



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.

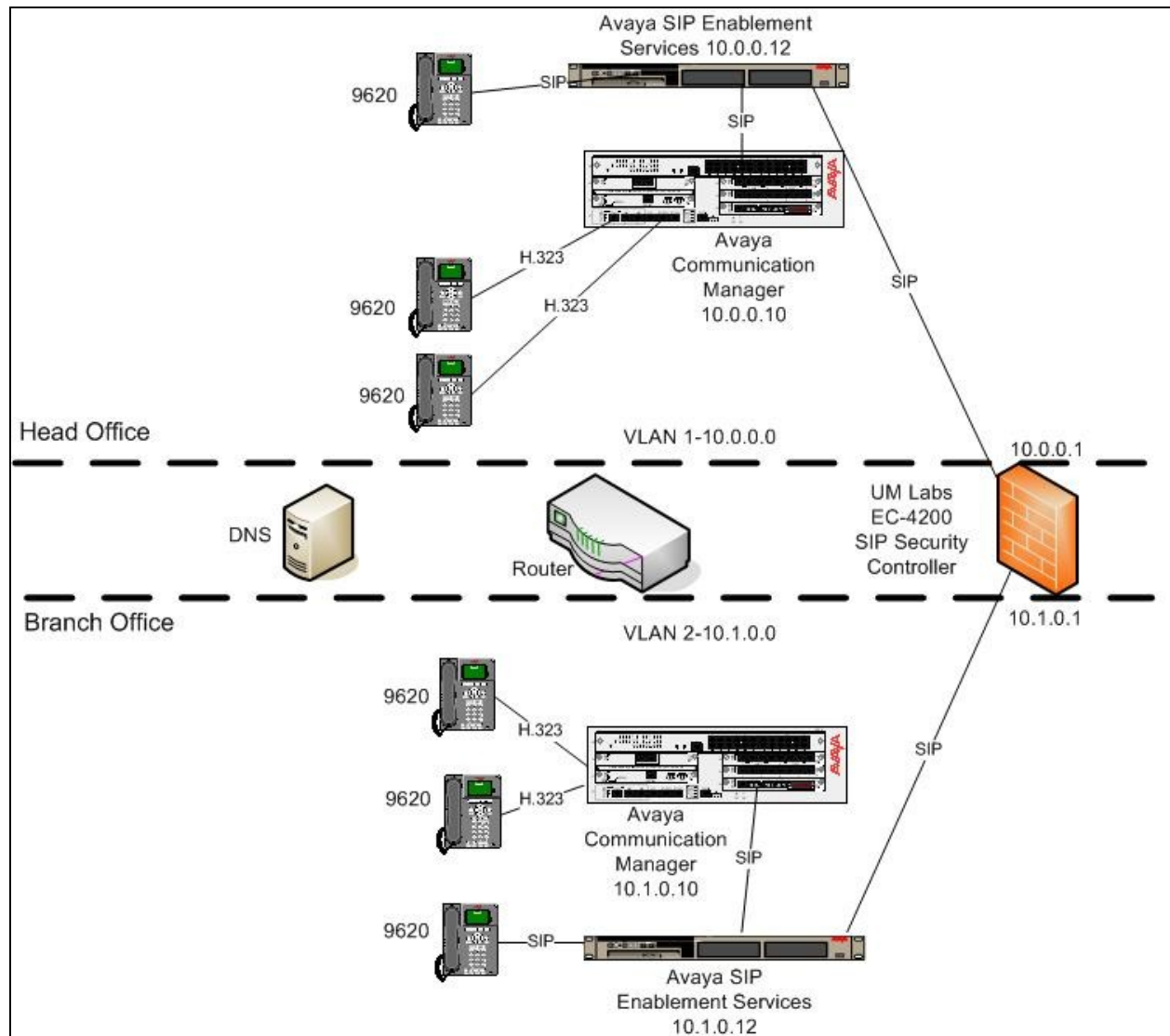


Figure 1: Network Configuration Diagram

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8300 Server	Avaya Communication Manager 5.1.1 SP1 01.1.415.1-16988
Avaya G350 Media Gateway	28.22.0
Avaya 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 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 String	Total Length	Call 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 String	Total Length	Call 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:		
DTMF over IP: rtp-payload	Bypass If IP Threshold Exceeded? n	
	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
Direction: two-way	Outgoing Display? n	TAC: 103
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
Signaling Group: 3		
Number of Members: 10		

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

JR; Reviewed;
SPOC 2/16/2010

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		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 60001	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
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 Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config 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.

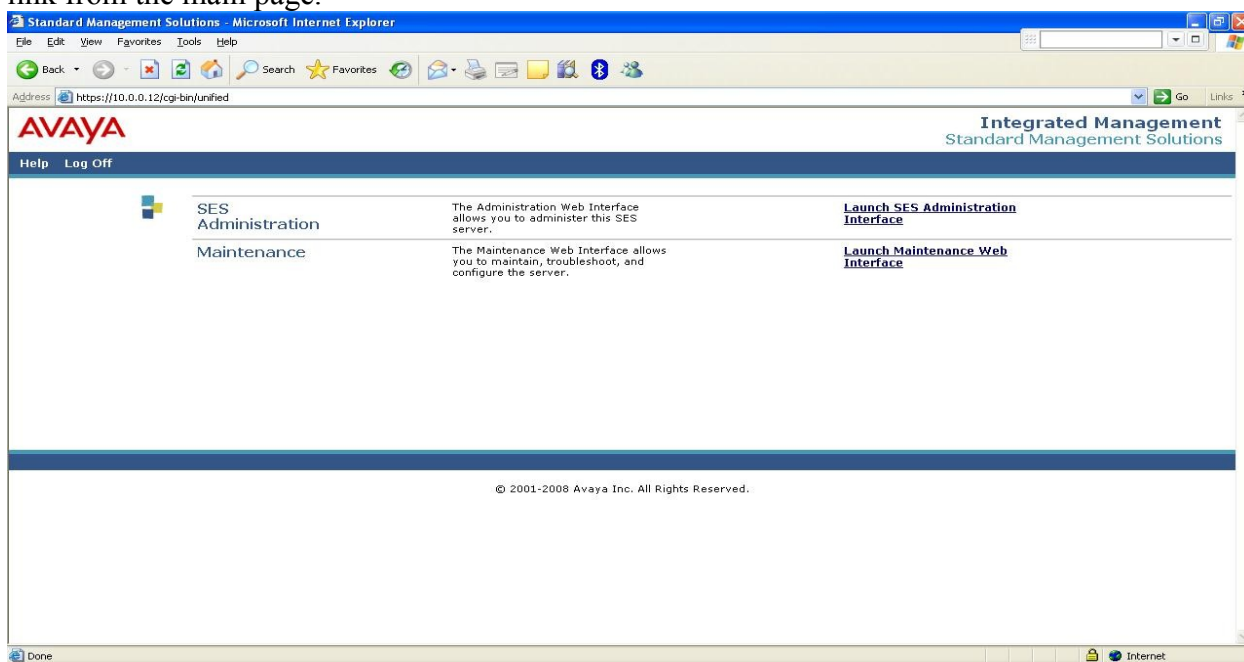
5. Configure Avaya SIP Enablement Services

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.

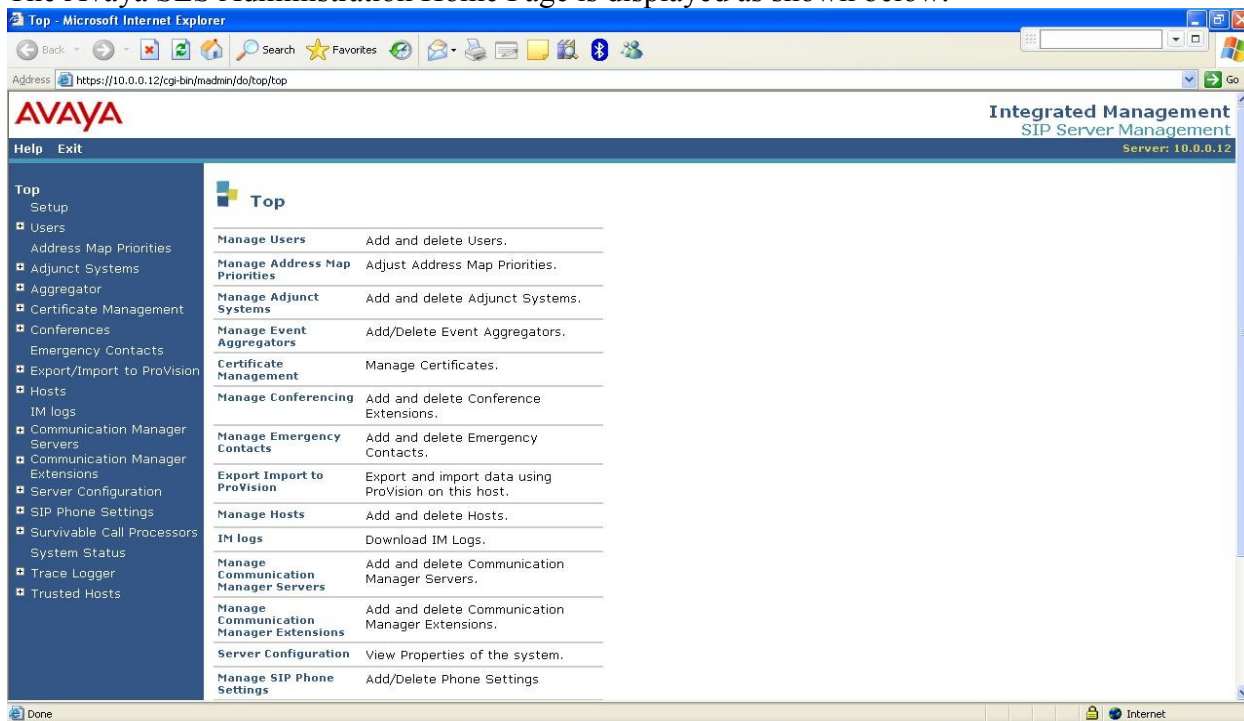
- Administer SIP OPTIM Users
- Administer Communication Manager Server Interface
- Administer Mapping in Host and on Communication Manager
- Administer Trusted Hosts

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**

Top

Setup

Users

Add

Default Profile

Delete

Edit

List

Password

Search

Manage All Registered Users

Search Registered Devices

Search Registered Users

Address Map Priorities

Adjunct Systems

Aggregator

Certificate Management

Conferences

Emergency Contacts

Export/Import to ProVision

Hosts

IM logs

Communication Manager Servers

Add User

Primary Handle*

60003

User ID

60003

Password*

•••••

Confirm Password*

•••••

Host*

10.0.0.12

First Name*

Avaya

Last Name*

Avaya

Address 1

Address 2

Office

City

State

Country

Zip

Survivable Call Processor

none

Add Communication Manager Extension

☒

Fields marked * are required.

Add

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



Help Exit

Top

- Setup
- Users
 - Add
 - Default Profile
 - Delete
 - Edit
 - List
 - Password
 - Search

Add Communication Manager Extension

Add Communication Manager extension for user 60003.

Extension

Communication Manager Server

Fields marked * are required.

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

Edit Communication Manager Server Interface

Communication Manager Server Interface Name* 10.0.0.10

Host 10.0.0.12

SIP Trunk

SIP Trunk Link Type ☐ TCP ☒ TLS

SIP Trunk IP Address* 10.0.0.10

Communication Manager Server

Communication Manager Server Admin Address* 10.0.0.10 (see Help)

Communication Manager Server Admin Port* 5022

Communication Manager Server Admin Login* init

Communication Manager Server Admin Password*

Communication Manager Server Admin Password Confirm*

SMS Connection Type ☒ SSH ☐ Telnet ☐ Not Available

Note: If the Communication Manager Server connection type is changed and the admin port value is not also changed, changing connection type to SSH will change the admin port to 5022 when Add or Update is clicked and changing connection type to Telnet will change admin port to 5023 when Add or Update is clicked.

Fields marked * are required.

Update

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.

The screenshot shows a web application interface for editing a host map entry. On the left is a dark blue sidebar with a navigation menu. The menu items are: Top, Setup, Users, Address Map Priorities, Adjunct Systems, Aggregator, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts (expanded), List (highlighted with a red box), and Migrate Home/Edge. The main content area is white and titled 'Edit Host Map Entry'. It contains three input fields: 'Name*' with the value 'To_HO_GW', 'Pattern*' with the value '^sip:7[0-9]{4}@', and 'Replace URI' with a checked checkbox. Below these fields is a note: 'Fields marked * are required.' At the bottom of the form is a blue 'Update' button.

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.

Help Exit

Top

- Setup
- Users
- Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
- Emergency Contacts
- Export/Import to ProVision
- Hosts
- List
- Migrate Home/Edge

Edit Host Contact

Host 10.0.0.12

Contact sip:\$(user)@10.0.0.1:5060;transport=udp

Fields marked * are required.

Submit

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

On the left panel expand **Communication Manager Servers → List → Map** and then 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 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**.

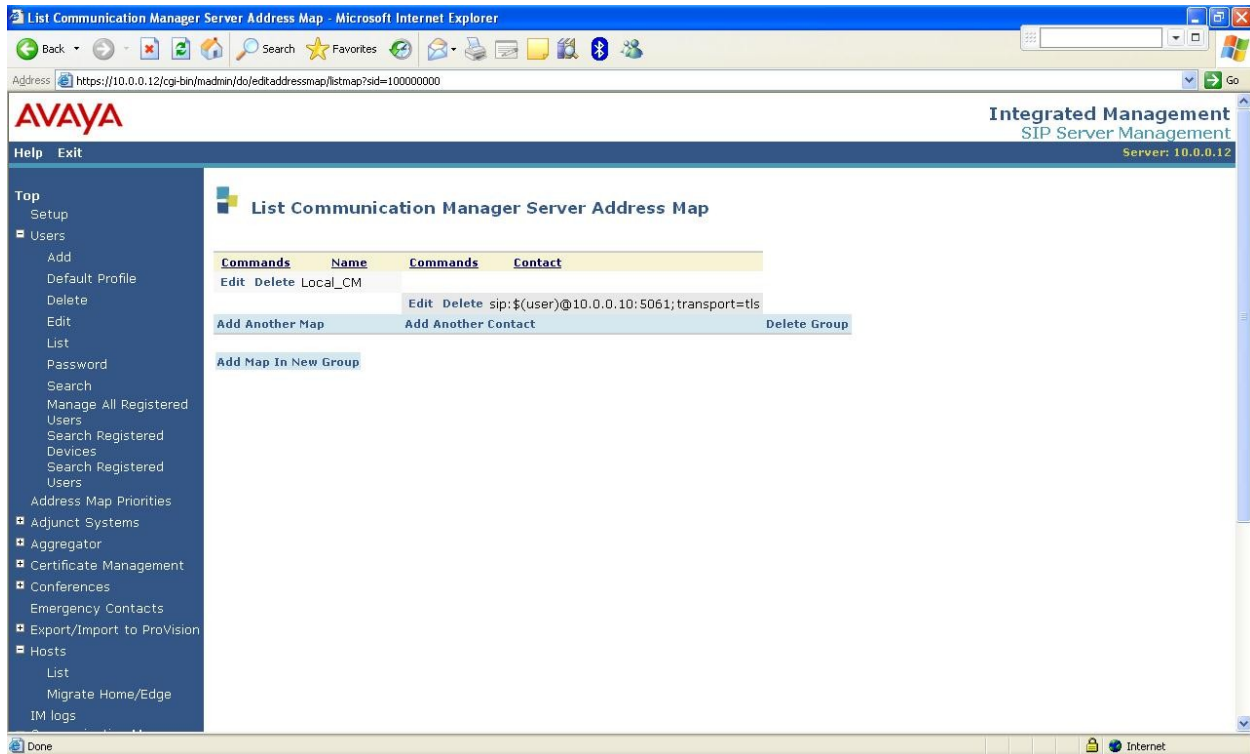
The screenshot displays the Avaya Communication Manager configuration interface. On the left is a dark blue sidebar with a tree view. The 'List' option under 'Communication Manager Servers' is highlighted with a red rectangle. The main area on the right is titled 'Edit Communication Manager Map Entry' and contains the following fields and controls:

- Name***: A text input field containing 'Local_CM'.
- Pattern***: A text input field containing '^sip:6[0-9]{4}@'.
- Replace URI**: A checkbox that is checked.
- A note below the fields states: 'Fields marked * are required.'
- An **Update** button is located at the bottom left of the main area.

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**.


Help Exit
Top
Setup
■ Users
Add
Default Profile
Delete
Edit
List
Password
 **Add Communication Manager Contact**
Handle Local_CM
Contact*
Fields marked * are required.

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**.



The screenshot displays the web interface of the UM Labs EC-4200 SIP Security Controller. The header includes the UM Labs Ltd logo and the text 'EC-4200 SIP Security Controller for Trunks and Remote Connections'. The main heading is 'Change Your Password'. Below this, there are three input fields: 'User Account' with 'admin' entered, 'Type a new Password' with masked characters, and 'Confirm the new Password' with masked characters. At the bottom of the form are 'Save' and 'Clear' buttons. The footer contains the copyright notice 'Copyright © 2008 UM Labs Ltd'.

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**.

The screenshot shows the 'System Settings' page in a network management interface. On the left is a sidebar menu with the following items: Dashboard, System Status, Network Config (expanded), System Settings (highlighted), Network Interfaces, VLANs, Static Routes, Firewall Control, SIP Routes, Advanced SIP Processing, Call Recording, Encryption Management, Logging & Reporting, User Management, Software Updates, License Management, and Config Management. The main content area is titled 'System Settings' and contains the following configuration fields:

- Host Name: sipgw
- Domain Name: um-labs.com
- Default Gateway: 10.1.0.90
- Web Proxy: (empty)
- Primary DNS: 10.1.0.40
- Secondary DNS: (empty)
- Tertiary DNS: (empty)
- Primary NTP: 10.1.0.40
- Secondary NTP: (empty)
- Time Zone: Dublin (selected from a dropdown menu)
- SysLog Server: (empty)
- SNMP Community String: public
- RTP Port Range: 2400 - 65000

Below these fields is a section titled 'System time and date' which is currently empty. To the right of the configuration fields is a vertical column of ten question mark icons.

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).

Network Config
System Settings
Network Interfaces
VLANs
Static Routes
Firewall Control
SIP Routes
Advanced SIP Processing
Call Recording
Encryption Management
Logging & Reporting
User Management
Software Updates
License Management
Config Management

eth0

MAC Address: 00:21:9b:fd:8a:b8
Interface Type: Physical Network Interface
Enabled:
MTU: 1500
Media: auto-sense
IP Address: 10.1.0.1
Network Mask: 255.255.255.0
SIP UDP Port: 5060
SIP TCP Port: 5060
SIP TLS Port: 5061
Transparent Proxy:
External Firewall IP:
Web GUI Enabled: 443
ICMP echo:
SNMP:
SNMP Client List

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

eth0

MAC Address: 00:21:9b:fd:8a:b8
Interface Type: Physical Network Interface
Enabled:
MTU: 1500
Media: auto-sense
IP Address: 10.1.0.1
Network Mask: 255.255.255.0
SIP UDP Port: 5060
SIP TCP Port: 5060
SIP TLS Port: 5061
Transparent Proxy:
External Firewall IP:
Web GUI Enabled: 443
ICMP echo:
SNMP:
SNMP Client List

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**.

Network Config ↓

System Settings

Network Interfaces

VLANs

Static Routes

Firewall Control »

SIP Routes

Advanced SIP Processing

Call Recording

Encryption Management »

Logging & Reporting

User Management »

Software Updates

License Management

Config Management

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

eth1

MAC Address: 00:21:9b:fd:8a:b9

Interface Type: Physical Network Interface

Enabled: ☒

MTU: ?

Media: ?

IP Address: ?

Network Mask: ?

SIP UDP Port: ☒ ?

SIP TCP Port: ☒ ?

SIP TLS Port: ☒ ?

Transparent Proxy: ☒ ?

External Firewall IP: ?

Web GUI Enabled: ☒ ?

ICMP echo: ☒ ?

SNMP: ☐ ?

[SNMP Client List](#)

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

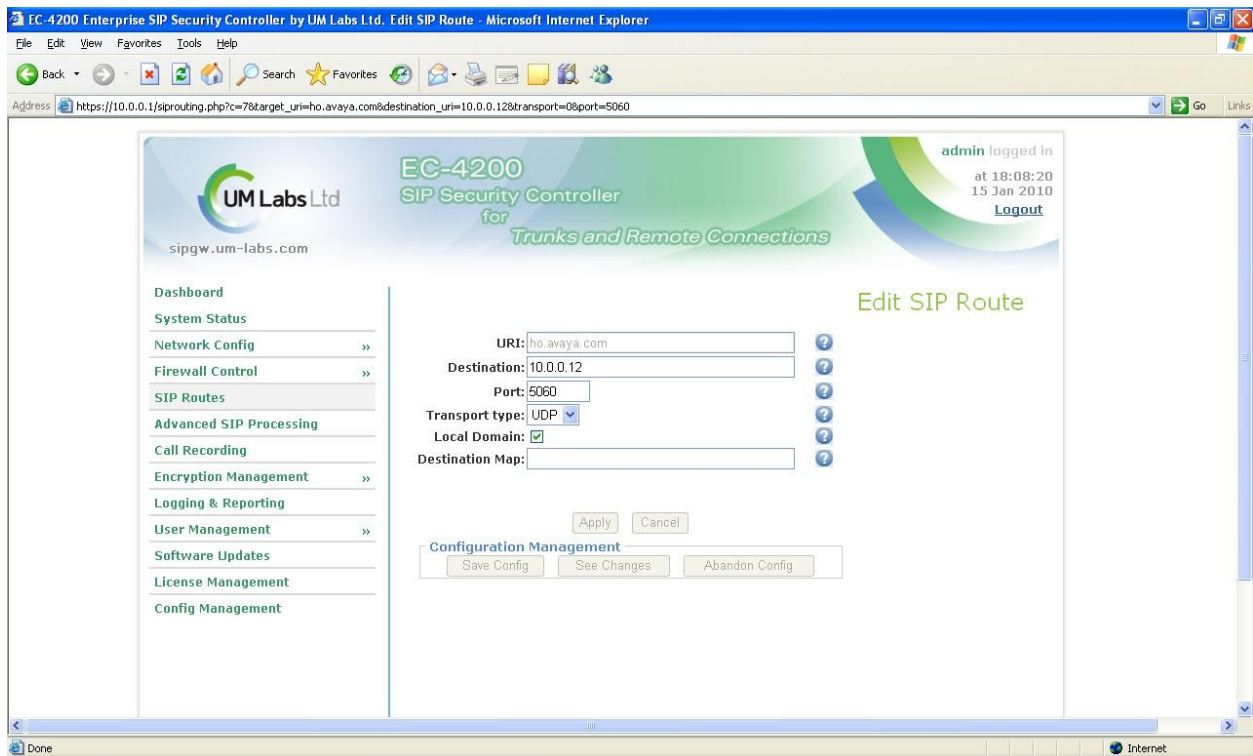
Name	Type	IP	Mask	UDP	TCP	TLS	Link Status
eth0	Physical	10.1.0.1	255.255.255.0	✓	✓	✓	✓
eth1	Physical	10.0.0.1	255.255.255.0	✓	✓	✓	✓

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.

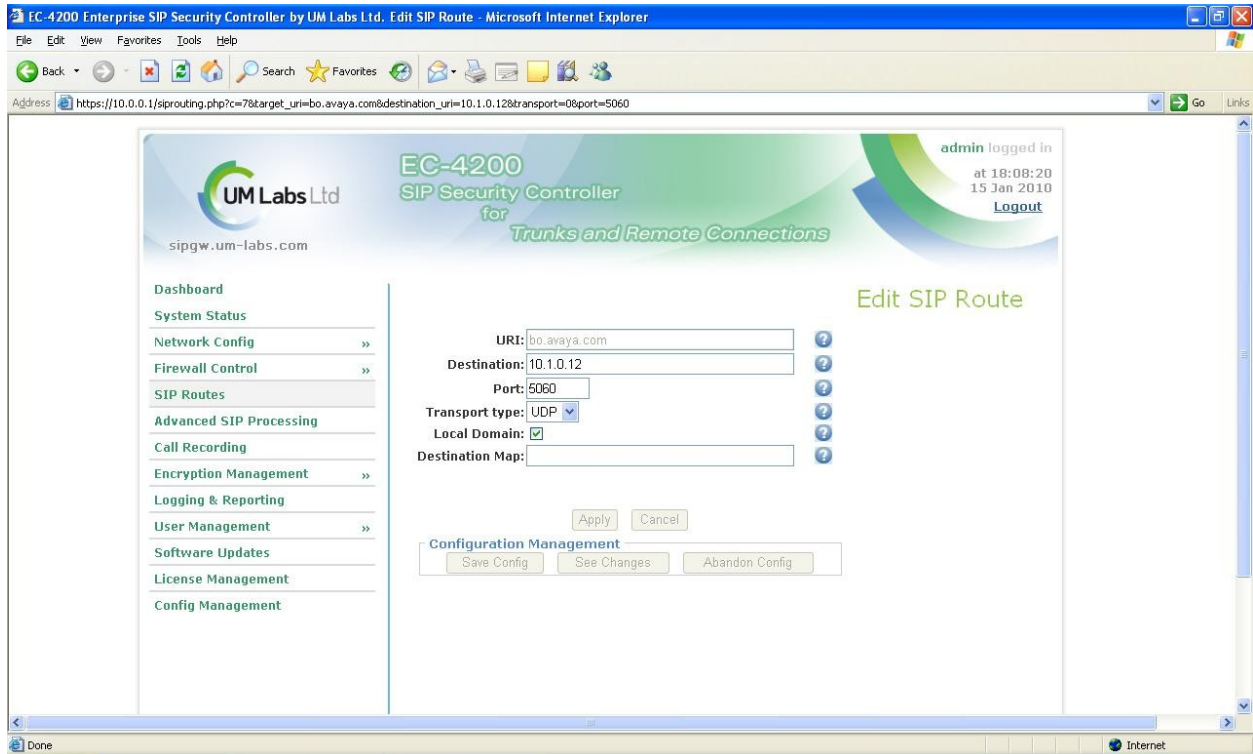
- **URI** = Enter descriptive name
- **Destination** = Head Office SES IP Address
- **Transport and Port** = **UDP** and **5060**
- **Local Domain** = Ticked

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.

<input type="checkbox"/>	bo.avaya.com	10.1.0.12	UDP			Auth
<input type="checkbox"/>	ho.avaya.com	10.0.0.12	UDP			Auth

6.5. Verify Software Version

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


sipgw.um-labs.com

EC-4200
SIP Security Controller
for
Trunks and Remote Connections

admin logged in
at 12:11:39
25 Jan 2010
[Logout](#)

[Dashboard](#)
[System Status](#)
[Network Config](#) »
[Firewall Control](#) »
[SIP Routes](#)
[Advanced SIP Processing](#)
[Call Recording](#)

System Status

Date/time: Mon Jan 25 12:19:08 GMT 2010
Uptime: 4 days 02:02:39
System Load: 0.00, 0.00, 0.00
Software Version: V1.4 (Rev 1887)

[Reboot](#) [Shutdown](#)

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 Manager 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.

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.