **Continue** on the subsequent screen (not shown). The screen below appears and enters the extension as shown. Click **Add**.



5.2. Administer Communication Manager Server Interface

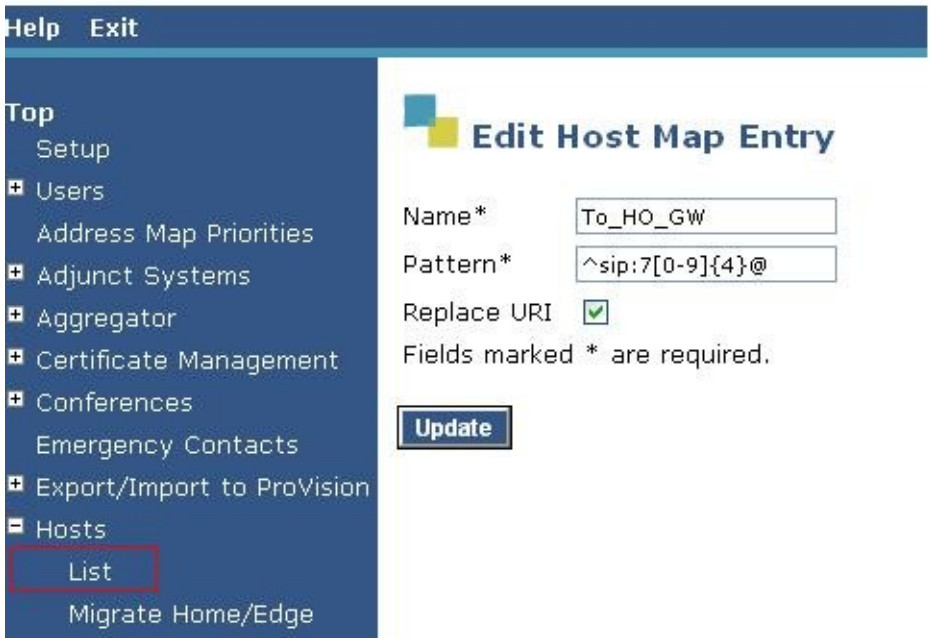
From the home page on the left panel expand **Communication Manager Servers→Add**. Enter the required details as shown in the sample configuration and click **Update**.

- **Communication Manager Server Interface Name = CM IP Address**
- **SIP Trunk Link Type = TLS**
- **SIP Trunk IP Address = CM IP Address**
- **Communication Manager Server Admin Address = CM IP Address**
- **Communication Manager Server Admin Port = 5022**
- **Communication Manager Server Admin Login = xxxx**
- **Communication Manager Server Admin Password = XXXXX**
- **SMS Connection Type = ssh**



5.3. Administer Mapping in Host and on Communication Manager

On the left panel expand **Hosts → List → Map** and then click on **Add Map In New Group.** Enter the required details as shown in the sample configuration below and click **Update.** Enter a descriptive name in the **Name** field. In the **Pattern** field, enter the regular expression to pattern match for extensions beginning with **7** on Branch Office. Verify the **Replace URI** checkbox is ticked.



Click the **Add** button once the form is completed. On the confirmation screen (not shown), click **Continue.**

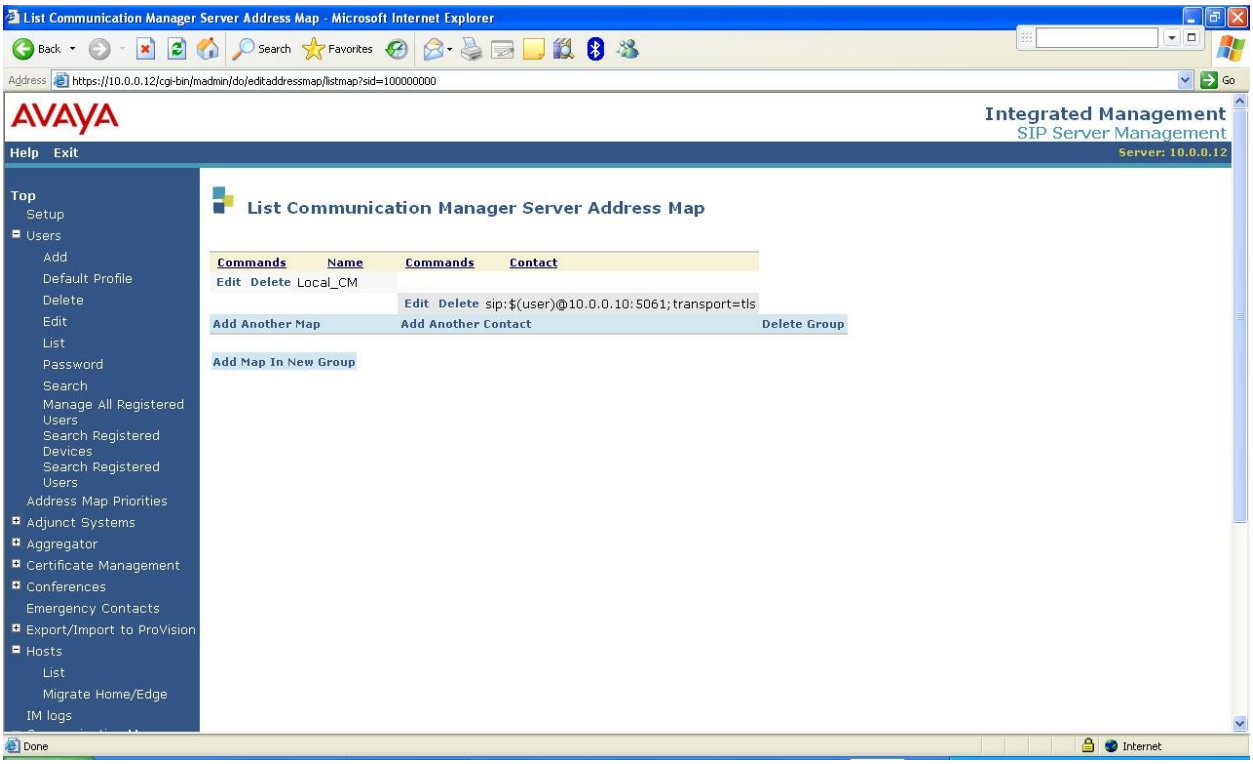
Click on **Add Another Contact** (not shown). In the **Contact** field, enter **sip:$(user)@10.0.0.1:5060;transport=udp**. The IP address is the SIP Security Controller eth1 which is connected to the Head Office. Transport is UDP as shown in the sample configuration.

Click **Submit** and **Continue** for the confirmation screen (not shown).

On the left panel expand **Communication Manager Servers → List → Map** and then **c**lick 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 Communication Manager at the Head Office. In this configuration extensions on the Head Office Communication Manager begin with **6**. Ensure the **Replace URI** checkbox is ticked. Click **Update**.

Add a contact entry for calls to Communication Manager at the Head Office. Click on **Add Another Contact** (not shown). Enter 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 Head Office Communication Manager IP address. Transport is TLS as shown in the sample configuration and click **Add**.

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



5.4. Administer Trusted Hosts

From the home page on the left panel click on **Trusted Hosts→Add** and enter the details of EC-4200, Branch Office SES and Communication Manager and click on **Add** (not shown). Repeat the configuration procedure in Section 5.1 to Section 5.4 to configure the Branch Office SIP Enablement Services Server.

6. Configure the UM Labs SSC EC-4200 in Head Office

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

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

6.1. Administer Initial Setup

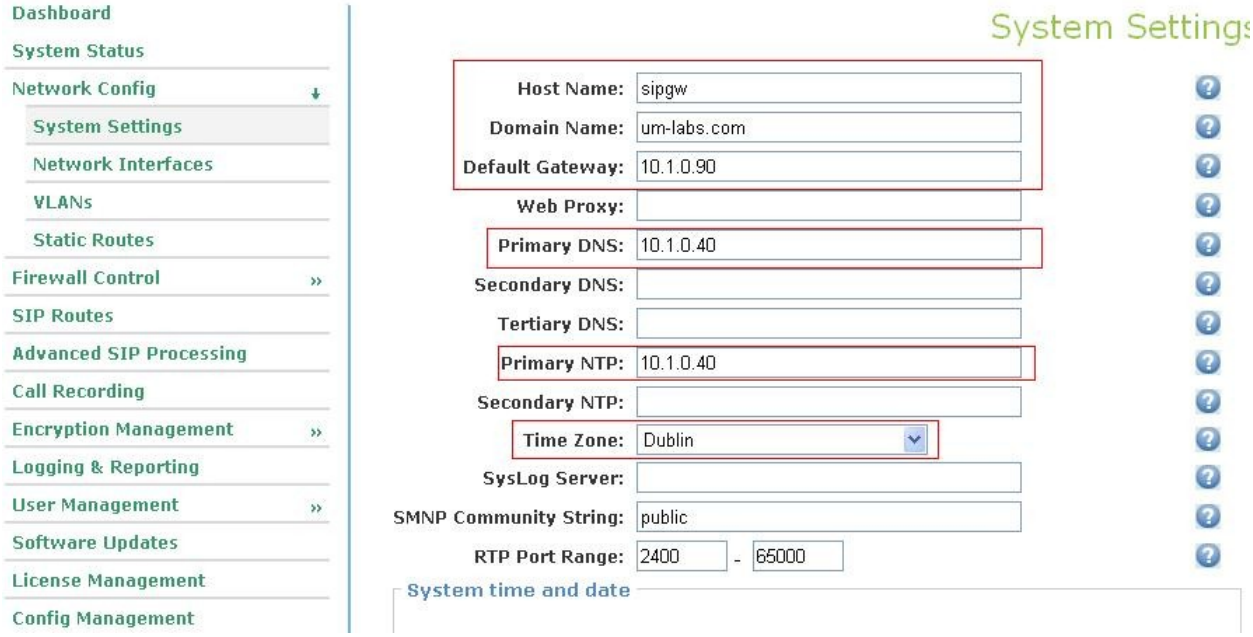
The EC-4200 ships with a default IP address on interface eth0 of 192.168.1.1. For the purposes of this test, this default address was left unchanged. Other installations may choose to change this default to simplify subsequent configuration. Refer to the UM Labs documentation for details. For the purposes of the certification test, the EC-4200 was linked on a test network using a private IP address. Follow the quick start guide (refer UM Labs Website) to change default IP of EC4200 to 192.168.1.1. Configure the EC4200 from GUI, connect to http://192.168.1.1, log in as admin and enter password.

6.2. Administer License

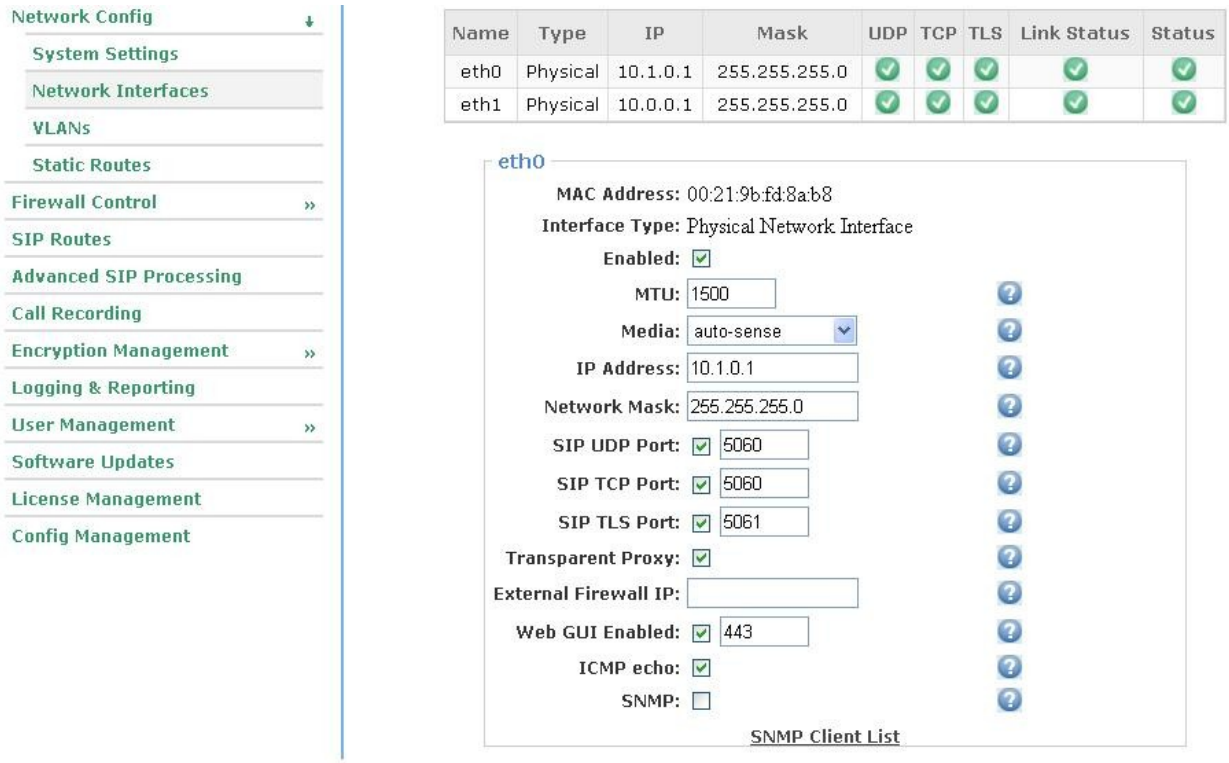
For the very first time log in using the above URL. Users need to accept license and change **admin password**, click on **Save**.

6.3. Administer Basic Configuration

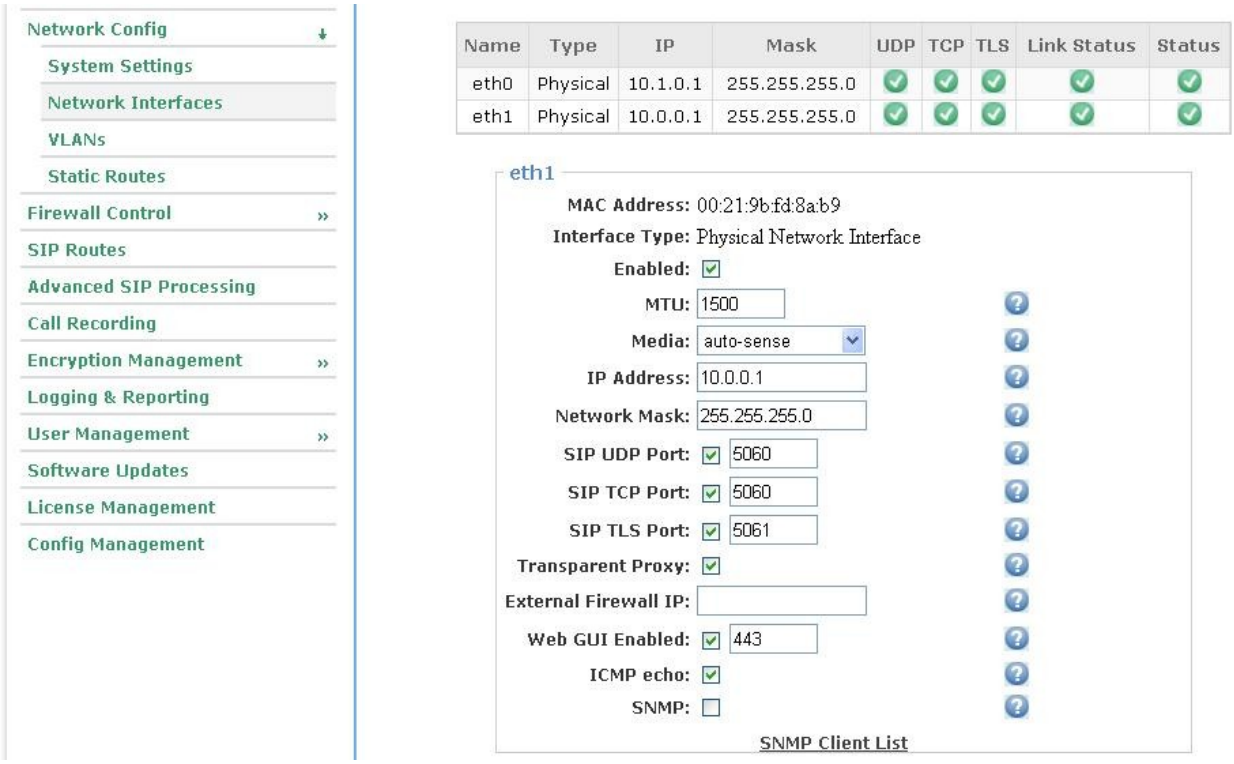
From the left panel click on **Network Config →System Settings**, enter the details for **Host Name, Domain Name, Default Gateway, Primary DNS, Primary NTP** and **Time Zone** as shown in the sample configuration. For the purposes of these tests, default gateway was NTP server in this configuration as 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. To save these changes, click on **Apply**.



From the left plane, choose **Network Config** and click on **Network Interfaces** to configure the IP Address as **eth0: 10.1.0.1/24** (Link to Branch Office).



To configure the IP Address for the **eth1**, click on **Network Interfaces** as **eth1: 10.0.0.1** (link to Head Office). Set each Interface to **Transparent Proxy** and enable **Ping and Web Admin** (not shown). To save these changes, click on **Apply**.



The configured eth0 and eth1 interfaces are shown in the sample configuration below.

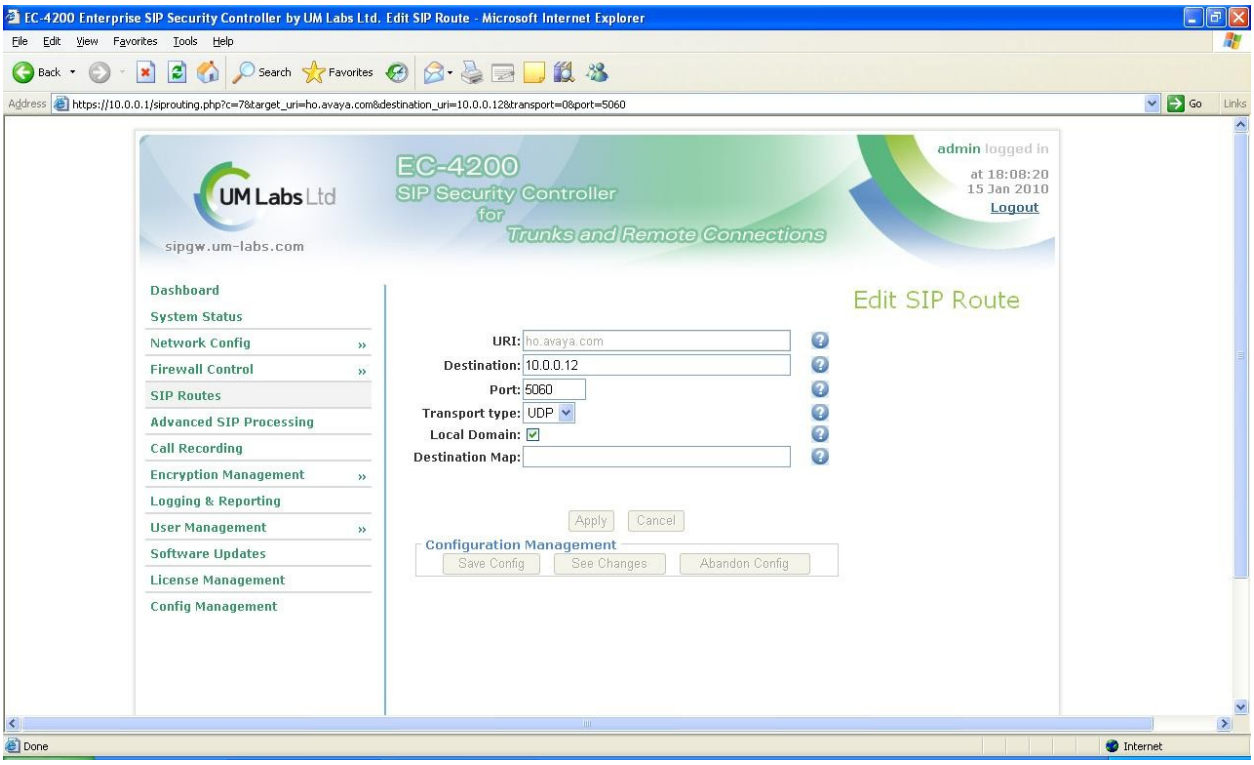
Name	Type	IP	Mask	UDP	TCP	TLS	Link Status
eth0	Physical	10.1.0.1	255.255.255.0	✓	✓	✓	✓
eth1	Physical	10.0.0.1	255.255.255.0	✓	✓	✓	✓

6.4. Administer SIP Routes

Configure routing between Head Office and Branch Office in EC-4200 using SIP Routes. Click on **SIP Routes** in the left hand panel, add routes for Head Office and Branch Office.

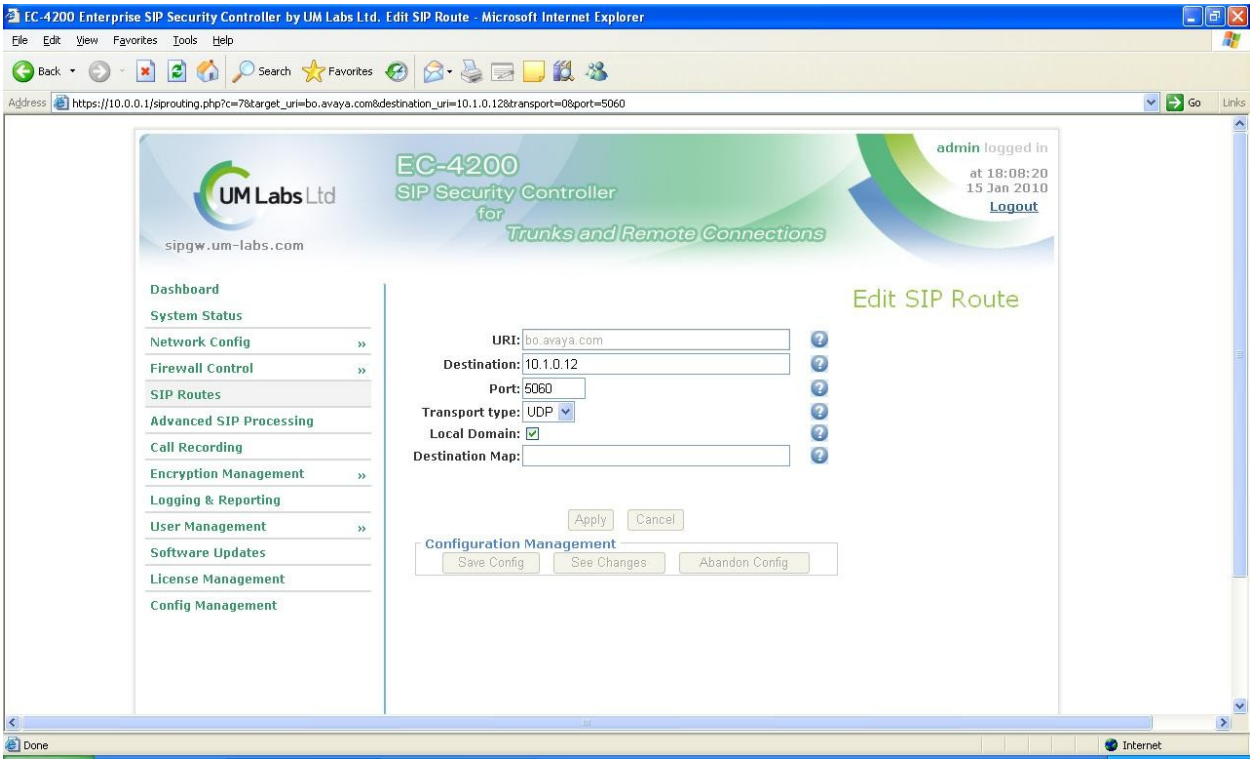
- **URI** = Enter descriptive name
- **Destination** = Head Office SES IP Address
- **Transport** and **Port** =**UDP** and **5060**
- **Local Domain** = Ticked

Other installations may require a more restrictive call flow policy. Refer to the UM Labs documentation for more information.



Configure routing between Branch Office and Head Office in EC-4200 using SIP Routes. Click on **SIP Routes** in the left hand panel, add routes for Head Office and Branch Office.

- **URI** = Enter descriptive name
- **Destination** = Branch Office SES IP Address
- **Transport** and **Port** =**UDP** and **5060**
- **Local Domain** = Ticked



The configured SIP Routes are shown in the sample configuration below.

☐	bo.avaya.com	10.1.0.12	UDP	✓	✗	Auth
☐	ho.avaya.com	10.0.0.12	UDP	✓	✗	Auth

6.5. Verify Software Version

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

7. General Test Approach and Test Results

In this test configuration, a real time deployment scenario was simulated with UM–Labs EC-4200 SSC between the Head Office and Branch Office, with shuffling turned OFF on the Communication Manager server in both offices. All the Signaling and RTP was through SSC using UDP. Interoperability compliance testing focused on UM Labs SIP Security Controller EC-4200 between Avaya Head Office and Branch Office. Testing verified Point–to-Point and Telephony features like hold, transfer and conferencing.

8. Verification Steps

Verification and troubleshooting steps between UM Labs SSC, Avaya Communication Manager and Avaya SIP Enablement Services are as follows:

- Verify audio between two sites
- Verify Telephone features Hold, Transfer and Conference between two sites
- Verify SIP routes page shows status UDP links only, i.e. on EC-4200
- To verify UM Labs SSC logs, go to 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 traces from Communication Manager, using the **SAT**, enter **list trace tac n**, where n is the TAC used for the trunk group created on Communication Manger to Avaya SES.
- To verify traces on Avaya SES, use command line trace called **traceSES**.

9. Conclusion

The interoperability between UM Labs SSC EC-4200, Avaya Communication Manager, and Avaya SIP Enablement Services has passed with shuffling turned OFF on the Communication Manager at both the Head Office and Branch Office.

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.