



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager R6.2 and Avaya Aura® Communication Manager R6.2 to interoperate with Semafone in a Southbound Configuration – Issue 1.0

Abstract

These Application Notes describe the steps to configure Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager with Semafone. Semafone extracts DTMF tones entered by the caller from SIP signaling and replaces them with a generic tone for a call center agent to hear. The extracted DTMF tones can then be sent to a payment platform for processing.

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

The SemaFone solution in conjunction with Avaya Session Border Controller for Enterprise (ASBCE) enables DTMF tones delivered over a SIP trunk provided by a 3rd party service provider to be extracted and replaced with a generic DTMF tone. The DTMF tones captured can then be sent to a payment platform for processing; the agent hears only the replaced generic tone. In a ‘Southbound’ configuration, the SemaFone solution sits on the private or ‘south’ side of the Session Border Controller as shown in **Figure 1** below. This is in contrast with the “Northbound” configuration, where the SemaFone solution sits on the public or ‘north’ side of the Session Border Controller. The “Northbound” configuration is described in a separate application note.

The SemaFone solution addresses the traditional situation whereby an agent may ask a caller for payment details, which can be spoken by the caller and entered manually by the agent, or the agent would transfer the caller to a separate IVR for capture of the payment details. The SemaFone solution enables the caller and the agent to remain connected for the entire duration of the call, and eradicates the inherent risk and overhead of traditional methods used. As the DTMF tones captured are replaced with a generic tone, the agent is never made aware of the payment information. In addition, call recording playback cannot be used to surreptitiously collect the DTMF tones as the SemaFone solution sits on the trunk side, in this instance, between private or ‘enterprise’ interface of the ASBCE and Session Manager. When used in this way, the SemaFone solution typically enables a Call Center to more easily gain Payment Card Industry (PCI) compliance.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the SemaFone solution to establish a SIP trunk connection between the Avaya Session Border Controller for Enterprise and Session Manager and collect and clean DTMF tones when placed into SecureMode.

SecureMode is the feature by which a call routed via SemaFone is tagged by a Call Center agent using a unique code and the subsequent DTMF tones entered by the customer are masked. The unique code is generated by SemaFone and displayed to the agent through the payment page web interface. The Call Center agent enters the unique code on their telephone keypad, and an icon demonstrating that the call has entered SecureMode is shown on the web interface. The customer is then able to enter their card details using their telephone keypad without the Call Center agent having to perform any additional actions.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

The following tests were performed as part of the compliance testing.

- DTMF tones delivered by 3rd party service provider per RFC2833/in-band/SIP INFO method
- Collection and cleaning of DTMF tones received by the SemaFone solution using the above methods
- Entering SecureMode and verification that DTMF tones collected and passed to the payment engine are as entered
- Verification that none of the original DTMF tones entered are audible by the agent
- Various call routing and agent call handling scenarios

2.2. Test Results

All functionality and serviceability test cases were completed successfully.

2.3. Support

Support is available via www.semafone.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The solution consists of a simulated SIP service provider with a SIP trunk to the Public Interface of ASBCE. A separate SIP trunk is established from the Private interface of the ASBCE to the “dirty” interface of the Semafone server SIP Interworking Gateway (SIG). The “dirty” interface is the interface on which the true DTMF tones entered by the customer are received. A further SIP trunk is established between the “clean” side of the Semafone server and the Session Manager SIP Interface. The “clean” interface is the interface on which the DTMF tones entered by the customer have been removed and replaced with a generic tone. Session Manager has a further SIP trunk to Communication Manager. Communication Manager is connected to a G450 which provides DSP resources and services 9630 H.323 Deskphones.

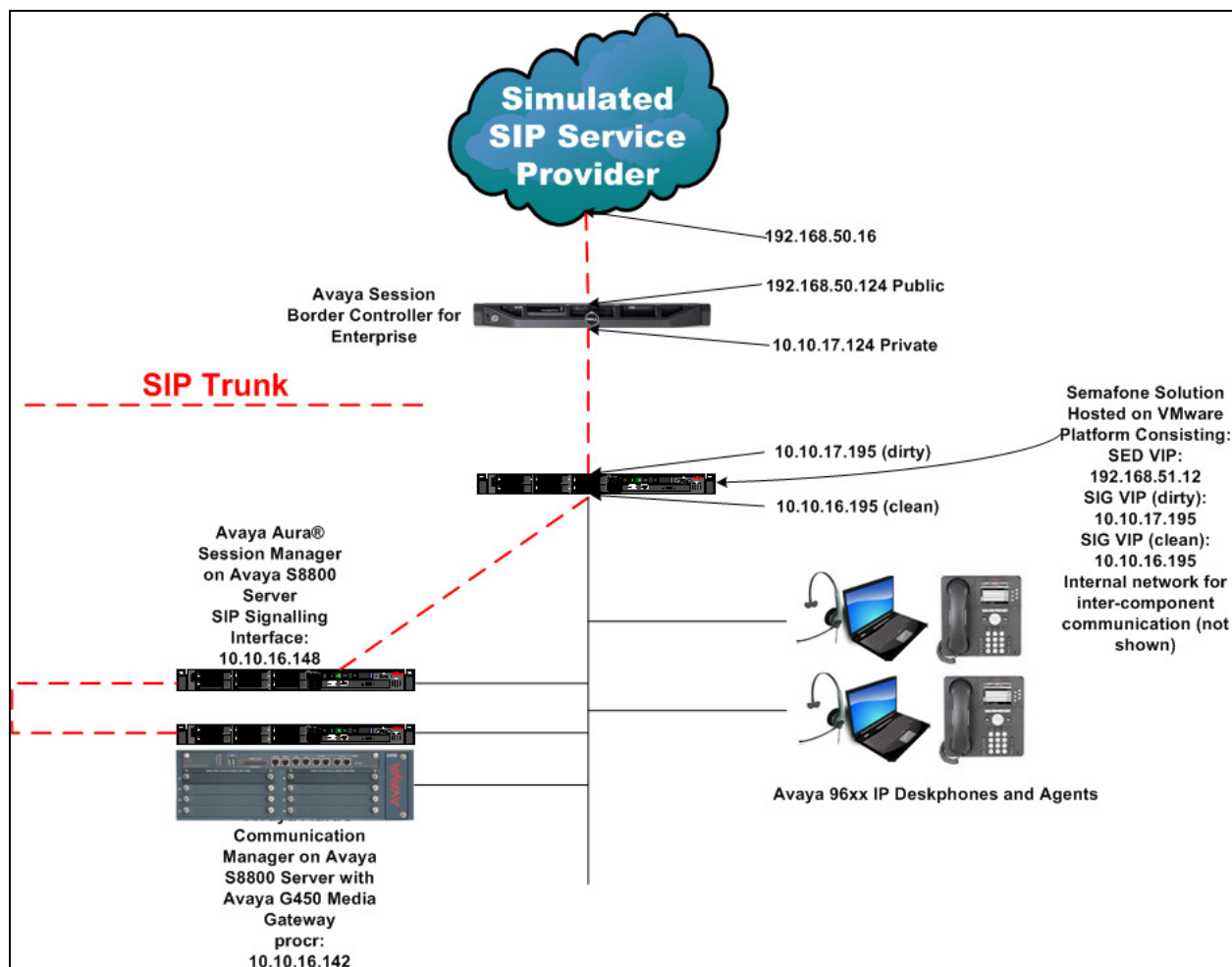


Figure 1: Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager with Semafone Solution

Figure 2 illustrates the payment network topology used during compliance testing. The solution consists of the same Semafone server hardware and agents shown in **Figure 1** with the addition of a payment page hosted on a webserver residing on the Semafone server.

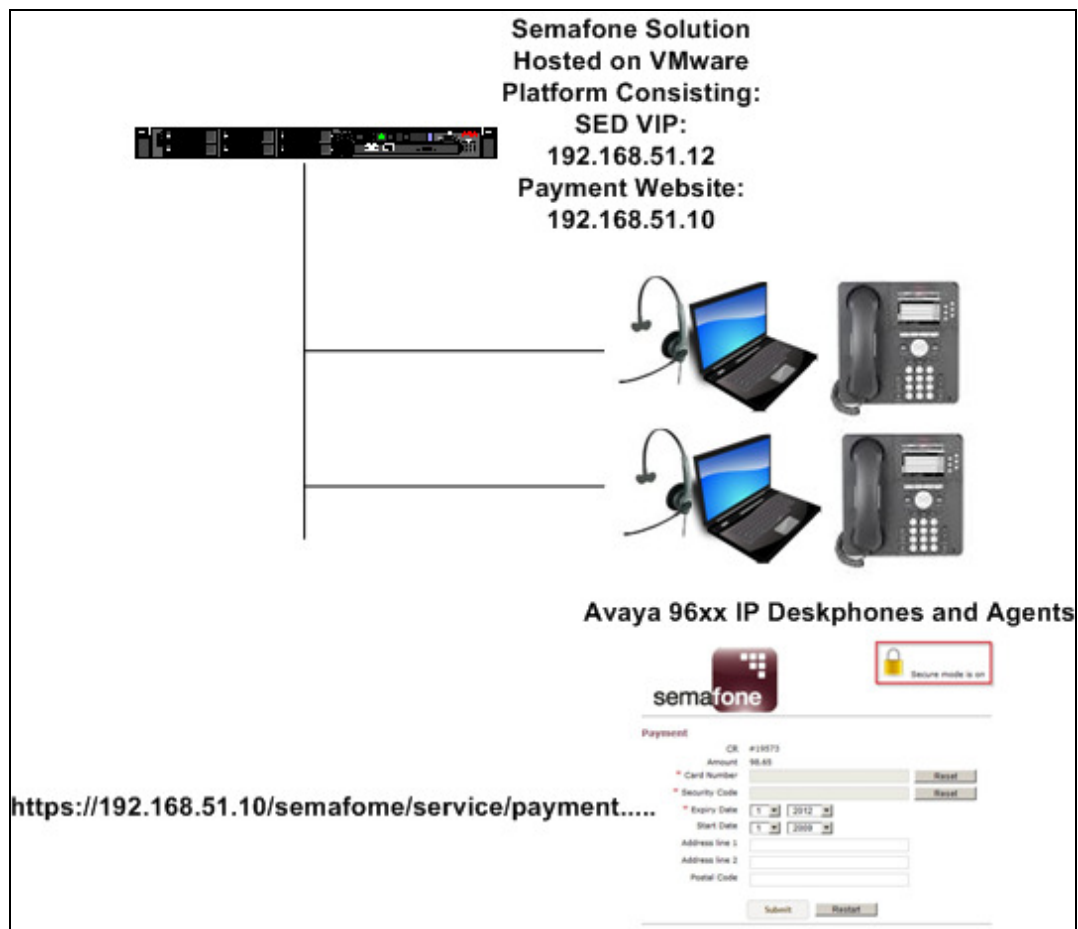


Figure 2: Avaya Agents and workstations with Semafone payment network

Note: The Semafone SED Virtual Machine is a high availability firewall and router appliance. It helps Semafone achieve Network Segmentation in the customer environment by creating a secure Semafone PCI Zone.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.2 SP5 build R016x.02.0.823.0-20396
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 SP4
Avaya Session Border Controller for Enterprise	4.0 Q19
Avaya G450 Media Gateway	32.24.0
Avaya 9630 IP Deskphone	H323 3.2
Semafone hosted on VMware ESXi 5.0 infrastructure	v3

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Configure Routing
- Configure DTMF option

5.1. Configure Routing

The AAR table must be configured with the relevant routing entry for calls to the simulated SIP Service Provider. In this instance trunk-group 1 is already configured as the SIP trunk to Session Manager and route-pattern 1 is configured to route calls over this trunk group. Enter the command **change aar analysis 0**. In the **Dialed String** column enter the digits which will be routed to the SIP Service Provider, in this case **20**. Set the **Total Min** and **Max** value to **4** and the **Route Pattern** value to **1**. When a 4-digit string is dialed beginning with 20, the call will route to Session Manager. The Session Manager configuration later in this document explains how the call is then routed to the SIP Service Provider via the Semafone gateway and the Avaya Session Border Controller for Enterprise.

change aar analysis 0						Page	1	of	2
AAR DIGIT ANALYSIS TABLE									
Location: all									
Percent Full: 0									
	Dialed String	Total		Route	Call	Node	ANI		
		Min	Max	Pattern	Type	Num	Reqd		
	13	4	4	4	aar		n		
	20	4	4	1	unku		n		
	3	11	11	1	unku		n		
	4	4	4	1	aar		n		
	402	4	4	4	aar		n		
	57	4	4	1	aar		n		
	5999	4	4	1	unku		n		
	6	4	4	1	unku		n		

5.2. Configure DTMF option

For the purposes of the compliance test, Communication Manager was configured to send DTMF using either the **in-band** (as part of the RTP stream), **out-of-band** (as a SIP INFO message) or **rtp-payload** (RFC2833 DTMF event) method. Enter the command **change signaling-group x** where **x** is the signaling group in relation to the SIP trunk-group connecting to Session Manager, and configure the **DTMF over IP** field as appropriate.

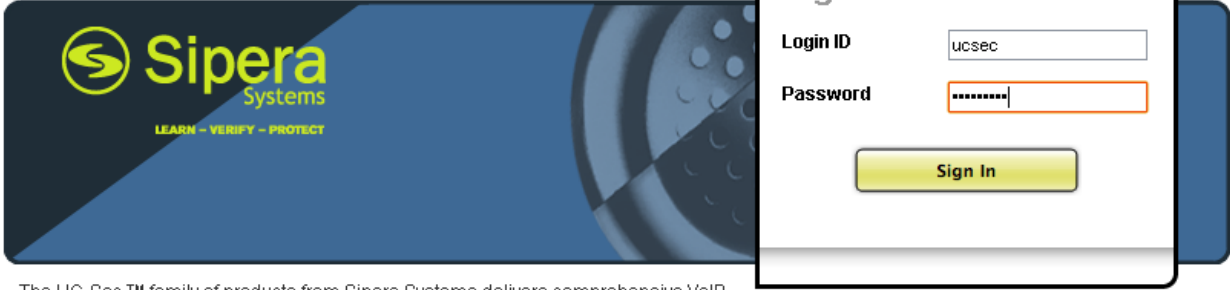
change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: sm62sigint	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: in-band	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 6	

6. Configure Avaya Session Border Controller for Enterprise

These Application Notes assume that the installation of ASBCE and the assignment of a Management IP Address has already been completed.

6.1. Access Management Interface

Use a WEB browser to access the web management interface by entering URL <https://<ip-addr>>, where <ip-addr> is the management LAN IP address assigned during installation. Select **UCSec Control Center** (not shown) on the displayed web page, and log in using proper login credentials.



The UC-Sec™ family of products from Siper Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Siper Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

6.2. System Status

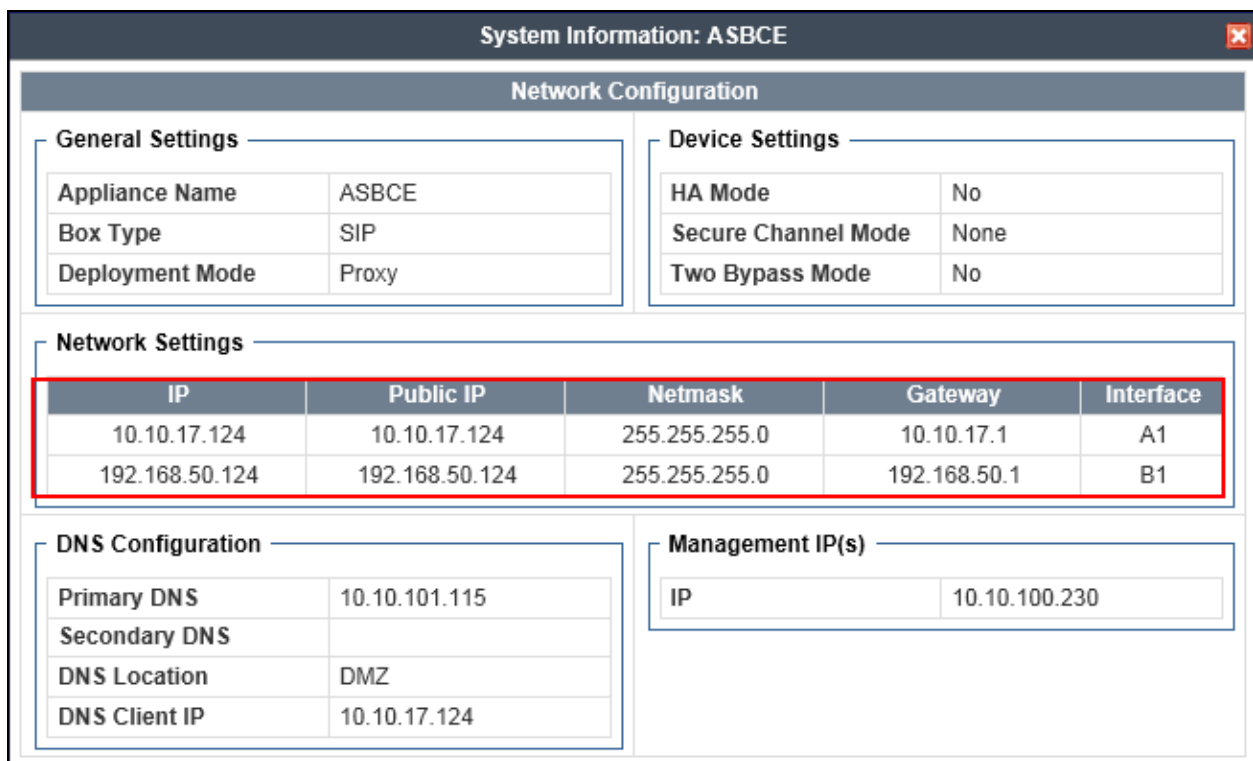
Navigate to **UC-Sec Control Center** → **System Management**. A list of installed devices is shown in the right pane. For the sample configuration, a single device named **ASBCE** is shown. The **Status** will appear as **Commissioned** as shown below.



The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a navigation menu with options like Alarms, Incidents, Statistics, Logs, Diagnostics, Users, and System Management. The main area is titled 'System Management' and has tabs for 'Installed' and 'Updates'. Below these tabs is a table listing installed devices. The table has columns for Device Name, Serial Number, Version, and Status. A single device named 'ASBCE' is listed with serial number 'IPCS31031233' and version '4.0.5.Q19'. The status is 'Commissioned', indicated by a green circle icon. The 'Status' column header and the 'ASBCE' device name are highlighted with red boxes.

Device Name	Serial Number	Version	Status
ASBCE	IPCS31031233	4.0.5.Q19	Commissioned

To view the network information of this device, which was assigned during installation, click the **View Config** icon button (the third icon from the right). A **Network Configuration** window is displayed as shown below. Note that the **A1** and **B1** interface IP addresses correspond to the Private and Public interfaces, respectively, for the ASBCE as shown in **Figure 1** in **Section 3**.

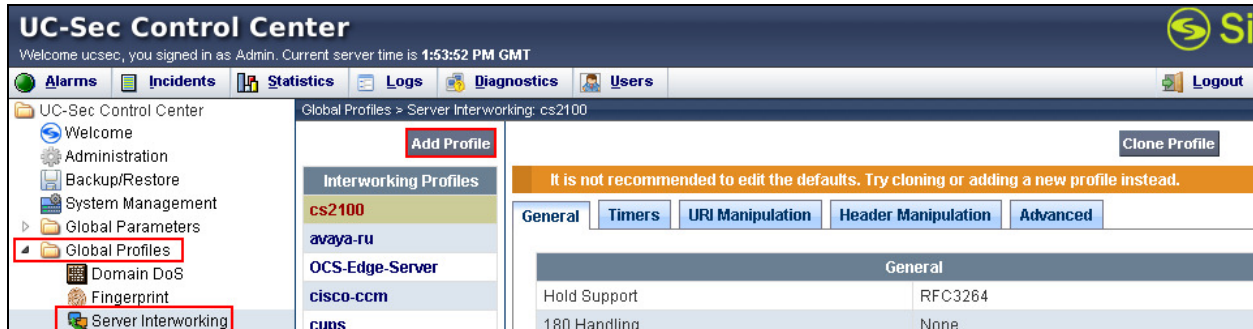


The screenshot shows the 'System Information: ASBCE' window. It has a title bar with a close button. The main content is titled 'Network Configuration' and is divided into several sections: General Settings, Device Settings, Network Settings, DNS Configuration, and Management IP(s). The Network Settings section contains a table with IP addresses for interfaces A1 and B1. The table has columns for IP, Public IP, Netmask, Gateway, and Interface. The rows for A1 and B1 are highlighted with a red box.

IP	Public IP	Netmask	Gateway	Interface
10.10.17.124	10.10.17.124	255.255.255.0	10.10.17.1	A1
192.168.50.124	192.168.50.124	255.255.255.0	192.168.50.1	B1

6.3. Global Profiles – Add Server Interworking Profiles

An interworking profile must be administered to define the features supported by the relevant server configured in **Section 6.4**. Server interworking is defined for each server connected to ASBCE. For the compliance test, the Simulated SIP Service Provider serves as the Trunk Server and the Semafone SIG interface serves as the Call Server. Navigate to **Global Profiles → Server Interworking** from the left-side menu and click **Add Profile** to configure new server interworking profiles.



Enter an appropriate **Profile Name** such as **Avaya SM** shown below and click **Next**.

Interworking Profile

Profile Name: Avaya SM

Next

The **General** page is displayed. In the sample configuration, **T.38 Support** was checked to enable T.38 faxing (though not relevant to the configuration), and **Hold Support** was set for **RFC2543**. Click **Next**.

Interworking Profile

General

Hold Support	<div><div><input type="radio"/> None</div><div><input checked="" type="radio"/> RFC2543 - c=0.0.0.0</div><div><input type="radio"/> RFC3264 - a=sendonly</div></div>
180 Handling	<div><input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP</div>
181 Handling	<div><input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP</div>
182 Handling	<div><input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP</div>
183 Handling	<div><input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP</div>
Refer Handling	<div><input type="checkbox"/></div>
3xx Handling	<div><input type="checkbox"/></div>
Diversion Header Support	<div><input type="checkbox"/></div>
Delayed SDP Handling	<div><input type="checkbox"/></div>
T.38 Support	<div><input checked="" type="checkbox"/></div>
URI Scheme	<div><input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY</div>
Via Header Format	<div><div><input checked="" type="radio"/> RFC3261</div><div><input type="radio"/> RFC2543</div></div>

Back

Next

Leave the **Privacy** and **DTMF** fields at their default values and click **Next**.

Interworking Profile

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Next

Leave the **SIP Timers** and **Transport Timers** fields at their default values and click **Next**.

Interworking Profile

Configuration is not required. All fields are optional.

SIP Timers

Min-SE	<input type="text"/>	seconds, [90 - 86400]
Init Timer	<input type="text"/>	milliseconds, [50 - 1000]
Max Timer	<input type="text"/>	milliseconds, [200 - 8000]
Trans Expire	<input type="text"/>	seconds, [1 - 64]
Invite Expire	<input type="text"/>	seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer	<input type="text"/>	seconds, [600 - 3600]
-------------------------------	----------------------	-----------------------

Back

Next

Leave the **Advanced Settings** fields at their default values and click **Finish**.

Interworking Profile

Advanced Settings

Record Routes	<input checked="" type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

Similarly add an identical interworking profile for the public side of the ASBCE named **PUBLIC**. The screenshot below displays the two newly administered profiles.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 1:41:10 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Subscriber Profiles

Global Profiles > Server Interworking: cs2100

Add Profile Clone Profile

Interworking Profiles

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- Sipera-Halo
- OCS-FrontEnd-Server
- Avaya SM
- PUBLIC

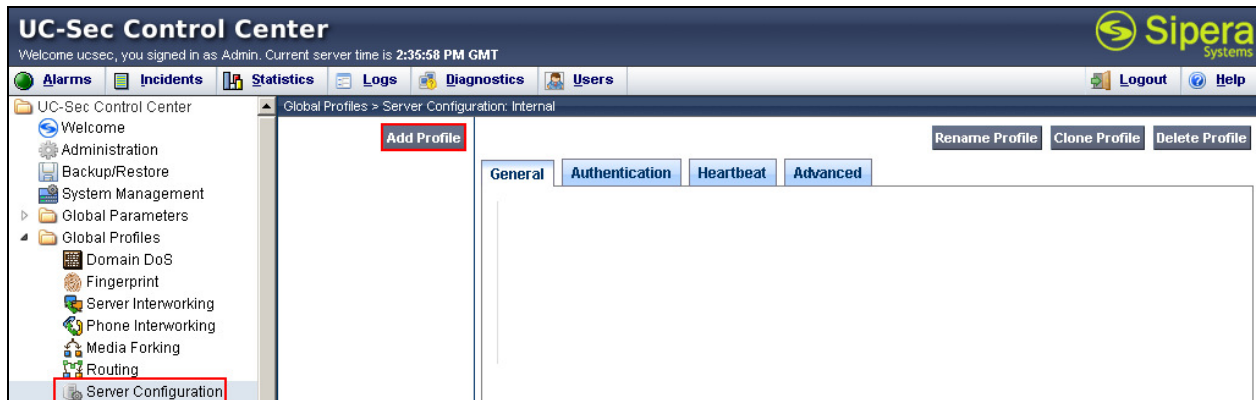
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General Timers URI Manipulation Header Manipulation Advanced

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No

6.4. Global Profiles – Server Configuration

In the compliance test, the Simulated SIP Service Provider is administered and connected as the Trunk Server and the Semafone SIG interface is administered and connected as the Call Server. Navigate to **Global Profiles → Server Configuration** from the left-side menu and click **Add Profile** to configure the first of the two servers.



Enter an appropriate **Profile Name** such as **Internal** shown below. Click **Next**.

This is a screenshot of a modal dialog box titled 'Add Server Configuration Profile'. It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled 'Profile Name' which contains the text 'Internal'. Below the input field is a button labeled 'Next'.

Configure the **General** fields as follows:

- **Server Type** – select **Call Server** from the drop down box
- **IP Addresses / Supported FQDNs** - enter the IP address assigned to the Semafone SIG interface, in this case **10.10.17.195**
- **Supported Transports** –place a check in the **TCP** and **UDP** boxes
- **TCP Port** and **UDP Port** – set to **5060**

This configuration relates to the connection between the ASBCE private interface and the Semafone SIG interface. Click **Next**.

Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.10.17.195
Supported Transports	<input checked="" type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	5060
TLS Port	

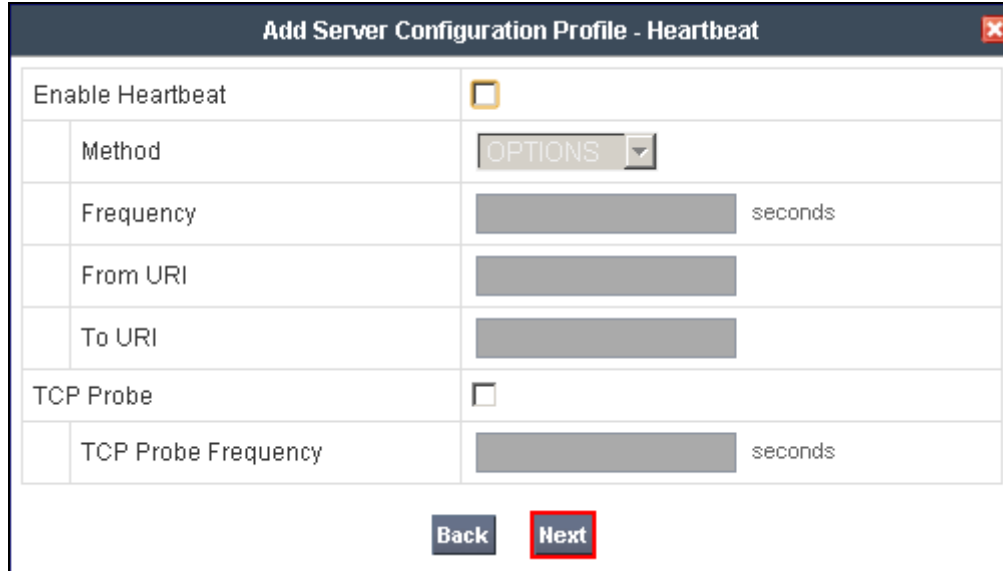
Back Next

Leave the **Authentication** screen fields at their default values and click **Next**.

Enable Authentication	<input type="checkbox"/>
User Name	
Realm (Leave blank to detect from server challenge)	
Password	
Confirm Password	

Back Next

Leave the **Heartbeat** fields at their default values and click **Next**.

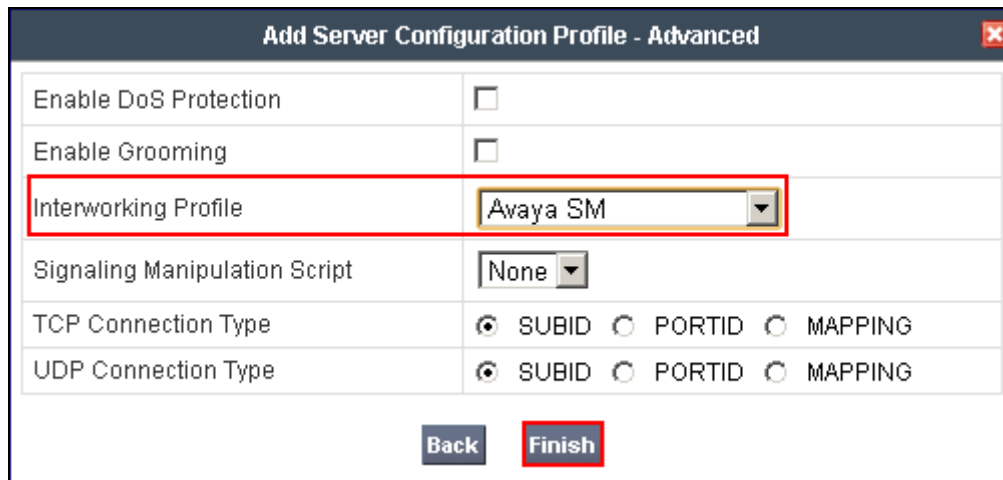


The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat". It contains several fields for configuring heartbeat settings. The "Enable Heartbeat" checkbox is unchecked. The "Method" dropdown is set to "OPTIONS". The "Frequency" field is empty, with "seconds" as a unit label. The "From URI" and "To URI" fields are empty. The "TCP Probe" checkbox is unchecked. The "TCP Probe Frequency" field is empty, with "seconds" as a unit label. At the bottom, there are "Back" and "Next" buttons. The "Next" button is highlighted with a red border.

Enable Heartbeat	<input type="checkbox"/>
Method	OPTIONS
Frequency	<input type="text"/> seconds
From URI	<input type="text"/>
To URI	<input type="text"/>
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	<input type="text"/> seconds

Back Next

From the drop down box select the **Interworking Profile** configured in the previous section for the internal side of the ASBCE, in this case **Avaya SM**. Leave all other fields at their default values and click **Finish**.

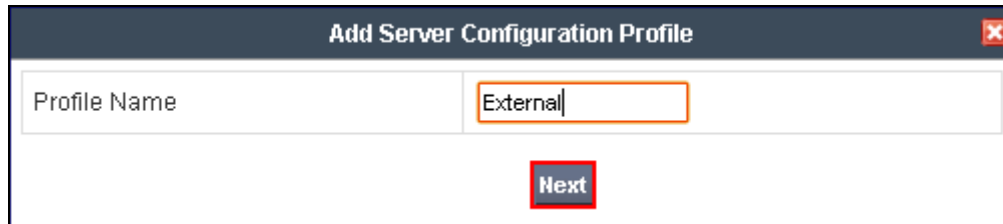


The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains several fields for configuring advanced settings. The "Enable DoS Protection" and "Enable Grooming" checkboxes are unchecked. The "Interworking Profile" dropdown is set to "Avaya SM" and is highlighted with a red border. The "Signaling Manipulation Script" dropdown is set to "None". The "TCP Connection Type" and "UDP Connection Type" fields have radio buttons for "SUBID", "PORTID", and "MAPPING", with "SUBID" selected for both. At the bottom, there are "Back" and "Finish" buttons. The "Finish" button is highlighted with a red border.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya SM
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back Finish

Repeat the steps above to configure the Server for the Public side of the ASBCE. Enter an appropriate **Profile Name** such as **External** shown below. Click **Next**.



Add Server Configuration Profile

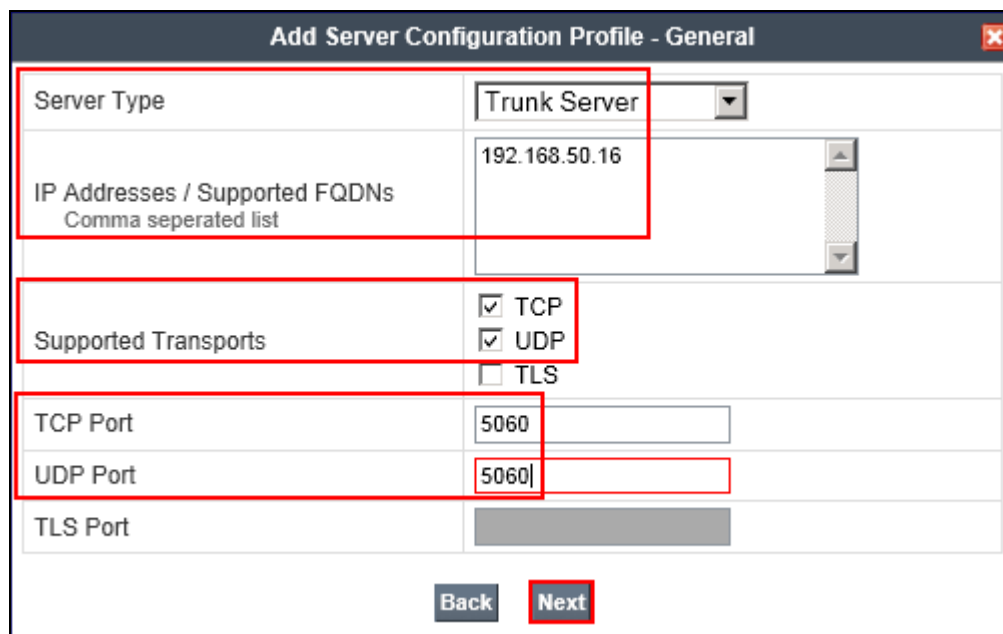
Profile Name: External

Next

Configure the **General** fields as follows:

- **Server Type** – select **Trunk Server** from the drop down box
- **IP Addresses / Supported FQDNs** - enter the IP address assigned to the Simulated SIP Service Provider, in this case **192.168.50.16**
- **Supported Transports** –place a check in the **TCP** and **UDP** boxes.
- **TCP Port** and **UDP Port** – set to **5060**

This configuration relates to the connection between the ASBCE public interface and the Simulated SIP Service Provider.



Add Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Comma seperated list: 192.168.50.16

Supported Transports:
☒ TCP
☒ UDP
☐ TLS

TCP Port: 5060

UDP Port: 5060

TLS Port:

Back Next

Leave the **Authentication** screen fields at their default values and click **Next**.

Add Server Configuration Profile - Authentication

Enable Authentication

☐

User Name

Realm
(Leave blank to detect from server challenge)

Password

Confirm Password

Back

Next

Leave the **Heartbeat** fields at their default values and click **Next**.

Add Server Configuration Profile - Heartbeat

Enable Heartbeat

☐

Method

OPTIONS

Frequency

seconds

From URI

To URI

TCP Probe

☐

TCP Probe Frequency

seconds

Back

Next

From the drop down box select the **Interworking Profile** configured in the previous section for the Public side of the ASBCE, in this case **PUBLIC**. Leave all other fields at their default values and click **Finish**.

Add Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	PUBLIC
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

The following screen will appear displaying the newly administered Server Configuration Profiles

UC-Sec Control Center
 Welcome ucsec, you signed in as Admin. Current server time is 12:44:41 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration

Global Profiles > Server Configuration: Internal

Add Profile

Profile: Internal (Selected), External

Rename Profile Clone Profile Delete Profile

General Authentication Heartbeat Advanced

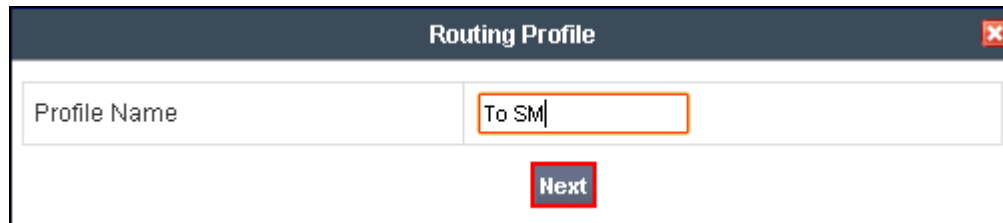
General	
Server Type	Call Server
IP Addresses / FQDNs	10.10.17.195
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

Edit

6.5. Global Profiles – Routing

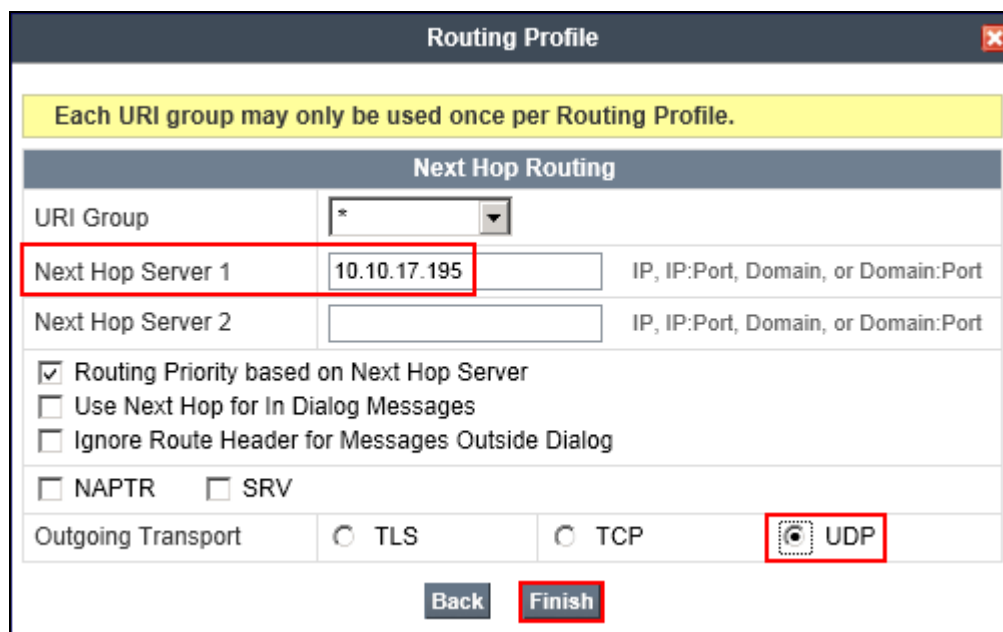
Routing information is required for traffic to be routed to Session Manager via Semafone on the internal side, and to the Simulated SIP Service Provider on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. If no port is specified, the default SIP port of 5060 is used.

Navigate to **Global Profiles → Routing → Add Profile**. Enter an appropriate **Profile Name** such as **To SM** as shown below. Click **Next**.



The screenshot shows a 'Routing Profile' configuration window. It has a title bar with a close button. Below the title bar, there is a text input field labeled 'Profile Name' containing the text 'To SM'. Below the input field is a red 'Next' button.

In the **Next Hop Routing** configuration, enter the IP Address of the Semafone SIG interface as **Next Hop Server 1**, as shown below. Choose **UDP** for **Outgoing Transport** and click **Finish**.



The screenshot shows the 'Routing Profile' configuration window with the 'Next Hop Routing' section expanded. A yellow warning banner at the top states 'Each URI group may only be used once per Routing Profile.' Below this, the 'Next Hop Routing' section contains a 'URI Group' dropdown menu with an asterisk. Below the dropdown are two rows for 'Next Hop Server 1' and 'Next Hop Server 2'. The 'Next Hop Server 1' row has the IP address '10.10.17.195' entered. Below these rows are three checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), and 'Ignore Route Header for Messages Outside Dialog' (unchecked). Below these are two more checkboxes: 'NAPTR' (unchecked) and 'SRV' (unchecked). At the bottom, there is a section for 'Outgoing Transport' with three radio buttons: 'TLS' (unchecked), 'TCP' (unchecked), and 'UDP' (checked). Below the radio buttons are 'Back' and 'Finish' buttons.

Similarly create a Routing Profile to the Simulated Service Provider interface.

Routing Profile

Profile Name:

Next

Note the **Next Hop Server 1** IP address is that assigned to the Simulated SIP Service Provider and the **Outgoing Transport** is **TCP**. Click **Finish**.

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group: *

Next Hop Server 1: IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2: IP, IP:Port, Domain, or Domain:Port

☒ Routing Priority based on Next Hop Server

☐ Use Next Hop for In Dialog Messages

☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport: ☐ TLS ☒ **TCP** ☐ UDP

Back **Finish**

The screenshot below shows the newly configured Routing Profiles.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 5:04:09 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: default

Add Profile **Clone Profile**

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Routing Profiles

default

To SM

To Public

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	---	---	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None

6.6. Global Profiles – Topology Hiding

Topology Hiding is a security feature which allows the changing of several parameters within SIP packets, preventing the private enterprise network information from being propagated to the un-trusted public network. Topology Hiding can also be used as an interoperability tool to adapt certain parameters in selected SIP headers to meet expectations by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case. For the compliance test, only the minimum configuration required to achieve interoperability was performed.

Navigate to **Global Profiles → Topology Hiding → Add Profile**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Parameters, Global Profiles, and Topology Hiding. The main area displays the 'Global Profiles > Topology Hiding: default' configuration. It includes an 'Add Profile' button, a 'Clone Profile' button, and a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this is a table titled 'Topology Hiding' with columns: Header, Criteria, Replace Action, and Overwrite Value. The table lists several SIP headers (Via, Record-Route, From, To, SDP, Request-Line) with their respective criteria (IP/Domain), replace actions (Auto), and overwrite values (---). An 'Edit' button is located at the bottom right of the table.

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

Enter a **Profile Name** such as **Internal** shown below. Click **Next**.

The screenshot shows the 'Topology Hiding Profile' configuration dialog. It has a title bar with a close button. Inside, there is a 'Profile Name' label and a text input field containing the word 'Internal'. Below the input field is a 'Next' button.

The screen below will appear. For the purposes of the compliance test it was unnecessary to make any changes or additions. Click **Finish**.

The screenshot shows the 'Topology Hiding Profile' configuration dialog. It has a title bar with a close button. Inside, there is an 'Add Header' button. Below it is a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The table contains one row with 'Request-Line' in the Header column, 'IP/Domain' in the Criteria column, 'Auto' in the Replace Action column, and a greyed-out 'Overwrite Value' column. At the bottom of the dialog are 'Back' and 'Finish' buttons.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

Similarly, configure a Topology Hiding Profile for the **External** interface.

Topology Hiding Profile

Profile Name: External

Next

Click **Finish** when completed.

Topology Hiding Profile

Add Header

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

Back Finish

The screenshot below shows the newly configured Topology Hiding Profiles.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 5:07:29 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Topology Hiding: default

Add Profile Clone Profile

Topology Hiding Profiles

- default
- cisco_th_profile
- Internal**
- External**

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Auto	---
To	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

Edit

6.7. Device Specific Settings – Network Management

The network information should have been previously specified during installation of the ASBCE.

Navigate to **Device Specific Settings → Network Management** from the left-side menu. Under **UC-Sec Devices**, select the device being managed, which was named **ASBCE** in the sample configuration. The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask**, **Gateway** and **Interface** information previously assigned. Note that only the **A1** and **B1** interfaces are used. Typically the A interfaces are used for the internal side and B interfaces are used for the external side of the ASBCE.

The screenshot shows the 'UC-Sec Control Center' interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, and 'Network Management' selected. The main area is titled 'Device Specific Settings > Network Management: ASBCE'. It has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.0), and 'B2 Netmask'. There is an 'Add IP' button and 'Save Changes' and 'Clear Changes' buttons. A table lists IP configurations:

IP Address	Public IP	Gateway	Interface	
10.10.17.124		10.10.17.1	A1	X
192.168.50.124		192.168.50.1	B1	X

Select the **Interface Configuration** tab. The **Administrative Status** can be toggled between **Enabled** and **Disabled** in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.

The screenshot shows the 'UC-Sec Control Center' interface. The left sidebar is the same as the previous screenshot. The main area is titled 'Device Specific Settings > Network Management: ASBCE'. It has two tabs: 'Network Configuration' and 'Interface Configuration' (active). A table lists the interfaces and their administrative status:

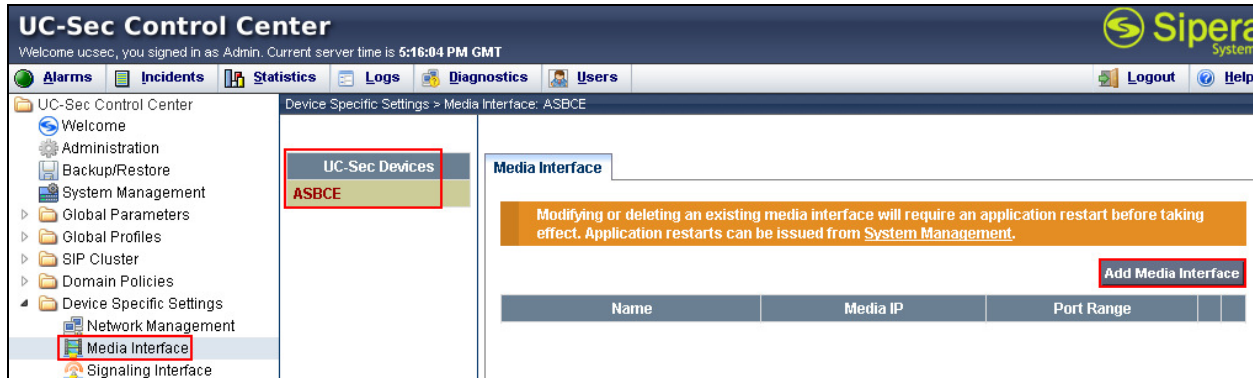
Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

When IP addresses and network masks are assigned to interfaces, these are then configured as Signaling Interfaces and Media Interfaces.

6.8. Device Specific Settings – Media Interface

Media Interfaces are created to adjust the port range assigned to media streams leaving the interfaces of ASBCE. The compliance test used the default port range of 35000 to 40000.

Navigate to **Device Specific Setting → Media Interface**. Under **UC-Sec Devices**, select the device being managed, which was named **ASBCE** in the sample configuration, and select **Add Media Interface**.



Enter an appropriate **Name** for the Media Interface facing the enterprise and select the inside private IP Address of the ASBCE from the **IP Address** drop-down menu. In the sample configuration, **Internal** was chosen as the **Name**, and the inside IP Address of the ASBCE is **10.10.17.124**. Leave the Port Range at its default value and click **Finish**.

The 'Add Media Interface' dialog box is shown. The 'Name' field contains 'Internal'. The 'IP Address' field is a dropdown menu showing '10.10.17.124'. The 'Port Range' field shows '35000 - 40000'. A 'Finish' button is at the bottom.

Similarly repeat the same for the Public interface.

The 'Add Media Interface' dialog box is shown. The 'Name' field contains 'Public'. The 'IP Address' field is a dropdown menu showing '192.168.50.124'. The 'Port Range' field shows '35000 - 40000'. A 'Finish' button is at the bottom.

The screenshot below shows the newly configured Media Interfaces.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, showing 'Media Interface' selected. The main content area is titled 'Device Specific Settings > Media Interface: ASBCE'. It features a 'Media Interface' tab and a table with two entries: 'Internal' and 'Public'. The 'Internal' entry has a Media IP of 10.10.17.124 and a Port Range of 35000 - 40000. The 'Public' entry has a Media IP of 192.168.50.124 and a Port Range of 35000 - 40000. A red box highlights the 'Internal' row. An orange warning banner at the top states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' A red box highlights the 'Add Media Interface' button.

Name	Media IP	Port Range		
Internal	10.10.17.124	35000 - 40000		
Public	192.168.50.124	35000 - 40000		

6.9. Device Specific Settings – Signaling Interface

Navigate to **Device Specific Settings → Signaling Interface**. Under **UC-Sec Devices**, select the device being managed, which was named **ASBCE** in the sample configuration and select **Add Signaling Interface**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, showing 'Signaling Interface' selected. The main content area is titled 'Device Specific Settings > Signaling Interface: ASBCE'. It features a 'Signaling Interface' tab and a table with columns: Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. A red box highlights the 'Add Signaling Interface' button.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
------	--------------	----------	----------	----------	-------------

In the **Add Signaling Interface** screen, enter an appropriate **Name** for the inside interface, and choose the private, inside IP Address of the ASBCE from the **IP Address** drop-down menu. Enter **5060** for the **UDP Port** since **UDP** port **5060** is used for the SIP connection between Semafone and ASBCE in the sample configuration. Click **Finish**.

Add Signaling Interface

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

Name	Internal
IP Address	10.10.17.124
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

Finish

Similarly enter an appropriate **Name** for the external interface, and choose the public, external IP Address of the ASBCE from the **IP Address** drop-down menu. Enter **5060** for the **TCP Port** since TCP port **5060** is used for the SIP Trunk between ASBCE and the Simulated SIP Service Provider in the sample configuration. Click **Finish**.

Add Signaling Interface

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

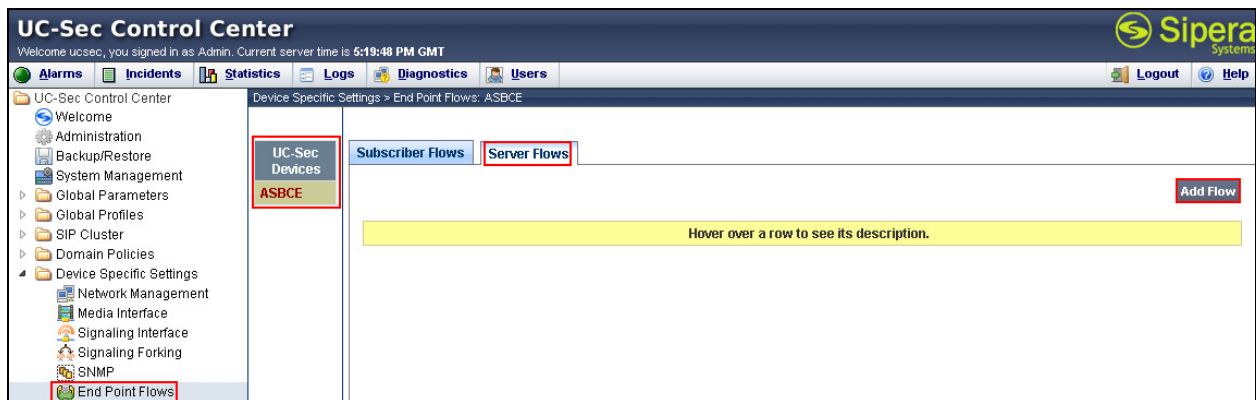
Name	Public
IP Address	192.168.50.124
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

Finish

6.10. Device Specific Settings – End Point Flows

End Point Flows combine the previously defined profiles into an outgoing flow from the Call Server (SemaFone) to the Trunk Server (Simulated SIP Service Provide) and an incoming flow from the Trunk Server to the Call Server. This configuration ties all the previously entered information together so that calls can be routed from SemaFone to the Simulated SIP Service Provider and vice versa.

Select **Device Specific Settings → End Point Flows**. Under **UC-Sec Devices**, select the device being managed, which was named **ASBCE** in the sample configuration, and select the **Server Flows** tab. Select **Add Flow**.



Configure a server flow from the internal network to the public network.

Criteria	
Flow Name	FromInternalToPublic
Server Configuration	External
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	Public
Media Interface	Public
End Point Policy Group	default-low
Routing Profile	To SM
Topology Hiding Profile	External
File Transfer Profile	None

Finish

- Flow Name FromInternalToPublic [described as “SemaFone to the Simulated SIP Service Provider and vice versa”]
- Server Configuration: **External**: Simulated SIP Service Provider **192.168.50.16**
- Received Interface: **Internal**:
- Signaling Interface: **Public**: SBCE Public Interface **192.168.50.124**
- Media Interface: **Public**: SBCE Public Interface **192.168.50.124**
- Routing profile: **To SM**: SemaFone ‘Dirty’ Interface **10.10.17.195**
- Topology Hiding Profile: **External**

Similarly, configure a server flow from the public to the internal network.

Criteria	
Flow Name	FromPublicToInternal
Server Configuration	Internal
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	default-low
Routing Profile	To Public
Topology Hiding Profile	Internal
File Transfer Profile	None

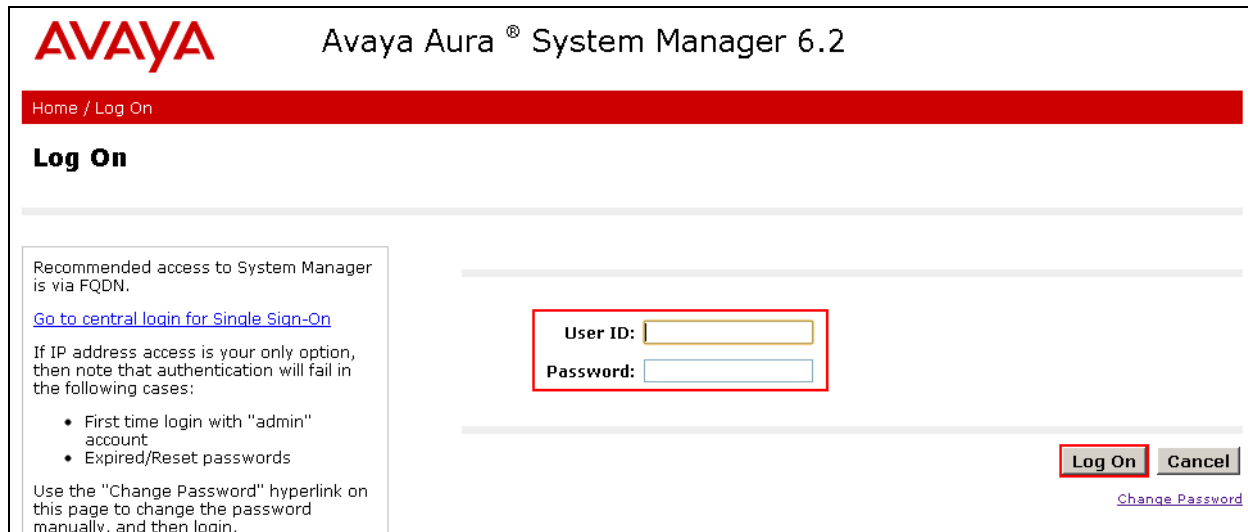
Finish

- Flow Name FromPublicToInternal [described as “SemaFone to the Simulated SIP Service Provider and **vice versa**”]
- Server Configuration: **Internal**: SemaFone SIG interface **10.10.17.195**
- Received Interface: **Public**:
- Signaling Interface: **Internal**: inside IP Address of the ASBCE **10.10.7.124**
- Media Interface: **Internal**: inside IP Address of the ASBCE **10.10.7.124**
- Routing profile: **To Public**: Simulated SIP Service Provider **192.168.50.16**
- Topology Hiding Profile: **Internal**
-

7. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Session Manager configuration required for interoperating with Semafone.

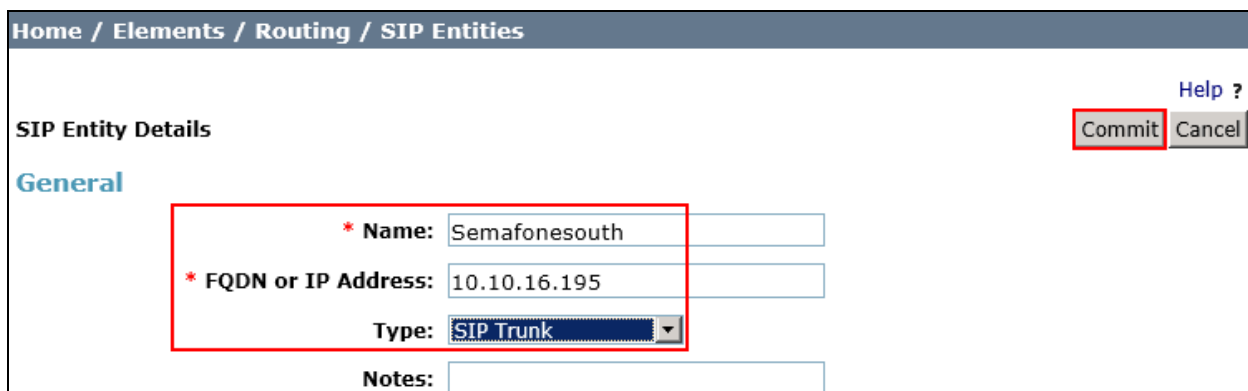
Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button.



The screenshot shows the Avaya Aura System Manager 6.2 Log On page. The header includes the Avaya logo and the title "Avaya Aura® System Manager 6.2". Below the header is a red navigation bar with "Home / Log On". The main heading is "Log On". On the left, there is a text box with instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: First time login with 'admin' account, Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login." On the right, there are input fields for "User ID:" and "Password:". Below these fields are "Log On" and "Cancel" buttons. A "Change Password" link is also present at the bottom right.

7.1. Configure Semafone SIP Entity

A SIP Entity must be created for the Semafone SIG interface. Click **Routing → SIP Entities → New**. Assign an identifying **Name** and the **FQDN or IP Address** for the Semafone clean interface, set the **Type** field to **SIP Trunk**, and click **Commit** when done.



The screenshot shows the "SIP Entity Details" form in the System Manager. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page has a "Help ?" link and "Commit" and "Cancel" buttons. The "General" section is active. It contains three required fields: "Name" with the value "Semaforesouth", "FQDN or IP Address" with the value "10.10.16.195", and "Type" with a dropdown menu set to "SIP Trunk". There is also a "Notes" field at the bottom.

7.2. Configure Entity Link

The configuration of an Entity Link connects the Session Manager SIP Entity with the Semafone SIP Entity. Click **Routing → Entity Links → New**. Assign an identifying **Name**, choose the entity assigned to the preconfigured Session Manager SIP Signaling Interface as **SIP Entity 1**, set the **Protocol** as **UDP**, enter **5060** for the **Port**, choose the Semafone SIP entity as **SIP Entity 2**, set the **Port** to **5060**, and select **Trusted** from the **Connection Policy** drop down box. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to Semafone.

Home / Elements / Routing / Entity Links

Entity Links

Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
*ToSemafone	*SM62	UDP	*5060	*Semafonesouth	*5060	Trusted	

7.3. Create Routing Policy

Click **Routing → Routing Policies → New**. Assign an identifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select**.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

* Name: ToSemafonesouth

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Choose the Semafone Entity configured in **Section 7.1** and click **Select**.

Home / Elements / Routing / Routing Policies

SIP Entity List Select Cancel

SIP Entities

16 Items [Refresh](#) Filter: [Enable](#)

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	CM62	10.10.16.142	CM	
<input type="radio"/>	CMM62	10.10.16.142	CM	
<input checked="" type="radio"/>	Semaforesouth	10.10.16.195	SIP Trunk	

Review the configuration and click **Commit** when done.

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Semaforesouth	10.10.16.195	SIP Trunk	

7.4. Administer Dial Patterns

Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate destination. In **Section 5.1** Communication Manager is configured to route 4-digit strings beginning with 20 to Session Manager. To create a Dial Pattern to route these digits from Session Manager to Semafone click **Routing → Dial Patterns → New**. Under **General** enter the number presented to Session Manager by Communication Manager in the **Pattern** box. Set the **Min** and **Max** digit string length, and set **SIP Domain** to **-ALL-**. In the **Originating Locations and Routing Policies** section of the web page, click **Add**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Help ?](#)

General

* Pattern: 20

* Min: 4

* Max: 4

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Place a tick in the **Apply The Selected Routing Policies to All Originating Locations** tick box, and select the **Routing Policy** created in **Section 7.3**. Click **Select** when done

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns](#)

Originating Location and Routing Policy List Select Cancel

Originating Location

☒ **Apply The Selected Routing Policies to All Originating Locations**

1 Item [Refresh](#) Filter: [Enable](#)

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	DevConnectLab	

Select : [All](#), [None](#)

Routing Policies

12 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToCM6.2	<input type="checkbox"/>	CM62	
<input type="checkbox"/>	ToCMM62	<input type="checkbox"/>	CMM62	
<input checked="" type="checkbox"/>	ToSemaforesouth	<input type="checkbox"/>	Semaforesouth	

Review the configuration and click **Commit** when done.

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns](#)

[Help ?](#)

Dial Pattern Details

Commit

Cancel

General

* Pattern:

20

* Min:

4

* Max:

4

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

[Refresh](#)

Filter: [Enable](#)

<input checked="" type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input checked="" type="checkbox"/>	-ALL-	Any Locations	ToSemaforesouth	0	<input type="checkbox"/>	Semaforesouth

Similarly, configure the appropriate Dial Patterns for routing calls arriving via ASBCE from the PSTN to Communication Manager. For the purpose of the compliance testing, Dial Patterns were administered to route 58xx, (shown below), and 6xxx (not shown) digit strings to Communication Manager.

Home / Elements / Routing / Dial Patterns

[Help ?](#)

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ToCM6.2	0	<input type="checkbox"/>	CM62	

8. Configure SemaFone

The SemaFone solution is installed, configured and commissioned directly by SemaFone. The following items summarise the configuration options selected which are pertinent to the interworking scenarios discussed. Additional configuration, unrelated to interworking with the Avaya solution components, is required, but is not detailed here. No unusual settings are required by SemaFone for successful interworking.

8.1. Configure Interfaces

The two external interfaces of the SIG must be configured to take the correct IP addresses for the networks into which they will be deployed. In the file `/etc/network/interfaces`, **eth1** represents the “clean” interface, and **eth0** represents the “dirty” interface. Standard IPv4 parameters are specified here and referenced in **Figure 1**:

```
auto eth0
iface eth0 inet static
    address 10.10.17.195
    netmask 255.255.255.0
    network 10.10.17.0
    broadcast 10.10.17.255

auto eth1
iface eth1 inet static
    address 10.10.16.195
    netmask 255.255.255.0
    network 10.10.16.0
    broadcast 10.10.16.255
```

8.2. Telephony Configuration - SIG

In addition to standard SIG configuration, the following entry must be present in the general section of the SIG’s `/etc/semafone/sip.conf` configuration file in order to define the UDP port on which the SIG will receive SIP signaling (this is a global setting; if this must be changed then the CCM configuration must be adapted to match)..

```
[general]
...
bindport=5060
```

The two entities with which the SIG will communicate must also be defined in this configuration file; one for the “dirty” interface connecting to ASBCE and one for the “clean” interface” connecting to Session Manager. For both entities, the procedure is the same:

- 1) Define IP address of ASBCE and Session Manager in the **host** and **permit** entries – in this case **10.10.17.124** and **10.10.16.148** respectively.
- 2) Specify the required DTMF interworking in the **dtmfmode** entry (**inband**, **info**, or **rfc2833**)
- 3) Select the appropriate G.711 encoding via the **allow** entry (either **alaw** or **ulaw**)

```
[public_dirty]
insecure=invite
type=peer
allow=alaw
deny=0.0.0.0/0.0.0.0
host=10.10.17.124
permit=10.10.17.124/255.255.255.255
context=public_dirty
dtmfmode=inband

[public_clean]
insecure=invite
type=peer
allow=alaw
deny=0.0.0.0/0.0.0.0
host=10.10.16.148
permit=10.10.16.148/255.255.255.255

context=public_clean
dtmfmode=inband
```

8.3. Telephony Configuration – CCM

The Semafone CCM Virtual Machine captures all telephony events and updates the DPM Virtual Machine accordingly. The Semafone DPM Virtual Machine processes secure data and provides access to Semafone APIs. The DPM supports multiple software configurations to accommodate varying integration requirements for payment pages and payment provider integrations.

In order to support extended SIP message lengths seen in the Avaya environment, one change is required to the CCM configuration. On the CCM, in the file **/pkg/ccma/etc/ccm.cfg**, the entry:

```
if (msg:len >= 2048) {
```

should be changed to:

```
if (msg:len >= 4096) {
```

If the SIP port defined in the SIG `/etc/semafone/sip.conf` file above is changed from **5060**, then the following four entries in the `/pkg/ccma/etc/ccm.cfg` must be changed to reflect the new port number:

```
listen=udp:192.168.70.65:5060  
listen=udp:192.168.60.65:5060
```

```
if (dst_ip==192.168.60.65) force_send_socket(192.168.70.65:5060);  
if (dst_ip==192.168.70.65) force_send_socket(192.168.60.65:5060);
```

8.4. Payment Page

No specific configuration of the payment page is required for the integration with Avaya. Due to the abstraction provided by the SIG and CCM components of the SemaFone solution, customization of the payment page to meet specific requirements of the deployment is permissible, and will not impact the telephony integration tested here.

9. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the Avaya and Semafone solution.

9.1. Verify Communication Manager SIP Trunk

Using the SAT, enter the **status signaling-group <n>** command, where <n> is the number of the SIP signaling group which connects to Session Manager. Verify that the signaling **Group State** is **in-service**.

```
status signaling-group 1
                        STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

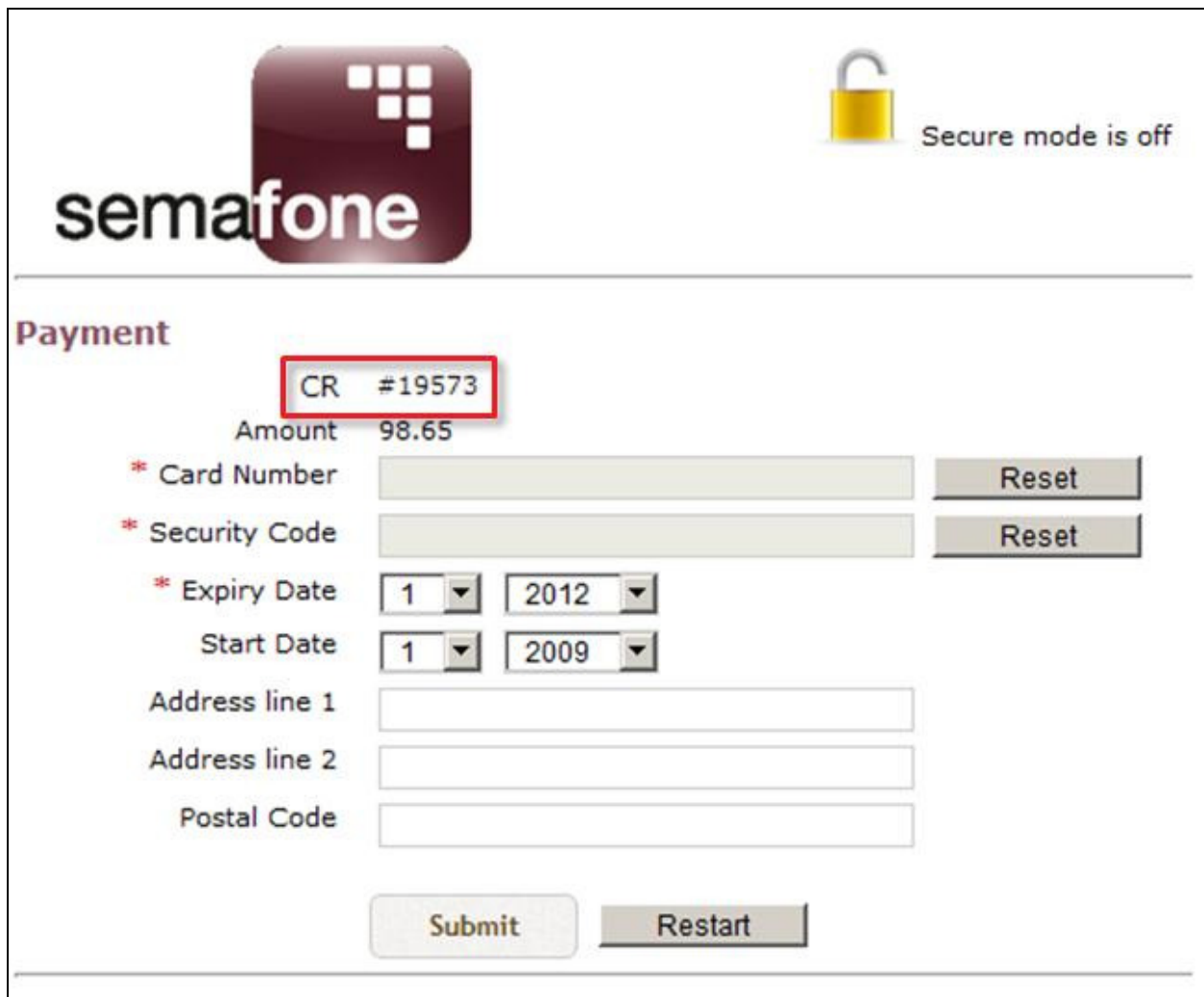
9.2. Verify Entity Link to Semafone

From the System Manager web interface click **Home → Session Manager → System Status → SIP Entity Monitoring**. Click on the entity configured for the Semafone SIP Entity in **Section 7.1** and confirm the **Conn. Status** is **Up**, the **Reason Code** is **200 OK** and the **Link Status** is **Up**.

1 Item Refresh		Filter: Enable					
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	SM62	10.10.16.195	5060	UDP	Up	200 OK	Up

9.3. Verify Call Routing, Semafone DTMF Manipulation and Semafone Payment Page Operation


Place a call to/from the PSTN, ensure the call can be answered, controlled and terminated by a call center agent. When the agent receives a call, the agent navigates to the simulated payment page, retrieves the code displayed in the **CR** field, and enters the code on the telephone keypad.




The screenshot shows the Semafone payment interface. At the top left is the Semafone logo, and at the top right is a yellow padlock icon with the text "Secure mode is off". Below the header, the word "Payment" is displayed in a dark red font. The main form area contains the following elements:

- A red-bordered box containing the text "CR #19573".
- The text "Amount 98.65".
- A field for "Card Number" with a "Reset" button to its right.
- A field for "Security Code" with a "Reset" button to its right.
- An "Expiry Date" field consisting of two dropdown menus, the first showing "1" and the second showing "2012".
- A "Start Date" field consisting of two dropdown menus, the first showing "1" and the second showing "2009".
- A field for "Address line 1".
- A field for "Address line 2".
- A field for "Postal Code".
- At the bottom, there are two buttons: "Submit" and "Restart".

Verify the padlock icon changes indicating the secured state has been entered.



Secure mode is on

Payment

CR #19573

Amount 98.65

* Card Number

Reset

* Security Code

Reset

* Expiry Date

1

▼

2012

▼

Start Date

1

▼

2009

▼

Address line 1

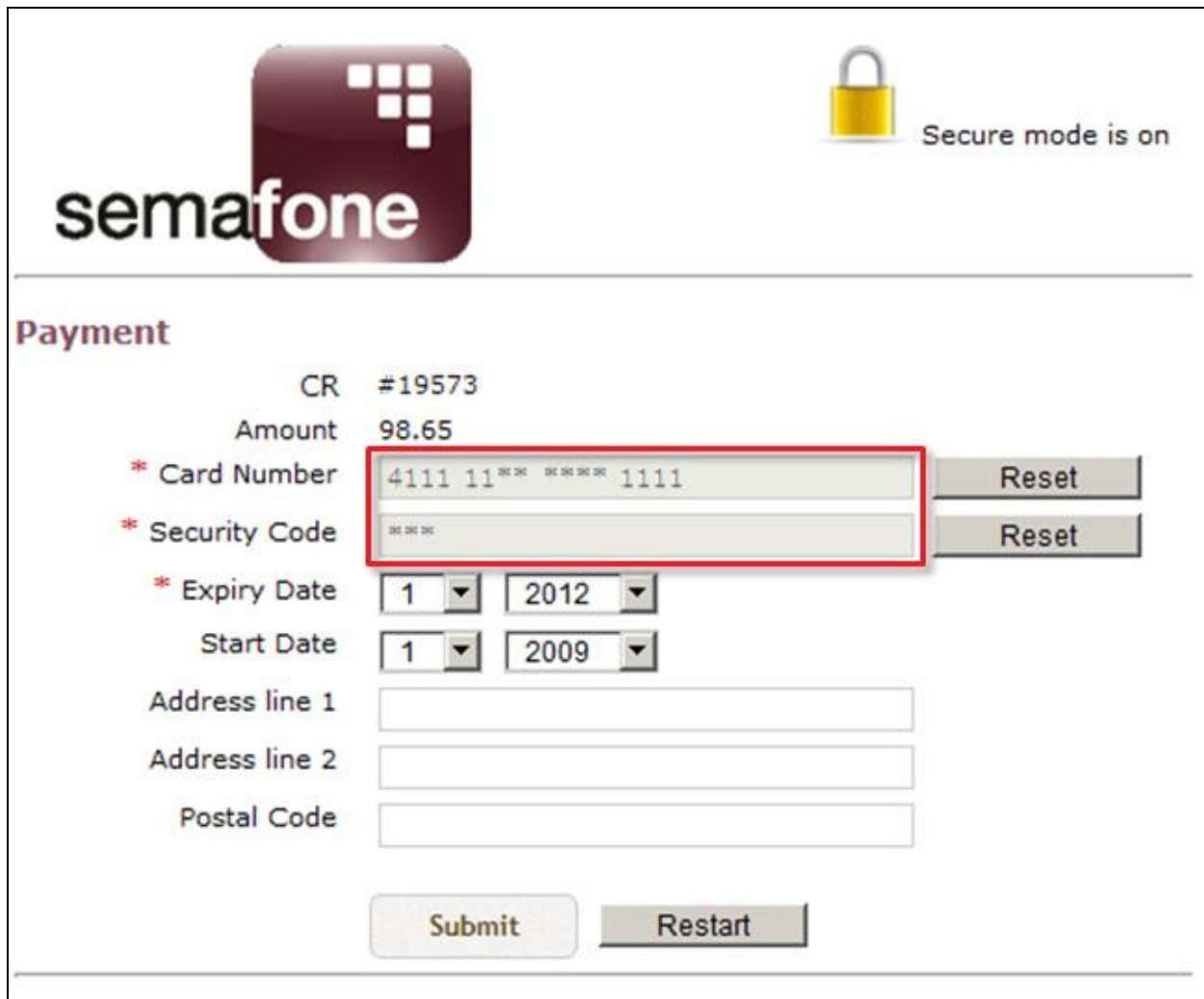
Address line 2

Postal Code

Submit

Restart

Enter the appropriate card number using the keypad on the customer telephone and ensure the correct digits and number of digits are accurately captured on the payment page.



The screenshot shows the SemaFone payment interface. At the top left is the SemaFone logo, and at the top right is a yellow padlock icon with the text "Secure mode is on". Below the header, the word "Payment" is displayed in a red font. The form contains the following fields and controls:

- CR #19573
- Amount 98.65
- * Card Number: A text input field containing "4111 11" followed by several "X" characters, and "1111" at the end. It has a "Reset" button to its right.
- * Security Code: A text input field containing "X" characters. It has a "Reset" button to its right.
- * Expiry Date: Two dropdown menus, the first showing "1" and the second showing "2012".
- Start Date: Two dropdown menus, the first showing "1" and the second showing "2009".
- Address line 1: A text input field.
- Address line 2: A text input field.
- Postal Code: A text input field.
- At the bottom, there are "Submit" and "Restart" buttons.

Verify the agent hears only a generic DTMF tone, and not that of the actual card number entered.

10. Conclusion

These Application Notes describe the configuration steps required for SemaFone to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise. All functionality cases were completed successfully with any observations noted in **Section 2.2**.

11. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

Details for the configuration of SemaFone can be obtained from the following:
<http://www.semafone.com>

©2013 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.