



Avaya Solution & Interoperability Test Lab

Application Notes for Convergys AppTrigger with Avaya SIP Enablement Services - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Convergys AppTrigger to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services (SES).

The overall objective of the interoperability compliance testing is to verify the SIP trace between Convergys AppTrigger and Avaya SIP Enablement Services.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Convergys AppTrigger which was compliance tested with Avaya Communication Manager and Avaya SIP Enablement Services (SES). Convergys AppTrigger is a network element that sits between the application cloud and the converging network and control layer to provide and manage connectivity to the evolving network for multiple applications. It is a scalable, carrier grade network element that enables legacy, intelligent network (IN), IP and next generation IMS applications to be immune from the ever evolving network. It insulates enhanced applications from the network via a programmable network abstraction engine, thereby providing the application consistent call/session control functions independent of each network.

Convergys AppTrigger is an Application Session Controller (ASC) which transfers the received calls to Avaya SES via a SIP trunk. Avaya SES will then send the received calls from Convergys AppTrigger to operators using the Communication Manager Server Address Map in Avaya SES.

These Application Notes assume that Avaya Communication Manager and Avaya SES are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult [3].

1.1. Interoperability Compliance Testing

The overall objective of the interoperability compliance testing is to verify SIP traces between Avaya SES and Convergys AppTrigger for each call. SIP traces were verified for the following scenarios:

Description: SIP-SIP A>B Success Case – A side terminates
Description: SIP-SIP A>B Success case – B side terminates
Description: SIP-SIP – 404 Not Found
Description: SIP-SIP – 486 Busy
Description: SIP-SIP – Unanswered call abandoned
Description: SIP-SIP A>B Success Case – Verify Voice path
Description: SIP-SIP A>B Success Case – Verify inband DTMF
Description: SIP-SIP – Unanswered call RNA Timer expiry
Description: SIP-SIP A>B Success Case – Verify call trace

1.2. Support

Technical support for Convergys AppTrigger can be obtained by contacting AppTrigger via support@apptrigger.com or by calling 866-227-7487 Option 2

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8720 Server, an Avaya G650 Media Gateway, an Avaya SIP Enablement Services (SES) server, and Convergys AppTrigger. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways. Avaya S8300 Servers with an Avaya G450 Media Gateway were included in

the test to provide an inter-switch scenario. For completeness, Avaya 4600 Series SIP IP Telephones, Avaya 4600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 9600 Series H.323 IP Telephones were included during the compliance test.

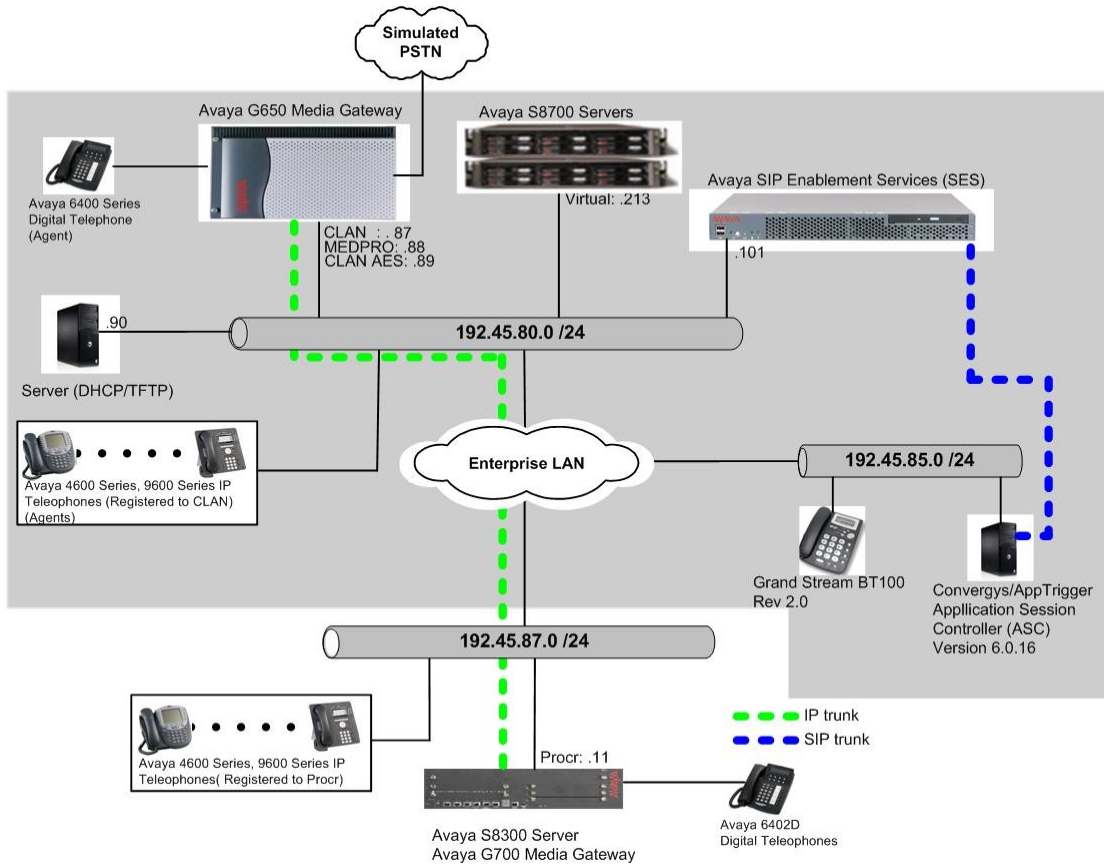


Figure 1. Test configuration of Convergy's AppTrigger with Avaya SIP Enablement Services

3. Equipment and Software Validated

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

Equipment		Software
Avaya S8720 Servers		Avaya Communication Manager 5.1.2 (R015x.01.2.416.4)
Avaya G650 Media Gateway		
	TN2312BP IPSI TN799DP CLAN TN2302AP MEDPRO	HW11 FW030 HW20 FW017 HW01 FW108
Avaya S8300 Server		Avaya Communication Manager 5.1.2 (R015x.01.2.416.4)
Avaya G700 Media Gateway		28.17
Avaya 4600 Series IP Telephone		
	4620SW	2.9
	4625SW	2.9
Avaya 9600 Series IP Telephone		
	9630	2.0
	9650	2.0
Avaya 64xx Series Digital Telephones		
	6408D+	-
	6402D	-
Analog Telephone		
Avaya C363T Converged Stackable Switch (Layer 3)		4.5.14
Extreme Summit 48 Switch (Layer 3)		4.1.21
Convergys AppTrigger on linux MV3.1		6.0.16.B554-183

4. Configure Avaya Communication Manager

This section provides the procedures for configuring node names, hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, stations, SIP trunk, SIP signaling, and Incoming Call Handling Treatment on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

4.1. Configure a node name for Avaya SIP Enablement Services

The node name configured in this section will be utilized for the SIP trunk configuration between Avaya Communication Manager and Avaya SIP enablement services. Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN and SIP IP address were utilized for Near-end Node and Far-end Node, respectively.

```
change node-names ip                                     Page 1 of 2
IP NODE NAMES
Name            IP Address
CLAN            192.45.80.87
ESS             192.45.80.216
MEDPRO         192.45.80.88
MEDPRO2        192.45.80.161
S8300G700      192.45.87.11
SIP            192.45.80.101
```

4.2. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD, Expert Agent Selection (EAS) and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options             Page 6 of 11
CALL CENTER OPTIONAL FEATURES

Call Center Release: 3.0

ACD? y                    Reason Codes? n
BCMS (Basic)? y          Service Level Maximizer? n
BCMS/VuStats Service Level? n Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? n Service Observing (Remote/By FAC)? y
Business Advocate? n    Service Observing (VDNs)? n
Call Work Codes? n      Timed ACW? N

DTMF Feedback Signals For VRU? n Vectoring (Basic)? y
Dynamic Advocate? n     Vectoring (Prompting)? n
Expert Agent Selection (EAS)? y Vectoring (G3V4 Enhanced)? n
EAS-PHD? n              Vectoring (3.0 Enhanced)? n
Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? n
Least Occupied Agent? n Vectoring (G3V4 Advanced Routing)? n
Lookahead Interflow (LAI)? n Vectoring (CINFO)? n
Multiple Call Handling (On Request)? n Vectoring (Best Service Routing)? n
Multiple Call Handling (Forced)? n Vectoring (Holidays)? n
PASTE (Display PBX Data on Phone)? n Vectoring (Variables)? n
(NOTE: You must logoff & login to effect the permission changes.)
```

Once the Expert Agent Selection (EAS) field is set to **y**, from the previous step, enter the **change system-parameters features** command. On **Page 11**, verify that the Expert Agent Selection (EAS) Enabled field is set to **y**. To enable the EAS feature, the Expert Agent Selection field in both system-parameters customer-options and system-parameters features pages should be set to **y**.

```

change system-parameters features                                     Page 11 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:          Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone (msec): 100    Pause (msec): 30
    Prompting Timeout (secs): 10

    Reverse Star/Pound Digit For Collect Step? n

    Store VDN Name in Station's Local Call Log? y
  SERVICE OBSERVING
    Service Observing: Warning Tone? y      or Conference Tone? n
    Service Observing Allowed with Exclusion? n
    Allow Two Observers in Same Call? y
  
```

Enter the **add hunt-group <n>** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

```

add hunt-group 1                                                  Page 1 of 3
                                HUNT GROUP

    Group Number: 1
    Group Name: test
    Group Extension: 50011
    Group Type: ucd-mia
    TN: 1
    COR: 1
    Security Code:
    ISDN/SIP Caller Display:

    ACD? y
    Queue? y
    Vector? y

    MM Early Answer? n
    Local Agent Preference? n

    Queue Limit: unlimited
    Calls Warning Threshold:      Port:
    Time Warning Threshold:      Port:
  
```

On **Page 2**, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

```
add hunt-group 1                                     Page 2 of 3

                                HUNT GROUP

Skill? y
AAS? n
Measured: internal
Supervisor Extension:

Controlling Adjunct: none

VuStats Objective:

                                Redirect on No Answer (rings):
                                Redirect to VDN:
Forced Entry of Stroke Counts or Call Work Codes? n
```

Enter the **add agent-loginID <p>** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the agent-loginID form, enter a descriptive Name and Password.

```
add agent-loginID 50021                             Page 1 of 2

                                AGENT LOGINID

Login ID: 50021                                     AAS? n
Name: Agent-1                                       AUDIX? n
TN: 1                                               LWC Reception: spe
COR: 1                                              LWC Log External Calls? n
Coverage Path:                                     AUDIX Name for Messaging:
Security Code:                                     LoginID for ISDN/SIP Display? n
                                                Password:
                                                Password (enter again):
                                                Auto Answer: station
                                                MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :
```

WARNING: Agent must log in again before changes take effect

On **Page 2**, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```

add agent-loginID 50021                                     Page 2 of 2

                                AGENT LOGINID

    Direct Agent Skill:
Call Handling Preference: skill-level                       Local Call Preference? n

    SN      SL          SN      SL          SN      SL          SN      SL
1: 1       1           16:          31:          46:
2:         17:          32:          47:
  
```

Enter the **change vector <q>** command, where **q** is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```

change vector 1                                           Page 1 of 3

                                CALL VECTOR

    Number: 1                               Name: Queue to skill1

                                Meet-me Conf? n           Lock? n
    Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
    Prompting? n   LAI? n   G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
    Variables? n   3.0 Enhanced? n

01 wait-time 2 secs hearing ringback
02 queue-to skill 1 pri m
03
  
```

Enter the **add vdn <r>** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the **Vector Number** configured in the previous step. In the example below, incoming calls to extension 50000 will be routed to testVDN50000, which in turn will invoke the actions specified in vector 1.

```

add vdn 50000                                             Page 1 of 2

                                VECTOR DIRECTORY NUMBER

                                Extension: 50000
                                Name*: testVDN50000
                                Vector Number: 1

    Meet-me Conferencing? n
    Allow VDN Override? n
                                COR: 1
                                TN*: 1
    Measured: none

    1st Skill*:
    2nd Skill*:
    3rd Skill*:
  
```


Enter the **change feature-access-codes** command. Define the Auto-In Access Code, Login Access Code, Logout Access Code, and Aux Work Access Code.

```
change feature-access-codes                                     Page 5 of 6
                    FEATURE ACCESS CODE (FAC)

                    Automatic Call Distribution Features

                    After Call Work Access Code: 120
                    Assist Access Code: 121
                    Auto-In Access Code: 122
                    Aux Work Access Code: 123
                    Login Access Code: 124
                    Logout Access Code: 125
                    Manual-in Access Code: 126
                    Service Observing Listen Only Access Code: 127
                    Service Observing Listen/Talk Access Code: 128
                    Add Agent Skill Access Code: 130
```

Enter the **add abbreviated-dialing group <g>** command, where **g** is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```
add abbreviated-dialing group 1                               Page 1 of 1
                    ABBREVIATED DIALING LIST

                    Group List: 1          Group Name: Call Center
                    Size (multiple of 5): 5  Program Ext:          Privileged? n
DIAL CODE
11: 124
12: 125
13:
```

4.3. Configure Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and make sure that the IP Softphone field is set to **y**.

```

add station 22001                                     Page 1 of 5
                                                    STATION
Extension: 22001                                     Lock Messages? n          BCC: 0
Type: 4620                                           Security Code: *          TN: 1
Port: IP                                             Coverage Path 1:         COR: 1
Name: 22001                                          Coverage Path 2:         COS: 1
                                                    Hunt-to Station:

STATION OPTIONS
Loss Group: 19                                       Time of Day Lock Table:
                                                    Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 22001
Speakerphone: 2-way                                  Mute Button Enabled? y
Display Language: english                            Expansion Module? n
Survivable GK Node Name:                             Media Complex Ext:
Survivable COR: internal                             IP SoftPhone? y
Survivable Trunk Dest? y                             IP Video Softphone? n
                                                    Customizable Labels? y

```

On Page 4 of the STATION form, for ABBREVIATED DIALING List 2, enter the abbreviated dialing group configured in Section 4.2. Configure the following BUTTON ASSIGNMENTS:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

```

add station 22001                                     Page 4 of 5
                                                    STATION
SITE DATA
Room:                                                Headset? n
Jack:                                                Speaker? n
Cable:                                               Mounting: d
Floor:                                               Cord Length: 1
Building:                                            Set Color:

ABBREVIATED DIALING
List1: personal 1                                   List2: group 1           List3: system

BUTTON ASSIGNMENTS
1: call-appr                                       5: auto-in              Grp: 1
2: call-appr                                       6: aux-work            RC:   Grp: 1
3: call-appr                                       7: abrv-dial          List: 2 DC: 11
4:                                                8: abrv-dial          List: 2 DC: 12

```

4.4. Configure Incoming Call Handling Treatment

As an INVITE message comes to Avaya SES from Convergys AppTrigger, the message contains the extension of Convergys AppTrigger. Avaya SES will send the call to Avaya Communication Manager using the destination extension as the extension of Convergys AppTrigger. In Avaya Communication Manager the extension is converted to either a VDN or Hunt group extension

utilizing the **change inc-call-handling-trmt trunk-group 202** form, so the agent can answer the call. The following screen shows that the extension 79017 (Convergys AppTrigger extension) is converted to extension 50000 (VDN extension). The trunk group 202 is a trunk group created for a trusted host (Convergys AppTrigger – refer to **Section 5.3**).

```
change inc-call-handling-trmt trunk-group 202                               Page 1 of 30
                                INCOMING CALL HANDLING TREATMENT
Service/          Called      Called      Del Insert
Feature          Len        Number
tie              5 79017          5 50000
tie
tie
tie
```

4.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SIP Enablement Services. For a trusted host, a second SIP signaling group is needed, on top of the SIP signaling group between Avaya Communication Manager and Avaya SES. Enter the **add signaling-group <t>** command, where **t** is an available signaling group and configure the following:

- Group Type – Set to **sip**.
- Near-end Node Name - Set to **CLAN** as displayed in **Section 4.1**.
- Far-end Node Name - Set to the Avaya SES name, **SIP**, configured in **Section 4.1**.
- Far-end Domain - Set to the IP address of Convergys AppTrigger. In the compliance test **192.45.85.60** was assigned as IP address of Convergys AppTrigger.

```
add signaling-group 202                               Page 1 of 1
                                SIGNALING GROUP
Group Number: 202                                Group Type: sip
                                                Transport Method: tls
Near-end Node Name: CLAN                        Far-end Node Name: SIP
Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                                Far-end Network Region: 1
Far-end Domain: 192.45.85.60
                                                Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                       Direct IP-IP Audio Connections? y
                                                IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3              Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

For a trusted Host, a second SIP trunk is needed, on top of a SIP trunk between Avaya Communication Manager and Avaya SES. To create a SIP trunk, enter the **add trunk-group <u>**, where **u** is an available trunk group, and configure the following:

- Group Name – Enter a descriptive name.
- Group Type – Set to the Group Type field to **sip**.
- TAC (Trunk Access Code) – Set to any available trunk access code.
- Signaling Group – Set to the Group Number field value configured in **Section 4.5**.
- Number of Members – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 202                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 202                                     Group Type: sip          CDR Reports: y
Group Name: AppTrigger                               COR: 1                 TN: 1                TAC: 1001
Direction: two-way                                Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                    Signaling Group: 202
                                                    Number of Members: 10
```

5. Configure Avaya SIP Enablement Services

This section describes the steps for creating SIP trunks between Avaya SES and Avaya Communication Manager, and between Avaya SES and Convergys AppTrigger. Convergys AppTrigger will be treated as a trusted host. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.


5.1. Configure Communication Manager Servers

Launch a web browser, enter <https://<IP address of SES server>/admin> in the URL, and log in with the appropriate credentials. Click on the **Launch SES Administration Interface** link upon successful login.

Address <https://192.45.80.101/cgi-bin/unified> Go Links SnagIt

AVAYA Integrated Management
Standard Management Solutions

Help Log Off

 **SES Administration** The Administration Web Interface allows you to administer this SES server. [Launch SES Administration Interface](#)

Maintenance The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the server. [Launch Maintenance Web Interface](#)

This section provides steps to add SIP-enabled media servers to the SIP domain. In the **Integrated Management SIP Server Management** page, select the **Communication Manager Servers** → **Add** link from the left pane of the screen. The following screen shows the Add Media Server Interface page. The highlighted fields were configured for the compliance test:

- Communication Manager Server Interface Name – Enter a descriptive name for the communication manager server interface.
- SIP Trunk IP Address – Enter the IP address for the media server's CLAN IP interface that terminates the SIP link from SES.

Click **Add** when finished.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

Add Communication Manager Server Interface

Communication Manager Server Interface Name* S8720

Host 192.45.80.101

SIP Trunk

SIP Trunk Link Type TCP TLS

SIP Trunk IP Address* 192.45.80.87

Communication Manager Server

Communication Manager Server Admin Address* 192.45.80.213
(see Help)

Communication Manager Server Admin Port* 5022

Communication Manager Server Admin Login* crkim

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.

Add

Navigate to **Communication Manager Servers** → **List**, and select **Map** on the right pane of the screen.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

Top

- Users
 - Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
 - Emergency Contacts
- Export/Import to ProVision
- Hosts
 - IM logs
- Communication Manager Servers
 - Add
 - List

List Communication Manager Servers

Commands			Interface	Host
Edit	Extensions	Map	S8720	192.45.80.101

Add Another Communication Manager Server Interface

Select **Add Map In New Group** to start adding an address map.

AVAYA Integrated Management SIP Server Management
This Server: [1] SIPServer

Help Exit

Top

- Users
 - Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
 - Emergency Contacts
- Export/Import to ProVision
- Hosts
 - IM logs
- Communication Manager Servers
 - Add
 - List

List Communication Manager Server Address Map

No address map entries.

Add Map In New Group

In the Add Communication Manager Server Address Map page, provide the following information:

- Name – Enter a descriptive alphanumeric name to identify the map.
- Pattern – Enter a regular expression that will match the extension numbers.

Click **Add** when finished.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

Add Communication Manager Server Address Map

Name* 8720-1

Pattern* ^sip:79017

Replace URI

Fields marked * are required.

Add

Top

- Users
- Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
- Emergency Contacts
- Export/Import to ProVision
- Hosts
- IM logs
- Communication Manager Servers
 - Add
 - List

The following screen shows the Communication Manager Server Address Map, after completion.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

List Communication Manager Server Address Map

Commands	Name	Commands	Contact
Edit Delete	8720-1	Edit Delete	sip:\$(user) @192.45.80.87:5061;transport=tls

Add Another Map Add Another Contact Delete Group

Add Map In New Group

Top

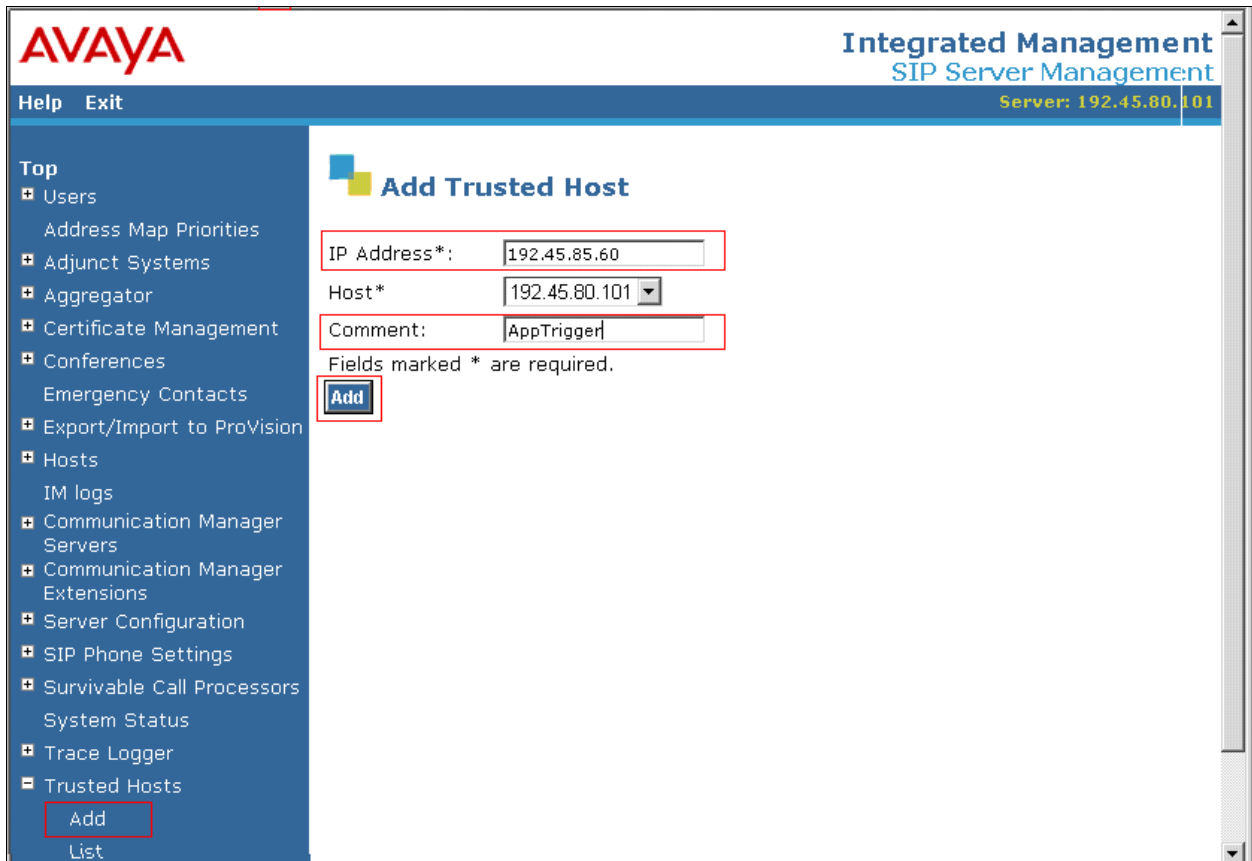
- Users
- Address Map Priorities
- Adjunct Systems
- Aggregator
- Certificate Management
- Conferences
- Emergency Contacts
- Export/Import to ProVision
- Hosts
- IM logs
- Communication Manager Servers
 - Add
 - List

5.2. Configure Trusted Hosts

This section provides steps to add trusted hosts to be administered in the SIP Enablement Services (SES) database. In the **Integrated Management SIP Server Management** page, select the **Trusted Hosts** → **Add** link from the left pane of the screen. The highlighted fields were configured for the compliance test

- IP Address – Enter an IP address of a trusted host.
- Comment – Enter a descriptive alphanumeric name to identify the trusted host.

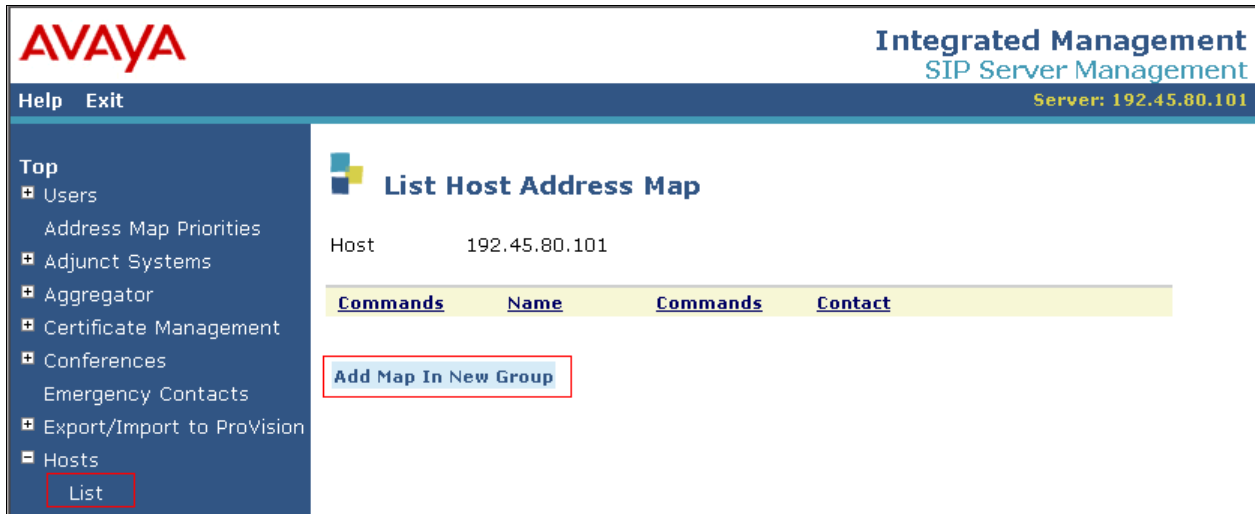
Click **Add** when finished.



The screenshot displays the Avaya Integrated Management SIP Server Management interface. The top left corner features the Avaya logo, and the top right corner shows the page title "Integrated Management SIP Server Management" and the server IP address "Server: 192.45.80.101". A navigation menu on the left includes "Help Exit" and a list of system components, with "Trusted Hosts" and its "Add" sub-link highlighted. The main content area is titled "Add Trusted Host" and contains a form with three input fields: "IP Address*" with the value "192.45.85.60", "Host*" with a dropdown menu showing "192.45.80.101", and "Comment:" with the value "AppTriggered". Below the form, a note states "Fields marked * are required." and an "Add" button is visible. The "Add" button in the left navigation menu is also highlighted.

5.3. Configure Host Address Map

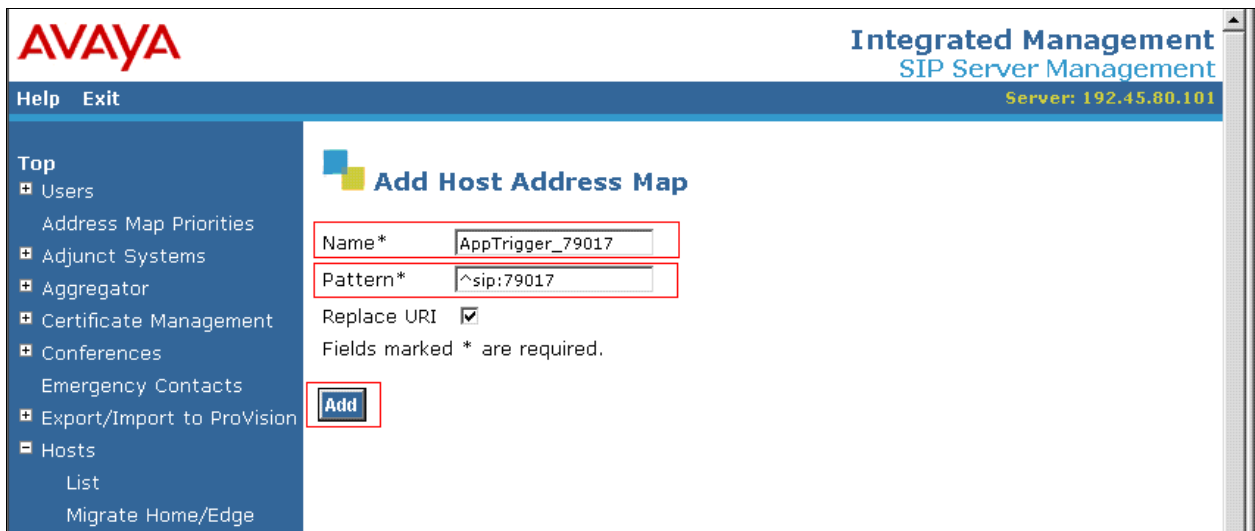
This section provides steps to add host address map to be administered in the SIP Enablement Services (SES) database. In the **Integrated Management SIP Server Management** page, select the **Hosts** → **List** link from the left pane, and select **Add Map In New Group** from the right pane of the screen.



The highlighted fields were configured for the compliance test

- Name – Enter a descriptive alphanumeric name to identify the map.
- Pattern – Enter a regular expression that will match the extension numbers. The pattern will be utilized to send calls to Convergys AppTrigger.

Click **Add** when finished.



To add a host contact, select the **Add Another Contact** from the right pane of the screen.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

Top

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

List Host Address Map

Host 192.45.80.101

Commands	Name	Commands	Contact
Edit Delete	AppTrigger_79017		

Add Another Map Add Another Contact Delete Group

Add Map In New Group

From the Add Host Contact screen, provide the following information on the Contact field:
sip:\$(user)@192.45.80.101:5060;transport=udp

Click **Add** when finished.

AVAYA Integrated Management SIP Server Management
Server: 192.45.80.101

Help Exit

Top

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

Add Host Contact

Handle AppTrigger_79017

Contact* sip:\$(user)@192.45.80.101:5060;transport=udp

Fields marked * are required.

Add

The following screen shows the completion of the Host Address Map configuration.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top right corner displays 'Server: 192.45.80.101'. The main content area is titled 'List Host Address Map' and shows the host '192.45.80.101'. Below this, there is a table with columns for 'Commands', 'Name', 'Commands', and 'Contact'. The table contains one entry: 'AppTrigger_79017' with a contact URI 'sip:\$(user)@192.45.80.101:5060;transport=udp'. There are 'Edit' and 'Delete' buttons for this entry. At the bottom of the table, there are buttons for 'Add Another Map', 'Add Another Contact', and 'Delete Group'. A 'Top' navigation menu is visible on the left side of the interface.

6. Configure Convergys AppTrigger

Convergys installs, configures, and customizes Apptrigger ASC for their end customers. This section only describes the interface configuration for Convergys AppTrigger to communicate with Avaya SES. Refer to [3] for configuring Convergys AppTrigger.

In the Linux, change directory to `/usr/local/sysadmin/RT-ENV`. Run `exe/rlwrap exe/RShell-SM.bash`, and the `>>` prompt will appear. Execute the `showsipelement /v` command to display the URI. The `Enter-SIP-Element` or `Modify-SIP-Element` is used to configure the uri.

```
SystemManager: >> showsipelement /v
showsipelement /v
SystemManager: ID LOCAL ELEMENT
SystemManager: -----
SystemManager: SIPELEM-1-GS SIPUA-1
SystemManager: Fields:
SystemManager: id..... SIPELEM-1-GS
SystemManager: RFC2833Enable..... true
SystemManager: SIDEnable..... true
SystemManager: autoOOSDetectionEnabled..... LOCAL_ELEMENT
SystemManager: autoOOSHeartBeatExpOnSwitchOver. 10000ms
SystemManager: autoOOSHeartBeatTimerMultiple... 200
SystemManager: echoCancelEnable..... true
SystemManager: echoTail..... 32
SystemManager: jitterDelay..... 50ms
SystemManager: localElement..... SIPUA-1
SystemManager: maxCallsAllowed..... 100000
SystemManager: onHoldFlag..... SEND_ONLY
SystemManager: packetInterval..... 20
SystemManager: packetIntervalG723OverRide..... false
SystemManager: payloadValue..... 96
SystemManager: playAnnouncement..... LOCAL_ELEMENT
SystemManager: privacyHeaderSupportFlag..... false
SystemManager: provideBackwardTones..... LOCAL_ELEMENT
SystemManager: silenceSupEnable..... true
SystemManager: terminateBearer..... true
SystemManager: typeOfService..... NORMAL
SystemManager: uri..... "sip:192.45.85.63:5060;transport=udp"
SystemManager: Attributes:
SystemManager: Admin state..... UNLOCKED
SystemManager: Oper state..... ENABLED
SystemManager: Statistics enabled..... false
SystemManager: Status..... *CALLS[0]
```

The following shows the initial settings file that contains all the provisioning commands of the system, and the file was used during the compliance test.

```
# Database Backup

#   Local Date/Time: Tue, Apr. 07, 2009 13:02:47 -0500
#       Version: 6.0.16
# Version Qualifier: B554-183
#       Build: V6.0.16B554_fixes:Friday-12
#       Build Time: 0903271233
#       Image: /usr/local/carrius/RT-ENV/exe/SystemManager
#       Image Date: Fri, Mar. 27, 2009 13:28:13 -0500
#       Image Size: 188781378
#       Host Name: SBC1

Load "factory-settings"
Enter-Switch 1 /sctpHeartBeatTimer=1500ms /maxH323Gateway=10
/alarmFloodThreshold=10 /location=PUBLIC_NET_LU /countryCode="1"
/ESWMonitorInterval=300000 /ESWInfoPacketErrorThreshold=0.0001%
/ESWMinPacketErrorThreshold=0.001% /ESWMajPacketErrorThreshold=0.01%
/ESWCrtlPacketErrorThreshold=0.1% /ESWInfoBandwidthThreshold=60%
/ESWMinBandwidthThreshold=70% /ESWMajBandwidthThreshold=80%
/ESWCrtlBandwidthThreshold=90% /CPLevel1Threshold=80%:70%
/CPLevel2Threshold=90%:80%
Enter-Shelf 1 /type=PDSI_4U
Enter-IOCard 1-1 /interfaces=192.45.85.61 /type=AC_TP1610_FRAMERS_04E
Enter-SBCCard 1-10 /interfaces=192.45.85.60 /type=PP332
Enter-CMM-Card 1-9-0 /type=PDSi_EAN /interfaces=192.45.85.62
Enter-IOManager IOCard1_1 /card=1-1 /processor=SBC-1-10
/exeDir="exe" /exeName="IOManager" /exeQualifier="" /exeOpts=HEADLESS
/exeTitle="IOCard1_1" /dlDirs="db/audio" /mode=AUTOMATIC
Enter-CallManager CallManager /processor=SBC-1-10
/alarmLogPath="alarms" /alarmLogPolicy=WEEKLY /exeDir="exe"
/exeName="CallManager" /exeQualifier="" /exeOpts=HEADLESS
/exeTitle="CallManager" /dlDirs="http.d" /mode=AUTOMATIC
/services=ResourceControl
Enter-SystemManager SystemManager /processor=SBC-1-10
/alarmLogPath="alarms" /alarmLogPolicy=WEEKLY /exeDir="exe"
/exeName="SystemManager" /exeQualifier="" /exeArgs="-v"
/exeTitle="SystemManager" /dlDirs="cmd" , "admin/cmd" , "admin/etc" ,
"admin/ini" , "bin.MinGW" , "http.d" , "db/audio" , "db/audio.orig" ,
"db/etc" /mode=AUTOMATIC

Enter-SSPPProgram SIP /processor=SBC-1-10 /exeName="SSPPProgram"

Enter-SIP-UserAgent 1 /maxCallsAllowed=100000 /terminateBearer=true
/typeOfService=NORMAL /packetInterval=20 /echoCancelEnable=true
/echoTail=32 /jitterDelay=50ms /silenceSupEnable=true /SIDEnable=true
/RFC2833Enable=true /payloadValue=96 /codecTypes=G711aLaw
/uri="sip:55555@192.45.85.60:5060;transport=udp" /maxForward=6
```

```

/T1=500ms /T2=4000ms /T4=40000ms /provideBackwardTones=NO
/playAnnouncement=NO /autoOOSDetectionEnabled=NO /app=SSPAPP-SIP
/packetIntervalG723Override=false /autoOOSHeartBeatTimerMultiple=200
/autoOOSHeartBeatExpOnSwitchOver=10000ms /translation=DEFAULT
Enter-SIP-Element 1-GS /localElement=1
/uri="sip:192.45.85.63:5060;transport=udp" /onHoldFlag=SEND_ONLY
/privacyHeaderSupportFlag=false /provideBackwardTones=LOCAL_ELEMENT
/playAnnouncement=LOCAL_ELEMENT /autoOOSDetectionEnabled=LOCAL_ELEMENT
/maxCallsAllowed=100000 /terminateBearer=true
/packetIntervalG723Override=false /autoOOSHeartBeatTimerMultiple=200
/autoOOSHeartBeatExpOnSwitchOver=10000ms /typeOfService=NORMAL
/packetInterval=20 /echoCancelEnable=true /echoTail=32
/jitterDelay=50ms /silenceSupEnable=true /SIDEnable=true
/RFC2833Enable=true /payloadValue=96
Enter-RouteTable DEFAULT
Modify-Shelf-Clock 1 /source=INTERNAL /refA=IOCARD-1-1

Enter-SIP-Element 2-AVAYA/localElement=1
/uri="sip:192.45.80.101:5060;transport=udp" /onHoldFlag=SEND_ONLY
/privacyHeaderSupportFlag=false /provideBackwardTones=LOCAL_ELEMENT
/playAnnouncement=LOCAL_ELEMENT /autoOOSDetectionEnabled=LOCAL_ELEMENT
/maxCallsAllowed=100000 /terminateBearer=true
/packetIntervalG723Override=false /autoOOSHeartBeatTimerMultiple=200
/autoOOSHeartBeatExpOnSwitchOver=10000ms /typeOfService=NORMAL
/packetInterval=20 /echoCancelEnable=true /echoTail=32
/jitterDelay=50ms /silenceSupEnable=true /SIDEnable=true
/RFC2833Enable=true /payloadValue=96

Enter-RouteList /id="avaya"
AddToRouteList /id="avaya" /resource=SIPELEM-2-AVAYA
AddToRouteTable /id=DEFAULT /numDigits=5 /prefix=""
/routeList="avaya"

Enter-User /id=Admin /type =Administrator /password=Password

Enter-APIProgram /id="TandemA" /interfaces=192.45.85.64 /port=50000
/allowOriginationsOnFailure=true /CallInfoPolicy=VR_CI_LOG
/bufferedCallInfoMaxSize=20 /releaseOnFailure=true
/ValidateParametersAndStates=true

Enter-APIProgram /id="TandemB" /interfaces=192.45.85.64 /port=50010
/allowOriginationsOnFailure=true /CallInfoPolicy=VR_CI_LOG
/bufferedCallInfoMaxSize=20 /releaseOnFailure=true
/ValidateParametersAndStates=true

Enter-ProtectedApp /id=TandemAB /apps=APIAPP-"TandemA", APIAPP-
"TandemB" /mode=LOAD_SHARED /reg=Shelf-1

Unlock-Device ALL /force=true
Unlock-App ALL /force=true

```

7. General Test Approach and Test Results

The general test approach was to verify the SIP trace between Avaya SES and Convergys AppTrigger, when calls were manually placed to Convergys AppTrigger. All test cases were successful, and verified utilizing SIP traces.

8. Verification Steps

The following steps may be used to verify the configuration:

- End-to-end verification: When a call was placed to Convergys AppTrigger, the call was answered by an operator (H.323 phone).
- Verified correct SIP traces on each call using Wireshark Network Analyzer.

9. Conclusion

Convergys AppTrigger was compliance tested with Avaya Communication Manager (Version 5.1.2) and Avaya SES (Version 5.1.2). The correct SIP traces were verified between Avaya SES and Convergys AppTrigger when a call was placed to Convergys AppTrigger.

10. References

This section references the Avaya and Convergys documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Administrator Guide for Avaya Communication Manager*, Release 5.0, Issue 4, January 2008, Document Number 03-300509.

[2] *Administering SIP Enablement Services on the Avaya S8300 Server*, Issue 1.0, January 2008, Document Number 03-602508.

The following document was provided by Convergys.

[3] 600-0600-002 *Compleat-100/-200* OAM&P and Installation Guide

©2009 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.