

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring SFR SIP Trunk with Avaya Aura<sup>®</sup> Communication Manager 8.0, Avaya Aura<sup>®</sup> Session Manager 8.0 and Avaya Session Border Controller for Enterprise 8.0 – Issue 1.0

### Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between SFR and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.0, Avaya Aura<sup>®</sup> Communication Manager 8.0, Avaya Session Border Controller for Enterprise 8.0 and various Avaya endpoints.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

SFR is a member of the Avaya DevConnect Service Provider program. 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.

#### **Table of Contents**

2.       GENERAL TEST APPROACH AND TEST RESULTS       4         2.1.       INTEROPERABILITY COMPLIANCE TESTING.       5         2.2.       TIST RESULTS.       6         2.3.       SUPPORT.       6         3.       REFERENCE CONFIGURATION.       7         4.       EQUIPMENT AND SOFTWARE VALIDATED.       8         5.       CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.       10         5.1.       LICENSING AND CAPACITY       10         5.2.       SYSTEM PEATURES.       12         5.3.       IP NODE NAMES       13         5.4.       CODECS.       13         5.5.       CONFIGURE INTERFACE OR PROCR.       18         5.7.       SIGNALING GROUP       18         5.8.       TRUN GROUP       20         5.9.       CALLING PARTY INFORMATION.       25         5.10.       OUTBOUND ROUTING       20         5.12.       CONTACT CENTR CONFIGURATION       30         5.12.       CONTACT CENTR CONFIGURATION       31         5.12.       CONTIGURATIC CONFIGURATION       31         5.12.       CONTIGURA AURA® COMMUNICATION MAAGER STATIONS       35         5.14.       MAVA AURA® COMMUNICATION MAAGER STATIONS       35	1.	INTI	RODUCTION	4		
2.2.       TEST RESULTS.	2.	2. GENERAL TEST APPROACH AND TEST RESULTS4				
2.3.       SUPPORT		2.1.	INTEROPERABILITY COMPLIANCE TESTING	5		
3.       REFERENCE CONFIGURATION       7         4.       EQUIPMENT AND SOFTWARE VALIDATED       8         5.       CONFIGURE AVAYA AURA® COMMUNICATION MANAGER       10         5.1.       LICENSING AND CAPACITY       10         5.2.       SYSTEM FEATURES       12         5.3.       IP NODE NAMES       13         5.4.       CODECS       13         5.5.       CONFIGURE IP INTERFACE FOR PROCE       18         5.6.       CONFIGURE IP INTERFACE FOR PROCE       18         5.7.       SIGNALING GROUP       20         5.8.       TRUNK GROUP       20         5.9.       CALLING PARTY INFORMATION       25         5.10.       OUTBOUND ROUTING       25         5.11.       INCOMING CALI HANDLING TREATMENT       30         5.12.       CONTACT CENTRE CONFIGURATION       31         5.12.       CONTIGURE AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® SESSION MANAGER       36         6.11.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION CHANGES.       35         6.2.       CONFIGURE AVAYA AURA® SESSION MANAGER       36 <t< td=""><td></td><td></td><td></td><td></td></t<>						
4. EQUIPMENT AND SOFTWARE VALIDATED       8         5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER       10         5.1. LICENSING AND CAPACITY       10         5.2. SYSTEM FEATURES       12         5.3. IP NODE NAMES       13         5.4. CODECS       13         5.5. IP NOTE NAMES       13         5.6. CONFIGURE IP INTERFACE FOR PROCE       18         5.7. SIGNALING GROUP       18         5.8. TRUNK GROUP       20         5.9. CALLING PARTY INFORMATION.       25         5.10. OUTBOUND ROUTING       26         5.11. INCOMING CALL HANDLING TREATMENT       30         5.12. CONTACT CENTER CONFIGURATION       31         5.12. CONTACT CENTER CONFIGURATION MANAGER STATIONS       35         5.13. AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14. SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6. CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1. AVAYA AURA® COMMUNICATION MANAGER STATIONS       37         6.2. SPECIFY SIP DOMAIN       39         6.3. ADD LOCATION       400         6.4. ADD SIP ENTITIES       41         6.5. ADD ENTITY LINKS       45         6.6. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53		2.3.	SUPPORT	6		
5.       CONFIGURE AVAYA AURA® COMMUNICATION MANAGER       10         5.1.       LICENSING AND CAPACITY       10         5.2.       SYSTEM FEATURES       12         5.3.       IP NODE NAMES       13         5.4.       CODECS       13         5.5.       IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER       15         5.6.       CONFIGURE IP INTERFACE FOR PROCE       18         5.7.       SIGNALING GROUP       20         5.8.       TRUNK GROUP       20         5.9.       CALLING PARTY INFORMATION       25         5.10.       OUTBOUND ROUTING       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.1.       ANDING OTALL HANDLING TREATMENT       30         5.12.1.       ANDIGURATION MANAGER STATIONS       35         5.13.       AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       36         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2.       SPECIFY SIP DOMAIN       3	3.	REF	ERENCE CONFIGURATION	7		
5.       CONFIGURE AVAYA AURA® COMMUNICATION MANAGER       10         5.1.       LICENSING AND CAPACITY       10         5.2.       SYSTEM FEATURES       12         5.3.       IP NODE NAMES       13         5.4.       CODECS       13         5.5.       IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER       15         5.6.       CONFIGURE IP INTERFACE FOR PROCE       18         5.7.       SIGNALING GROUP       20         5.9.       CALLING PARTY INFORMATION       25         5.10.       OUTBOUND ROUTING       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.1. Announcements       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® SESSION MANAGER       36         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SESSION MANAGER       36         6.3.       ADD LOCATION       MANAGER LOGIN AND NAVIGATION       37         6.4.       CONFIGURE AVAYA AURA® SESSION MANAGER       40         6.4.1.       Configure Awaya Session Border Controller for Enterprise SIP Entity	4.	EQU	IPMENT AND SOFTWARE VALIDATED	8		
5.1.       LICENSING AND CAPACITY       10         5.2.       SYSTEM FEATURES.       12         5.3.       IP NODE NAMES.       13         5.4.       CODECS.       13         5.5.       IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER.       15         5.6.       CONFIGURE IP INTERFACE FOR PROCR.       18         5.7.       SIGNALING GROUP       18         5.8.       TRUNK GROUP       20         5.9.       CALLING PARTY INFORMATION.       25         5.10.       OUTBOUND ROUTING       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION.       31         5.12.       ACD Configuration for Call Queued for Handling by Agent.       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION.       37         6.2.       SPECIFY SIP DOMAIN       39         6.3.       ADD LOCATION.       40         6.4.       ADD DAD PONTITIES       41	5.					
5.2.       SYSTEM FEATURES						
5.3.       IP NODE NAMES.       13         5.4.       CODECS.       13         5.5.       IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER       15         5.6.       CONFIGURE IP INTERFACE FOR PROCR.       18         5.7.       SIGNALING GROUP       18         5.8.       TRUNK GROUP       20         5.9.       CALLING PARTY INFORMATION.       25         5.10.       OUTBOUND ROUTING.       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.1.       Announcements.       31         5.12.2. ACD Configuration for Call Queued for Handling by Agent.       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.       36         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND AVIGATION.       37         6.2.       SPECIFY SIP DOMAIN       39         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES.       41         6.4.1.       Configure Session Manager SIP Entity.       42						
5.4.       CODECS						
5.5.       IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER       .15         5.6.       CONFIGURE IP INTERFACE FOR PROCR       .18         5.7.       SIGNALING GAOUP       .18         5.8.       TRUNK GROUP       .20         5.9.       CALLING PARTY INFORMATION       .25         5.10.       OUTBOUND ROUTING       .26         5.11.       INCOMING CALL HANDLING TREATMENT       .30         5.12.       CONTACT CENTER CONFIGURATION       .31         5.12.1.       Announcements       .31         5.12.2.       ACD Configuration for Call Queued for Handling by Agent.       .31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       .35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       .35         6.1.       AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       .36         6.1.       AVAYA AURA® SESSION MANAGER       .36         6.3.       ADD LOCATION       .39         6.3.       ADD LOCATION       .40         6.4.       ADD SIP ENTITIES       .41         6.4.1.       Configure Session Manager SIP Entity       .42         6.4.2.       Configure Communication Manager SIP Entity       .42         6.5.						
5.6.       CONFIGURE IP INTERFACE FOR PROCR.       18         5.7.       SIGNALING GROUP.       18         5.8.       TRUNK GROUP.       20         5.9.       CALLING PARTY INFORMATION.       25         5.10.       OUTBOUND ROUTING.       26         5.11.       INCOMING CALL HANDLING TREATMENT.       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.       ADD CORTIGURATION MANAGER STATIONS       31         5.12.       ADRA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SESSION MANAGER       39         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES       41         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Communication Manager SIP Entity       42         6.4.       ADD EDERTITIES       41         6.4.       ADD EDERTITIES       41         6.4.       ADD EDERTITIES       42         6.4.       ADD EDERTITIES       44         6.4.       Configure Communication Mana						
5.8.       TRUNK GROUP		5.6.				
5.9.       CALLING PARTY INFORMATION.       25         5.10.       OUTBOUND ROUTING       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.       ACD Configuration for Call Queued for Handling by Agent       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2.       SPECIFY SIP DOMAIN       39         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure TIME RANGES       47         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.7.       ADD ROUTING POLICIES <td></td> <td>5.7.</td> <td></td> <td></td>		5.7.				
5.10.       OUTBOUND ROUTING       26         5.11.       INCOMING CALL HANDLING TREATMENT       30         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.       CONTACT CENTER CONFIGURATION       31         5.12.       ACD Configuration for Call Queued for Handling by Agent.       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SESSION MANAGER       39         6.3.       ADD LOCATION       37         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Session Manager SIP Entity.       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR EN		5.8.	TRUNK GROUP	20		
5.11.       INCOMING CALL HANDLING TREATMENT		5.9.				
5.12.       CONTACT CENTER CONFIGURATION       31         5.12.1.       Announcements       31         5.12.2.       ACD Configuration for Call Queued for Handling by Agent.       31         5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION.       37         6.2.       SPECIFY SIP DOMAIN.       39         6.3.       ADD LOCATION.       40         6.4.       ADD SIP ENTITIES.       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       44         6.4.3.       Configure E TIME RANGES       47         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53		5.10.				
5.12.1. Announcements       31         5.12.2. ACD Configuration for Call Queued for Handling by Agent       31         5.13. AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14. SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6. CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1. AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2. SPECIFY SIP DOMAIN       37         6.3. ADD LOCATION       40         6.4. ADD SIP ENTITIES       41         6.4. ADD SIP ENTITIES       41         6.4. ADD SIP ENTITIES       41         6.4. Configure Communication Manager SIP Entity       42         6.4. Configure Communication Manager SIP Entity       42         6.5. ADD ENTITY LINKS       45         6.6. CONFIGURE TIME RANGES       47         6.7. ADD ROUTING POLICIES       47         6.8. ADD DIAL PATTERNS       49         7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1. LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2. GLOBAL PROFILES       56         7.2. Configure Server Intervorking Profile - Avaya Site       56         7.2. Configure Server Intervorking Profile - SFR SIP Trunk Site       57         7.2.3. Con						
5.12.2. ACD Configuration for Call Queued for Handling by Agent						
5.13.       AVAYA AURA® COMMUNICATION MANAGER STATIONS       35         5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES       35         6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2.       SPECIFY SIP DOMAIN       37         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       42         6.4.3.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Communication Manager SIP Entity       45         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       56         7.2.3.       Configure Server Interworking Profile - Avaya Site       56         7.2.4.       Configure Server Interworking Profile - S						
5.14.       SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES						
6.       CONFIGURE AVAYA AURA® SESSION MANAGER       36         6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2.       SPECIFY SIP DOMAIN       39         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2.3.       GLOBAL PROFILES       56         7.2.1.       Configure Server Interworking Profile - Avaya Site       56         7.2.2.       Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3.       Configure Server - Avaya Site       56         7.2.4.       Configure Server - Avaya Site       59         7.2.5.       Configure Server - Avaya Site						
6.1.       AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION       37         6.2.       SPECIFY SIP DOMAIN       39         6.3.       ADD LOCATION       40         6.4.       ADD SIP ENTITIES       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2.       GLOBAL PROFILES       56         7.2.1.       Configure Server Interworking Profile - Avaya Site       56         7.2.2.       Configure Signaling Manipulation       58         7.2.3.       Configure Signaling Manipulation       58         7.2.4.       Configure Signaling Manipulation       58         7.2.5.       Configure Routing – Avaya Site       59 <td< td=""><td></td><td></td><td></td><td></td></td<>						
6.2.       SPECIFY SIP DOMAIN	6.	CON	FIGURE AVAYA AURA® SESSION MANAGER	36		
6.3.       ADD LOCATION						
6.4.       ADD SIP ENTITIES.       41         6.4.1.       Configure Session Manager SIP Entity       42         6.4.2.       Configure Communication Manager SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       44         6.4.3.       Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2.       GLOBAL PROFILES       56         7.2.1.       Configure Server Interworking Profile - Avaya Site       56         7.2.2.       Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3.       Configure Server - Avaya Site       59         7.2.4.       Configure Server - SFR SIP Trunk       61         7.2.6.       Configure Routing - Avaya Site       64         7.2.7.       Configure Routing - SFR SIP Trunk Site       65						
6.4.1. Configure Session Manager SIP Entity.       42         6.4.2. Configure Communication Manager SIP Entity       44         6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5. ADD ENTITY LINKS       45         6.6. CONFIGURE TIME RANGES       47         6.7. ADD ROUTING POLICIES       47         6.8. ADD DIAL PATTERNS       49         7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1. LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2. GLOBAL PROFILES       56         7.2.1. Configure Server Interworking Profile - Avaya Site       56         7.2.2. Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3. Configure Server - Avaya Site       59         7.2.4. Configure Server - Avaya Site       59         7.2.5. Configure Routing - Avaya Site       59         7.2.6. Configure Routing - Avaya Site       61         7.2.7. Configure Routing - Avaya Site       64         7.2.7. Configure Routing - SFR SIP Trunk Site       65						
6.4.2. Configure Communication Manager SIP Entity       44         6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5. ADD ENTITY LINKS       45         6.6. CONFIGURE TIME RANGES       47         6.7. ADD ROUTING POLICIES       47         6.8. ADD DIAL PATTERNS       49         7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1. LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2. GLOBAL PROFILES       56         7.2.1. Configure Server Interworking Profile - Avaya Site       56         7.2.2. Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3. Configure Server - Avaya Site       58         7.2.4. Configure Server - Avaya Site       59         7.2.5. Configure Server - SFR SIP Trunk       61         7.2.6. Configure Routing - Avaya Site       61         7.2.7. Configure Routing - SFR SIP Trunk Site       64						
6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity       45         6.5. ADD ENTITY LINKS       45         6.6. CONFIGURE TIME RANGES       47         6.7. ADD ROUTING POLICIES       47         6.8. ADD DIAL PATTERNS       49         7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1. LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2. GLOBAL PROFILES       56         7.2.1. Configure Server Interworking Profile - Avaya Site       56         7.2.2. Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3. Configure Server - Avaya Site       59         7.2.4. Configure Server - Avaya Site       59         7.2.5. Configure Server - SFR SIP Trunk       61         7.2.6. Configure Routing - Avaya Site       64         7.2.7. Configure Routing - SFR SIP Trunk Site       65						
6.5.       ADD ENTITY LINKS       45         6.6.       CONFIGURE TIME RANGES       47         6.7.       ADD ROUTING POLICIES       47         6.8.       ADD DIAL PATTERNS       49         7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2.       GLOBAL PROFILES       56         7.2.1.       Configure Server Interworking Profile - Avaya Site       56         7.2.2.       Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3.       Configure Signaling Manipulation       58         7.2.4.       Configure Server – Avaya Site       59         7.2.5.       Configure Server – SFR SIP Trunk       61         7.2.6.       Configure Routing – Avaya Site       64         7.2.7.       Configure Routing – SFR SIP Trunk Site       65						
6.6.CONFIGURE TIME RANGES						
6.7.       ADD ROUTING POLICIES						
6.8.       ADD DIAL PATTERNS						
7.       CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.1.       LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE       53         7.2.       GLOBAL PROFILES       56         7.2.1.       Configure Server Interworking Profile - Avaya Site       56         7.2.2.       Configure Server Interworking Profile - SFR SIP Trunk Site       57         7.2.3.       Configure Signaling Manipulation       58         7.2.4.       Configure Server - Avaya Site       59         7.2.5.       Configure Server - SFR SIP Trunk       61         7.2.6.       Configure Routing - Avaya Site       64         7.2.7.       Configure Routing - SFR SIP Trunk Site       65						
7.1.LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE537.2.GLOBAL PROFILES567.2.1.Configure Server Interworking Profile - Avaya Site567.2.2.Configure Server Interworking Profile - SFR SIP Trunk Site577.2.3.Configure Signaling Manipulation587.2.4.Configure Server - Avaya Site597.2.5.Configure Server - SFR SIP Trunk617.2.6.Configure Routing - Avaya Site647.2.7.Configure Routing - SFR SIP Trunk Site65	7.	CON	FIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	53		
7.2.GLOBAL PROFILES	-					
7.2.1. Configure Server Interworking Profile - Avaya Site567.2.2. Configure Server Interworking Profile - SFR SIP Trunk Site577.2.3. Configure Signaling Manipulation587.2.4. Configure Server - Avaya Site597.2.5. Configure Server - SFR SIP Trunk617.2.6. Configure Routing - Avaya Site647.2.7. Configure Routing - SFR SIP Trunk Site65						
7.2.2. Configure Server Interworking Profile – SFR SIP Trunk Site577.2.3. Configure Signaling Manipulation587.2.4. Configure Server – Avaya Site597.2.5. Configure Server – SFR SIP Trunk617.2.6. Configure Routing – Avaya Site647.2.7. Configure Routing – SFR SIP Trunk Site65		=.				
7.2.3. Configure Signaling Manipulation						
7.2.4. Configure Server – Avaya Site597.2.5. Configure Server – SFR SIP Trunk617.2.6. Configure Routing – Avaya Site647.2.7. Configure Routing – SFR SIP Trunk Site65						
7.2.5. Configure Server – SFR SIP Trunk617.2.6. Configure Routing – Avaya Site647.2.7. Configure Routing – SFR SIP Trunk Site65						
7.2.6. Configure Routing – Avaya Site						
7.2.7. Configure Routing – SFR SIP Trunk Site						
		7.2.8	Configure Topology Hiding	66		

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

	7.3.	DOMAIN POLICIES	68
	7.3.1	. Create Application Rules	68
	7.3.2	Create Media Rules	69
		Create Signaling Rules	
		!. Create Endpoint Policy Groups	
	7.4.	DEVICE SPECIFIC SETTINGS	
		. Manage Network Settings	
		P. Create Media Interfaces	
		Create Signaling Interfaces	
		P. Configuration Server Flows	
		4.4.1 Create End Point Flows – SMVM Flow	
	7.	4.4.2 Create End Point Flows – SFR SIP Trunk Flow	80
8.	SFR	SIP TRUNK CONFIGURATION	81
9.	VER	RIFICATION STEPS	81
10.	CON	NCLUSION	82
11.	REF	ERENCES	83
12.	APP	ENDIX A – REMOTE WORKER CONFIGURATION	84
	12.1.	NETWORK MANAGEMENT ON AVAYA SBCE	
	12.2.	MEDIA INTERFACE ON AVAYA SBCE	
	12.3.	SIGNALING INTERFACE ON AVAYA SBCE	
	12.4.	ROUTING PROFILE ON AVAYA SBCE	
	12.5.	USER AGENT ON AVAYA SBCE	
	12.6.	APPLICATION RULES ON AVAYA SBCE	
	12.7.	END POINT POLICY GROUPS ON AVAYA SBCE	
	12.8.	END POINT FLOWS ON AVAYA SBCE	
		1. Subscriber Flow	
		2. Server Flow on Avaya SBCE	
		2.8.2.1 Remote Worker Server Flow	
	12.9.	2.8.2.2 Trunking Server Flow	
		SYSTEM MANAGER 1. Modify Session Manager Firewall: Elements $\rightarrow$ Session Manager $\rightarrow$ Network Configuration $\rightarrow$	
		1. Modify Session Manager Firewall. Elements – Session Manager – Network Configuration wall	
	12 0	2. Disable PPM Limiting: Elements $\rightarrow$ Session Manager $\rightarrow$ Session Manager Administration	102
	12.10.	REMOTE WORKER CLIENT CONFIGURATION	
		Global Settings Screen	
13.		ENDIX B - SIGMA SCRIPT	
10			

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between SFR and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager 8.0, Avaya Aura<sup>®</sup> Communication Manager 8.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.0 and various Avaya endpoints, listed in **Section 4**.

Customers using this Avaya SIP-enabled enterprise solution with SFR SIP Trunk are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

## 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to SFR SIP Trunk via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the SFR SIP Trunk Service did not include use of any specific encryption features as requested by SFR.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

## 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test.

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various Avaya deskphone types including H.323, SIP, digital, and analog at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X<sup>®</sup> Communicator (1XC) and Avaya Equinox<sup>TM</sup> for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Equinox<sup>TM</sup> for Windows was used in testing as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060, between the Avaya enterprise and SFR
- Direct IP-to-IP Media (also known as "Shuffling") over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server.
- Various call types including: local call, international, outbound call to short number, Police, Firemen services
- Codec G.711A, G.729
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura<sup>®</sup> Messaging and EC500 mobility (extension to cellular)
- SIP re-Invite/Update in off-net call transfer
- SIP Diversion header in off-net call forward
- Call Center scenarios
- Fax T.38 mode
- DTMF RFC2833
- Remote Worker

The following was not supported:

- TLS/SRTP SIP transport
- Use of the SIP REFER method for network call redirection (transferring calls with the PSTN back to the PSTN)

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	5 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

### 2.2. Test Results

Interoperability testing of SFR was completed with successful results with limitation and observation below:

- SIP INVITE and 200 OK messages from SFR to the enterprise included T.38 attributes in the SDP, even for calls that were not T.38 Fax calls SFR was unable to remove T.38 attributes from the SDP, this was part of SFR network behavior. An issue was found during the compliance test related to the T.38 attributes in the SDP when using Avaya one-X Communicator. The work-around to this issue is to use a SIP Signaling Manipulation Script (SigMa) on Avaya SBCE to remove the T.38 attributes (See Section 7.2.3 for details)
- **Fax support**: Fax calls using the T.38 protocol failed during the compliance test. G.711 pass-through fax was also tested, but it behaved unreliably. The issue related to G.711 pass-through fax failing during the compliance test may be related to the unpredictability of G.711 pass-through techniques, which only works well on networks with very few hops and with limited end-to-end delay. The issue related to T.38 fax calls failing is related to the PSTN carriers used by SFR to route calls to the PSTN, not all PSTN carriers used by SFR support T.38. This issue could be resolved by SFR selecting specific PSTN carriers that do support T.38 and routing T.38 fax traffic via these PSTN carriers.

### 2.3. Support

For technical support on the Avaya products described in these Application Notes visit: <u>http://support.avaya.com</u>.

For technical support on SFR SIP Trunking, contact SFR at https://www.sfrbusiness.fr/

# 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to SFR SIP Trunk. This is the configuration used for compliance testing.

For confidentiality and privacy purposes, actual public IP Addresses used in this testing have been masked out and replaced with fictitious IP Addresses throughout the document.

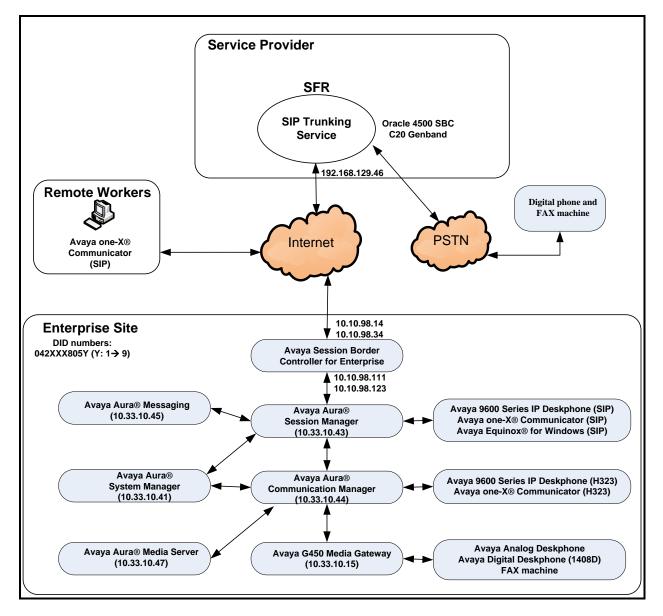


Figure 1: Avaya IP Telephony Network and SFR SIP Trunk

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

# 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components				
Equipment/Software Release/Version				
Avaya Aura <sup>®</sup> Communication Manager	8.0.0.1.2.822.25183			
running on VMware <sup>®</sup> -based Avaya appliance				
Avaya G450 Media Gateway	HW2 FW40.25			
– MM711AP Analog	HW46 FW096			
<ul> <li>MM712AP Digital</li> </ul>	HW10 FW014			
– MM710AP	HW5 FW020			
Avaya Aura <sup>®</sup> Session Manager	8.0.1.1.801103			
running on VMware <sup>®</sup> -based Avaya appliance				
Avaya Aura <sup>®</sup> System Manager	8.0.1.1			
running on VMware <sup>®</sup> -based Avaya appliance	Build-8.0.0.931077			
	Revision 8.0.1.1.039340			
Avaya Aura <sup>®</sup> Messaging	7.1.0.1.532.002.0 (SP1)			
running on VMware <sup>®</sup> -based Avaya appliance				
Avaya Aura <sup>®</sup> Media Server	8.0.0.183			
running on VMware <sup>®</sup> -based Avaya appliance				
Avaya Session Border Controller for Enterprise	8.0.0.19-16991			
running on Dell R210 V2 Server				
Avaya 9621G IP Deskphone (SIP)	Avaya <sup>®</sup> Deskphone SIP 7.1.5.0.11			
Avaya 9621G IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone			
	6.8.003			
Avaya 9641 IP Deskphone (H.323)	Avaya <sup>®</sup> IP Deskphone			
	6.8.003			
Avaya Digital Deskphone (1408D)	R48			
Avaya Equinox <sup>TM</sup> for Windows	3.5.5.113.24			
Avaya one-X <sup>®</sup> Communicator (H.323 & SIP)	6.2.13.2-SP13 Patch 1			
Avaya Analog Deskphone	N/A			
HP Officejet 4500 Fax	N/A			
SFR SIP Trunk				
Equipment/Software	Release/Version			
Oracle 4500 SBC	SCZ7.2.0 MR-5 Patch 4			
C20 Genband	R18			

#### **Table 1: Equipment and Software Tested**

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

**Note**: It is assumed the general installation of VMware<sup>®</sup>- based Avaya Appliance Virtualization Platform, Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> System Manager, Avaya Aura<sup>®</sup> Session Manager, Avaya Aura<sup>®</sup> Messaging, Avaya Aura<sup>®</sup> Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for SFR SIP Trunk.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

### 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 30000 SIP trunks are available and 100 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options OPTIONAL FEATURES		Page	<b>2</b> of 12
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	12000	0	
Maximum Concurrently Registered IP Stations:	18000	2	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	41000	0	
Maximum Video Capable IP Softphones:	18000	5	
Maximum Administered SIP Trunks:	30000	100	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	688	0	

Figure 2: System-Parameters Customer-Options Form – Page 2

On Page 4, verify that ARS is set to y.



#### Figure 3: System-Parameters Customer-Options Form – Page 4

On Page 6, verify that Private Networking and Processor Ethernet are set to y.

```
display system-parameters customer-options
                                                               Page
                                                                      6 of 12
                               OPTIONAL FEATURES
               Multinational Locations? n
                                                     Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n
                                           Station as Virtual Extension? y
                    Multiple Locations? n
                                           System Management Data Transfer? n
         Personal Station Access (PSA)? y
                                                        Tenant Partitioning? y
                                               Terminal Trans. Init. (TTI)? y
                       PNC Duplication? n
                                                       Time of Day Routing? y
                  Port Network Support? n
                                              TN2501 VAL Maximum Capacity? y
                       Posted Messages? y
                                                       Uniform Dialing Plan? y
                    Private Networking? y
                                            Usage Allocation Enhancements? y
              Processor and System MSP? y
                    Processor Ethernet? y
                                                         Wideband Switching? y
                                                                   Wireless? n
                         Remote Office? y
         Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

Figure 4: System-Parameters Customer-Options Form – Page 6

### 5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred back to the PSTN then leave the field set to **none**.

```
change system-parameters featuresPage1 of19FEATURE-RELATED SYSTEM PARAMETERS<br/>Self Station Display Enabled? nTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing? nAutomatic Callback - No Answer Timeout Interval (rings): 3<br/>Call Park Timeout Interval (minutes): 10Off-Premises Tone Detect Timeout Interval (seconds): 20<br/>AAR/ARS Dial Tone Required? y
```

#### Figure 5: System-Parameters Features Form – Page 1

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both. The value of **anonymous** is replaced for restricted numbers and unavailable numbers (refer to **Section 5.8**).

```
Page 9 of 19
change system-parameters features
                       FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous
DISPLAY TEXT
                                       Identity When Bridging: principal
                                       User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n
INTERNATIONAL CALL ROUTING PARAMETERS
              Local Country Code:
         International Access Code:
SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n
CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

Figure 6: System-Parameters Features Form – Page 9

### 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP Addresses as below:

- Messaging: Name: AAMVM, IP Address: 10.33.10.45
- Media Server: Name: AMS, IP Address: 10.33.10.47
- Session Manager: Name: bvwasm2, IP Address: 10.33.10.43
- Communication Manager: Name: procr, IP Address: 10.33.10.44

These node names will be needed for defining the service provider signaling group in **Section 5.7**.

change node-name:	s ip		Page	1 of	2
		IP NODE NAMES			
Name	IP Address				
AAMVM	10.33.10.45				
AMS	10.33.10.47				
bvwasm2	10.33.10.43				
default	0.0.0.0				
procr	10.33.10.44				
procr6	::				

#### Figure 7: Node-Names IP Form

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. In the compliance test, **ip-codec-set 1** was used for this purpose. SFR supports the **G.729**, and **G.711A** codecs. Default values can be used for all other fields.

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

        IP CODEC SET

        Codec Set: 1

        Audio
        Silence
        Frames
        Packet
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
        V
```

#### Figure 8: IP-Codec-Set Form – Page 1

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. On **Page 2**, set the **FAX Mode** to **t.38-standard**. SFR supports T.38 mode. (See **Section 2.2** for related t.38 Fax issues)

change ip-codec-set 1				Page	<b>2</b> of	2
	IP CODEC SET					
	Allow Direc	t-IP Multimedia	? n			
	Mode	Redundancy		E	Packet S	ize(ms)
FAX	t.38-standard	0	ECM:	У		
Modem	off	0				
TDD/TTY	US	3				
H.323 Clear-channel	n	0				
SIP 64K Data	n	0			20	

Figure 9: IP-Codec-Set Form – Page 2

### 5.5. IP Network Region for Media Gateway, Media Server

Network region provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. For the compliance test, IP network region 1 was chosen for the service provider trunk.

Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev.com**. This name appears in the From header of SIP messages originating from this IP region
- Enter a descriptive name in the **Name** field
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **Section 5.7**
- Set the Codec Set field to the IP codec set defined in Section 5.4
- Default values can be used for all other fields

change ip-network-region 1 Page 1 of 20						
IP NETWORK	REGION					
Region: 1						
Location: 1 Authoritative Domain:	bvwdev.com					
Name: procr Stub Net	work Region: n					
MEDIA PARAMETERS Intra-reg	ion IP-IP Direct Audio	: yes				
Codec Set: 1 Inter-reg	ion IP-IP Direct Audio	: yes				
UDP Port Min: 2048	IP Audio Hairpinning	? n				
UDP Port Max: 3329						
DIFFSERV/TOS PARAMETERS						
Call Control PHB Value: 46						
Audio PHB Value: 46						
Video PHB Value: 26						
802.1P/Q PARAMETERS						
Call Control 802.1p Priority: 6						
Audio 802.1p Priority: 6						
Video 802.1p Priority: 5 AUD	IO RESOURCE RESERVATIO	N PARAM	ETERS			
H.323 IP ENDPOINTS	RSVP E	nabled?	n			
H.323 Link Bounce Recovery? y						
Idle Traffic Interval (sec): 20						
Keep-Alive Interval (sec): 5						
- Keep-Alive Count: 5						
-						

#### **Figure 10: IP-Network-Region Form**

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (**10.33.10.44**), and that the gateway **MGP IPv4 Address** is **10.33.10.15**. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
display media-gateway 1
                                                              Page 1 of
                                                                            2
                            MEDIA GATEWAY 1
                   Type: g450
                   Name: g450
             Serial No: 12TGXXX00244
   Link Encryption Type: any-ptls/tls Enable CF? n
         Network Region: 1
                                           Location: 1
                                          Site Data:
          Recovery Rule: none
             Registered? y
  FW Version/HW Vintage: 40 .25 .0 /2
       MGP IPV4 Address: 10.33.10.15
       MGP IPV6 Address:
  Controller IP Address: 10.33.10.44
            MAC Address: 3c:4a:73:6b:c5:a8
  Mutual Authentication? optional
```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an **MM712** media module supporting Avaya digital phones in slot **V1**, an **MM711** supporting analog phones on slot **V2**, and the capability to provide announcements and music on hold via "gateway-announcements" in logical slot **V9**.

```
Page 2 of 2
display media-gateway 1
                             MEDIA GATEWAY 1
                                 Type: g450
Slot Module Type
V1: MM712
                                                       DSP Type FW/HW version
MP80 170 7
                              Name
                                                      MP80
                              DCP MM
V2: MM711
                              ANA MM
V3:
 V4:
 V5:
 V6:
 V7:
 V8:
                                                     Max Survivable IP Ext: 8
       gateway-announcements ANN VMM
 V9:
```

Figure 12: Media Gateway – Page 2

HV: Reviewed:

SPOC 6/5/2019

Solution & Interoperability Test Lab Application Notes	16 of 105
©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1
MEDIA SERVER
Media Server ID: 1
Signaling Group: 11
Voip Channel License Limit: 10
Dedicated Voip Channel Licenses: 10
Node Name: AMS
Network Region: 1
Location: 1
Announcement Storage Area:
```

Figure 13: Media Server

### 5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**.

```
      change ip-interface procr
      IP INTERFACES

      Type: PROCR
      Target socket load: 19660

      Enable Interface? y
      Allow H.323 Endpoints? y

      Network Region: 1
      Allow H.248 Gateways? y

      IPV4 PARAMETERS
      Subnet Mask: /24
```

#### Figure 14: IP-Interface Form

### 5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups.

For the compliance test, signaling group **20** was used for the signaling group between Communication Manager and Session Manager. It was used for outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- Set the Group Type field to sip
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager
- Set the **Transport Method** to the value of **tls** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3
- Set the **Far-end Node Name** to **bvwasm2**. This node name maps to the IP Address of Session Manager as defined in **Section 5.3**
- Set the Near-end Listen Port and Far-end Listen Port to a valid unused port for TLS, such as 5061

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	18 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the **Far-end Domain** to **bvwdev.com**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the Alternate Route Timer (sec) to 6. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval
- Default values may be used for all other fields

Page 1 of 2 add signaling-group 20 SIGNALING GROUP Group Number: 20 Group Type: sig IMS Enabled? n Transport Method: tls Group Type: sip Q-SIP? n IP Video? n Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Prepend '+'to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y Remove '+' from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n Near-end Node Name: procr Far-end Node Name: bywasm2 Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Secondary Node Name: Far-end Domain: bvwdev.com Bypass If IP Threshold Exceeded? n Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Session Establishment Timer(min): 3 Enable Layer 3 Test? y Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Enable Layer 3 Test? y Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload IP-IP Audio Connections? y IP Audio Hairpinning? n Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6

#### Figure 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the Group Type field to sip
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- Set the Near-end Node Name to procr. This node name maps to the IP Address of Communication Manager as defined in Section 5.3

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	19 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

- Set the **Far-end Node Name** to **AMS**. This node name maps to the IP Address of Media Server as defined in **Section 5.3**
- Set the Near-end Listen Port to 9061 and Far-end Listen Port to a valid unused port for TLS, such as 5071
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**
- Set the Far-end Domain to 10.33.10.47 (This is Media Server IP Address)

```
      change signaling-group 11
      Page 1 of 2

      SIGNALING GROUP
      SIGNALING GROUP

      Group Number: 11
      Group Type: sip<br/>Transport Method: tls

      Peer Detection Enabled? n Peer Server: AMS

      Near-end Node Name: procr<br/>Near-end Listen Port: 9061

      Far-end Node Name: procr<br/>Far-end Listen Port: 5071<br/>Far-end Network Region: 1

      Far-end Domain: 10.33.10.47
```

#### Figure 16: Signaling-Group 11

### 5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group for Session Manager created in **Section 5.7**.

For the compliance test, trunk group **20** was used for both outbound and inbound calls to the service provider. It was configured using the parameters highlighted below.

- Set the Group Type field to sip
- Enter a descriptive name for the **Group Name**
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. (e.g., **\*020**). Note: Refer to **Section 5.10** for adding \* in dialing plan
- Set Class of Restriction (COR) to 1
- Set **Direction** to **two-way** for trunk group **20**
- Set the **Service Type** field to **public-ntwrk**
- Set Member Assignment Method to auto
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group 20 was associated to signaling group 20
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk
- Default values were used for all other fields

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	20 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

add trunk-group 20		Page 1 of 4
	TRUNK GROUP	
Group Number: 20	Group Type: sip	CDR Reports: y
Group Name: SIP Trunks	COR: 1	TN: 1 TAC: *020
Direction: two-way	Outgoing Display? n	
Dial Access? n	Nigh <sup>-</sup>	t Service:
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member A:	ssignment Method: auto
		Signaling Group: 20
	N	umber of Members: 50

Figure 17: Trunk-Group – Page 1

On Page 2, set the Redirect On OPTIM Failure timer to the same amount of time as the Alternate Route Timer on the signaling group form in Section 5.7. Note that the Redirect On OPTIM Failure timer is defined in milliseconds. Verify that the Preferred Minimum Session Refresh Interval (sec) is set to a value acceptable to the service provider. This value defines the interval that UPDATEs must be sent to keep the active session alive. For the compliance test, the value of 1200 seconds was used.

add trunk-group 20 Group Type: sip TRUNK PARAMETERS Unicode Name: auto Redirect On OPTIM Failure: 6000 SCCAN? n Digital Loss Group: 18 Preferred Minimum Session Refresh Interval (sec): 1200 Disconnect Supervision - In? y Out? y XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n

Figure 18: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10-digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **public** unk (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to y. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

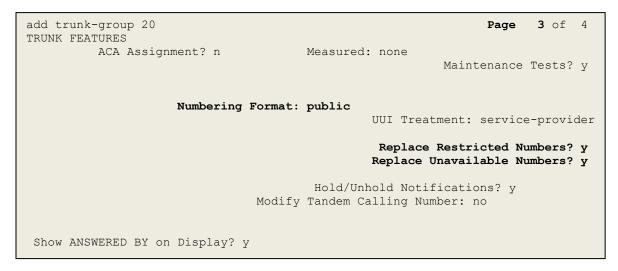


Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that CM will not send SIP Refer in redirected calls. Note: In the compliance test, SFR did not support SIP Refer. SFR supported SIP re-Invite/Update in redirected calls.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been redirected. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging. The **Diversion Header** is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

```
add trunk-group 20
                                                                           4 of 4
                                                                    Page
                              PROTOCOL VARIATIONS
                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 101
                        Convert 180 to 183 for Early Media? n
                 Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
```

Figure 20: Trunk-Group – Page 4

## 5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "P-Asserted-Identity" headers. Since public numbering was selected to define the format of this number (Section 5.8), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and it is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single public-unknown-numbering entry can be applied for all extensions. In the compliance test, stations with a 4-digit extension beginning with **805** will send the calling party number as the **CPN Prefix** plus the extension number.

**Note**: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a '+' in front of user number in From, P-Asserted-Identity, Contact, and Diversion headers. This plus sign will be removed by using the SIP manipulation on SBCE (See Session 7.2.3).

<b>change public-unknown-numbering 0</b> NUMBERING - PUBLIC/UNKNOWN FORMAT					1 of	2
Ext Ext Len Code	Trk Grp(s)	CPN Prefix	Total CPN Len			
4 805	20	042xxx	10			

Figure 21: Public-Unknown-Numbering Form

## 5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an "outside line". This configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- Dialed String beginning with 805 for extension (ext)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with \* for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

change dial	plan anal	lysis					Page	1 of	12
				AN ANALY	SIS TABLE all		ercent F	ull: 2	
Dialed String 181 189 3 800 805 9 *	4 ex 4 e 4 ex <b>4 ex</b> <b>1 f</b>		Dialed String	Total Length		Dialed String	Total Length		

Figure 22: Dialplan–Analysis Form

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection** (**ARS**) – **Access Code 1**.

change feature-access-codes	Page	1 of	11
FEATURE ACCESS CODE (FAC)	1 ago	- 01	
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialin3g List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code: *111			
Answer Back Access Code:			
Attendant Access code:			
Auto Alternate Routing (AAR) Access Code:			
Auto Route Selection (ARS) - Access Code 1: 9 Access C	ode 2:		
Automatic Callback Activation: Deactivati	on:		
Call Forwarding Activation Busy/DA: All: Deactivati	on:		
Call Forwarding Enhanced Status: Act: Deactivati	on:		
Call Park Access Code:			
Call Pickup Access Code:			
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code:			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation: Deactiv			
Contact Closure Open Code: Close C	ode:		

Figure 23: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk group to the service provider (as defined next).

change ars analysis	0						Page	1 of	2
			ARS DIGIT Loca	ANALYSIS tion: all			Percent F	ull: 1	
Dialed	Tot	al	Route	Call	Node	ANI			
String	Min	Max	Pattern	Туре	Num	Reqd			
0	1	15	20	pubu					
17	2	2	20	pubu	1	n			
18	2	2	20	pubu	1	n			
32	4	4	20	pubu	1	n			
33	11	11	20	pubu	1	n			
825	9	9	20	pubu	1	n			

Figure 24: ARS-Analysis Form

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern 20 for the compliance test.

- **Pattern Name**: Enter a descriptive name
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **20** was used
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level
- **Numbering Format**: Set this field to **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

change route-pattern 20 Page 1 of 3 Pattern Number: 5 Pattern Name: SP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC Mrk Lmt List Del Digits OSIG No Dqts Intw 1: 20 0 n user 2: n user 3: user n 4: n user 5: n user 6: n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts Format Subaddress pub-unk 1: yyyyyn n rest none 2: yyyyyn n rest none 3: y y y y y n n rest none 4: y y y y y n n rest none 5: ууууул п rest none 6: уууууп п rest none

#### Figure 25: Route–Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction**: **none**. This setting allows the outbound call using feature access code (fac) 9 over SIP trunks.

1 of 23 change cor 1 Page CLASS OF RESTRICTION COR Number: 1 COR Description: FRL: 0 APLT? y Can Be Service Observed? n Calling Party Restriction: none Can Be A Service Observer? n Called Party Restriction: none Time of Day Chart: 1 Forced Entry of Account Codes? n Priority Queuing? n Direct Agent Calling? n Facility Access Trunk Test? n Direct Agent Calling? n Restriction Override: none Restricted Call List? n Can Change Coverage? n Access to MCT? y Fully Restricted Service? n Group II Category For MFC: 7 Hear VDN of Origin Annc.? n Send ANI for MFE? n Add/Remove Agent Skills? n MF ANI Prefix: Automatic Charge Display? n Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n Can Be Picked Up By Directed Call Pickup? n Can Use Directed Call Pickup? n Group Controlled Restriction: inactive

Figure 26: Class of Restriction Form

HV; Reviewed: SPOC 6/5/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 29 of 105 SFRCMSMSBCE80

## 5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by the service provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **20**. Use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers as follows:

- The incoming DID number **042XXX8059** to **8000** by deleting **10** of the incoming digits for voicemail testing purpose. (8000 is voice mail pilot number)
- The incoming DID number **042XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose

change inc-call-handling-trmt trunk-group 20 INCOMING CALL HANDLING TREATMENT					1 of	3	
Service/	Number	Number	Del Insert				
Feature	Len	Digits					
public-ntwrk	10	042XXX8059	10 8000				
public-ntwrk	10	042XXX	6				

Figure 27: Inc-Call-Handling-Trmt Form

### 5.12. Contact Center Configuration

This section describes the basic commands used to configure Announcements, Hunt-Groups, Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke Communication Manager to perform various call-related functions.

### 5.12.1. Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command "add announcement <extension>". The extension is an unused extension number.

list announcement				
Announcement	ANNOU	NCEMENTS/AUDIO SOURCES		Num of
Extension	Type	Name	Source	Files
1898	integrated	SP2	001V9	1
1899	integrated	SP1	001V9	1

#### Figure 28: Announcement Configuration

### 5.12.2. ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt-group, and agentloginID used to queue inbound calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

display hunt-group 13	Page 1 of 3
HUNT GROUP	
GROUP NUMBER: 13 Group Name: SP GROUP EXTENSION: 3211 GROUP TYPE: UCD-MIA TN: 1	ACD? y Queue? y Vector? y
COR: 1 SECURITY CODE: 1234 Local Agent	MM Early Answer? n Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited Calls Warning Threshold: Port: Time Warning Threshold: Port:	

#### Figure 29: Hunt Group Configuration – Page 1

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

display hunt-group 13		Page	2 of	3
	HUNT GROUP			
Skill? y	Expected Call Handling Time (sec)	: 180		
AAS? n	Service Level Target (% in sec):	80 in 2	0	

### Figure 30: Hunt Group Configuration – Page 2

VDN 8055, shown below, is associated with vector 3

display vdn 8055				Page	1 of	3
	VECTOR DIRECT	ORY NUMBER				
	EXTENSION: 8	055				
	Name*: Coi	ntact Center				
	DESTINATION: V	ECTOR NUMBER	3			
	Attendant Vectoring? n	l				
	Meet-me Conferencing? n	l				
	Allow VDN Override? n	l				
	COR: 1					
	TN*: 1					
	Measured: n	ione				

Figure 31: VDN Configuration

In this simple example, vector 3 briefly plays ring back, then plays announcement 1899 (Step 02). This is an announcement heard when the call is first answered before the call is queued to the skill 13 (Step 03). If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear announcement 1898 (Step 05). Once an agent becomes available, the call will be delivered to the agent.

display vector 3 Page 1 of 6 CALL VECTOR

Number: 3 Name: Contact Center
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y

01 wait-time 2 secs hearing ringback
02 announcement 1899
03 queue-to skill 13 prim
04 wait-time 2 secs hearing silence
05 announcement 1898
06 goto step 3 if unconditionally

#### Figure 32: Vector 3 Configuration

The following screen illustrates an example agent-loginID 3311. In the sample configuration, an Avaya IP Deskphone logged in using agent-loginID 3311 and the configured password to staff and take a call for skill 13.

```
add agent-loginID 3311
                                                                           2
                                                             Page
                                                                  1 of
                                 AGENT LOGINID
                Login ID: 3311
                                                                 AAS? n
                    Name: SP
                                                                AUDIX? n
                      TN: 1
                                                       LWC Reception: spe
                                   LWC Log External Calls? n
AUDIX Name for Messaging:
                     COR: 1
           Coverage Path:
           Security Code: 1234
                                        LoginID for ISDN/SIP Display? n
                                                            Password: 1234
                                               Password (enter again): 1234
                                                         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:
                                                                        :
```

#### Figure 33: Agent-loginID Configuration – Page 1

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (SN) has been set to 13.

```
Display agent-loginID 3311 Page 2 of

AGENT LOGINID

Direct Agent Skill:

Call Handling Preference: skill-level Local Call Preference? n

SN RL SL SN RL SL

1: 13 1 16:

2: 17:
```

#### Figure 34: Agent LoginID Configuration – Page 2

To enable a telephone or one- $X^{\otimes}$  Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

Figure 35: Enable Expert Agent Selection

2

Page 11 of 19

## 5.13. Avaya Aura<sup>®</sup> Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 8051. Use the **add station 8051** command to add an Avaya H.323 IP Deskphone.

- Enter Type: 9621, Name: H323-8051, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X<sup>®</sup> Communicator)
- Leave other values as default

Page 1 of 5 add station 8051 STATION Lock Messages? n Security Code: \* Coverage Path 1: 1 Coverage Path 2: Extension: 8051 BCC: 0 TN: 1 Type: 9621 COR: 1 COS: 1 Port: S000055 Name: H323-8051 Hunt-to Station: Tests? y STATION OPTIONS Time of Day Lock Table: Loss Group: 19 Personalized Ringing Pattern: 1 Speakerphone: 2-way Display Language: English able GK Node Name: Message Lamp Ext: 8051 Survivable GK Node Name: Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? y IP Video softphone? n Short/Prefixed Registration Allowed: default Customizable Labels? V

Figure 36: Add-Station Form

### 5.14. Save Avaya Aura<sup>®</sup> Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

# 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Time Ranges, which define the time-based-routing
- Routing Policies, which define route destinations and control call routing between the SIP Entities
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call

It may not be necessary to create all the items above when configuring a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

# 6.1. Avaya Aura<sup>®</sup> System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as **https://<ip-address>/SMGR**, where **<ip-address>** is the IP Address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

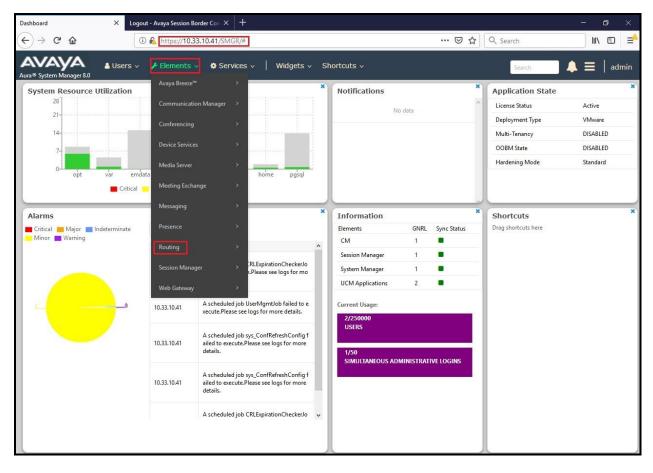


Figure 37: System Manager Home Screen

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

Aura® System Manager 8.0	Users v 🖌 Elements v 🌢 Services v 🛛 Widgets v Shortcuts v Search 🔰 🗮 🛛 admin
Home Routing	
Routing ^	Introduction to Network Routing Policy
Domains	Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
Locations	The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:
	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
Adaptations	Step 2: Create "Locations"
SIP Entities	Step 3: Create "Adaptations"
	Step 4: Create "SIP Entities"
Entity Links	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
Time Ranges	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
Routing Policies	Step 5: Create the "Entity Links"
Dial Patterns	- Between Session Managers
Regular Expressions	- Between Session Managers and "other SIP Entities"
Regular Expressions	Step 6: Create "Time Ranges"
Defaults	- Align with the tariff information received from the Service Providers
	Step 7: Create "Routing Policies"
	- Assign the appropriate "Routing Destination" and "Time Of Day"
	(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
	Step 8: Create "Dial Patterns"
	- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
	Step 9: Create "Regular Expressions"
	- Assign the appropriate "Routing Policies" to the "Regular Expressions"
	Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".
	IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

#### Figure 38: Network Routing Policy

# 6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.com**.

Navigate to **Routing**  $\rightarrow$  **Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name**: Enter the domain name
- **Type**: Select **sip** from the pull-down menu
- Notes: Add a brief description (optional)

Click **Commit** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

Avra® System Manager 8.0	▲ Users v 🖌 Elements v 🌣 Services v 📔 Widgets v	Shortcuts v	Search 👃 🗮 🛛 admin
Home Routing			
Routing	Domain Management		Help ?
Domains	New Edit Delete Duplicate More Actions •		
	1 Item		Filter: Enable
Adaptations	Name Name	Type Notes	
SIP Entities	Select : All, None	sip	

Figure 39: Domain Management

### 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville-GSSCP**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing**  $\rightarrow$  **Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

- Name: Enter a descriptive name for the Location
- Notes: Add a brief description (optional)

Click Commit to save

AVAYA Aura © System Manager 8.0	Users 🗸 🌶 Elements 🗸 🔷 Services 🗸 ╞ Widge	ets v Shortcuts v	Search 🔔 🗮 🛛 admin
Home Routing			
Routing ^	Location Details	Commit Cancel	Help ? 🔺
Domains		Comme Carter	
Locations	General * Name:	Belleville-GSSCP	
Adaptations	Notes:	Belleville-GSSCP	
SIP Entities			
on critica	Dial Plan Transparency in Survivable Mode	_	
Entity Links	Enabled:		
Time Ranges	Listed Directory Number:		
Routing Policies	Associated CM SIP Entity:		
Dial Patterns	Overall Managed Bandwidth		
Regular Expressions	Managed Bandwidth Units:	Kbit/sec 🗸	
	Total Bandwidth:		
Defaults	Multimedia Bandwidth:		
	Audio Calls Can Take Multimedia Bandwidth:		
	Per-Call Bandwidth Parameters		
	Maximum Multimedia Bandwidth (Intra-Location):	2000 Kbit/Sec	
	Maximum Multimedia Bandwidth (Inter-Location):	2000 Kbit/Sec	
	* Minimum Multimedia Bandwidth:	64 Kbit/Sec	
	* Default Audio Bandwidth:	80 Kbit/sec 🗸	
<	Alarm Threshold		
	Overall Alarm Threshold:	80 🗸 ‰	v

**Figure 40: Location Configuration** 

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. In the **Location Pattern** section, click **Add** to enter **IP Address Pattern**. The following patterns were used in testing:

- IP Address Pattern: 10.33.10.\*, 10.33.5.\*, 10.10.98.\*
- Click **Commit** to save

Loca	tion Pattern Remove			
3 Ite	ms 🥲			Filter: Enable
	IP Address Pattern	*	Notes	
	* 10.33.10.*			
	* 10.33.5.*			
	* 10.10.98.*			
Selec	t : All, None			
		Commit		

**Figure 41: IP Ranges Configuration** 

Note: Call bandwidth management parameters should be set per customer requirement.

### 6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes Communication Manager and Avaya SBCE.

Navigate to **Routing**  $\rightarrow$  **SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

٠	Name:	Enter a descriptive name
٠	FQDN or IP Address:	Enter the FQDN or IP Address of the SIP Entity that is
		used for SIP signaling
٠	Туре:	Select Session Manager for Session Manager, CM for
		Communication Manager and SIP Trunk for Avaya SBCE
٠	Adaptation:	This field is only present if <b>Type</b> is not set to <b>Session Manager</b> .
		Adaptation modules were not used in this configuration
٠	Location:	Select the Location that applies to the SIP Entity being created. For
		the compliance test, all components were located in Location
		Belleville-GSSCP
٠	Time Zone:	Select the time zone for the Location above

In this configuration, there are three SIP Entities:

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

#### 6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **bvwasm2**. The IP Address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.43**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 ╞ Widg	ets v Shortcuts v Search 🗼 🚍   admi	in
Home Routing			
Routing ^	SIP Entity Details	Help ? Commit Cancel	^
Domains	General		
Locations		bywasm2	
Adaptations	* IP Address: SIP FQDN:		
SIP Entities	Туре:	Session Manager	
Entity Links	Notes:	SM	
Time Ranges	Location:	Belleville-GSSCP V	
n n	Outbound Proxy:		
Routing Policies	Time Zone:	America/Toronto	
Dial Patterns	Minimum TLS Version:	Use Global Setting 🗸	
Regular Expressions	Credential name:		
Defaults	Monitoring		
Deraults	SIP Link Monitoring:	Use Session Manager Configuration 🗸	
	CRLF Keep Alive Monitoring:	CRLF Monitoring Disabled	

Figure 42: Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- Port: Port number on which Session Manager listens for SIP requests
- **Protocol**: Transport protocol to be used with this port
- **Default Domain**: The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save

The compliance test used port **5061** with **TLS** for connecting to Communication Manager and Avaya SBCE

Listen Ports TCP Failover port: TLS Failover port:				
Add Remove				
4 Items 🍣				Filter: Enable
Listen Ports	*	Protocol Default Domain	Notes	
5061		TLS  bvwdev.com		
Select : All, None				

Figure 43: Session Manager SIP Entity Port

#### 6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **CM8**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP Address of Communication Manager **10.33.10.44**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

Avra® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🗳	Services v   Widge	ets v Shortcuts v Search	📄 🜲 🗮   admin
Home Routing				
Routing ^	SIP Entity Details		Commit Cancel	Help ? ^
Domains	General			
Locations		* Name:	CM8	
Adaptations		* FQDN or IP Address:		
SIP Entities		Type: Notes:		
Entity Links		Adaptation:	×	
Time Ranges		100000000000000000000000000000000000000	Belleville-GSSCP v	
Routing Policies	* SIP	Time Zone: Timer B/F (in seconds):	America/Toronto	
Dial Patterns		Minimum TLS Version:	Use Global Setting 🗸	
Regular Expressions		Credential name:		
Defaults		Securable: Call Detail Recording:		
	Loop Detection	Loop Detection Mode:	Off 🗸	
	Monitoring	SIP Link Monitoring:	Link Monitoring Enabled	

Figure 44: Communication Manager SIP Entity

### 6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN** or **IP Address** field is set to the IP Address of the SBCE's private network interface **10.10.98.111**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

AVAYA Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🕻	Services v   Widge	gets v Shortcuts v Search 🗼 🚍   admin
Home Routing			
Routing ^	SIP Entity Details		Commit Cancel
Domains	General		
Locations		* Name:	
Adaptations		* FQDN or IP Address:	
SIP Entities		Type: Notes:	SIP Trunk
SIP Entities		notes.	
Entity Links		Adaptation:	
Time Ranges			Belleville-GSSCP
Routing Policies			: America/Toronto
	* SIP	Timer B/F (in seconds): Minimum TLS Version:	
Dial Patterns		Credential name:	
Regular Expressions		Securable:	
Defaults		Call Detail Recording:	egress 🗸
	Loop Detection		
		Loop Detection Mode:	On v
		Loop Count Threshold:	5
	Loop Dete	ction Interval (in msec):	: 200
	Monitoring		
		SIP Link Monitoring:	Link Monitoring Enabled

Figure 45: Avaya SBCE SIP Entity

### 6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by the service provider traffic and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing**  $\rightarrow$  Entity Links in the left-hand navigation pane and click on the New button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

- Name: Enter a descriptive name
- SIP Entity 1: Select the Session Manager being used
- **Protocol**: Select the transport protocol used for this link
- **Port**: Port number on which Session Manager will receive SIP requests from the far-end

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	45 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

- SIP Entity 2: Select the name of the other system as defined in Section 6.4
- **Port**: Port number on which the other system receives SIP requests from the Session Manager
- **Connection Policy**: Select **trusted**. **Note**: If **trusted** is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied

#### Click **Commit** to save

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

Aura® System Manager 8.0	Users 🗸 🎤 Elements 🗸 🕴	🌢 Services 🗸   Widgets 🗸	Shortcuts v			Search	] ♣ ≡	<b>∃</b>   admin
Home Routing	_							
Routing ^	Entity Links			Commi	t Cancel			Help ?
Domains	Entry Entry			Continu				
Locations	1 Item							Filter: Enable
Adaptations	□ Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
SIP Entities	SM_CM_TLS_5061	* Q bvwasm2	TLS 🗸	* 5061	* Q CM8	* 5061		trusted 🗸
Entity Links	< Select : All, None							>

Figure 46: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4**, **7.2.6** and **7.4.3**.

© System Manager 8.0 me Routing	占 Users 🦄	🗸 🎤 Elements 🗸 🤹	Services v   Widgets v	Shortcuts 🗸				Se	arch	▲ =	admin
uting ^ Domains		ity Links			Comm	t Cancel					He
	1 Ite	m @									Filter: Enal
Adaptations		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SIP Entities											

Figure 47: Avaya SBCE Entity Link

# 6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, select **Routing**  $\rightarrow$  **Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

AVAYA Aura® System Manager 8.0	🛔 Users 🗸	🖌 🔑 Elem	ents v	Servic	es v	Wid	gets 🗸	Shorto	cuts v			Search	▲ ≡	admin
Home Routing														
Routing	Tim	e Rang	es											Help ?
Domains	New	Edit D	elete) (C	uplicate	More	Actions	•							
Locations	1 Ite	im											Filter	: Enable
Adaptations		Name	Мо	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes		
on r an		24/7	~	~	~	~	~	V	V	00:00	23:59	Time Range 2	4/7	
SIP Entities	Selec	t : All, None												
Entity Links														
Time Ranges														



# 6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added; one for Communication Manager and one for Avaya SBCE.

To add a Routing Policy, navigate to **Routing**  $\rightarrow$  **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	47 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

- Name: Enter a descriptive name
- Notes: Add a brief description (optional)

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields.

Click **Commit** to save

The following screen shows the **Routing Policy Details** for the policy named **SFR Inbound Calls** associated with incoming PSTN calls from SFR to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM8**.

AV/ Aura® Syste	m Manager 8.0	Users 🗸 🎤 Elemen	ts 🗸 🌼 Services 🗸 🍐	Widgets v Shortcuts v		S	earch	▲ ≡	admin
Home	Routing								
Routing		Routing Poli	cy Details		Commit Cancel				Help ? 🔺
Dom Locat		General	Ē	* Name: SFR Inbound Calls					
Conc	itions		D	isabled:					
Adap	tations ~		L	Notes:					
SIP E	ntities	SIP Entity as De	estination						
Entity	Links	Select							
Time	Ranges	Name	FQDN or IP Addre	ess		Туре	Notes		
Routi	ng Policies	CM8 Time of Day	10.33.10.44			CM			

Figure 49: Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **SFR Outbound Calls** associated with outgoing calls from Communication Manager to the PSTN via SFR SIP Trunk through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

AVAYA Aura® System Manager 8.0	🛔 Users 🗸 🍃 Elemen	ts 🗸 🏘 Services 🗸	Widgets v Shortcuts v		Se	arch	. 🔳   admin
Home Routing							
Routing	A Routing Poli	cy Details		Commit Cancel			Help ? 🔨
Domains	General						
Locations			* Name: SFR Outbound Calls				
Conditions			Disabled:				
Adaptations	S∳.	Ľ	Notes:				
SIP Entities	SIP Entity as De	stination					
Entity Links	Select						
Time Ranges	Name	FQDN or IP Ad	ldress		Туре	Notes	
nine kanges	SBCE	10.10.98.111			SIP Trunk		
Routing Policies	Time of Day						

#### Figure 50: Routing to SFR SIP Trunk

# 6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to SFR SIP Trunk through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing**  $\rightarrow$  **Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

In the General section, enter the following values. Use default values for all remaining fields.

٠	Pattern:	Enter a dial string that will be matched against the Request-URI of the
		call

- Min: Enter a minimum length used in the match criteria
- Max: Enter a maximum length used in the match criteria
- SIP Domain: Enter the destination domain used in the match criteria
- Notes: Add a brief description (optional)

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	49 of 105
SPOC 6/5/2019	©2019 Avaya Inc. All Rights Reserved.	SFRCMSMSBCE80

Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns were similarly defined.

The first example shows that outbound 13-digit dialed numbers that begin with **0** and have a destination **SIP Domain** of **bvwdev.com** uses **Routing Policy Name** as **SFR Outbound Calls** which is defined in **Section 6.7**.

AVAYA Aura® System Manager 8.0	🛓 Users 🗸 🖌 Elements 🗸 🔹 Services 🗸   Widgets 🗸 Shortcuts 🗸	Search 🛕 🗮   admin
Home Routing		
Routing	Dial Pattern Details	Help ?
Domains	General	
Locations	* Pattern: 0	
Conditions	* Min: 3	
Adaptations	Emergency Call:	
SIP Entities	SIP Domain: bvwdev.com V Notes: SFR Outbound Calls	
Entity Links	Notes: SFR Outbound Calls	
Time Ranges	Originating Locations and Routing Policies	
Routing Policies	1 Item 🥲	Filter: Enable
Dial Patterns		outing Policy estination Routing Policy Notes
Regular Expressions	-ALL- SFR Outbound Calls 0 Select : All, None	SBCE

#### Figure 51: Dial Pattern\_0

Note that with the above Dial Pattern, SFR did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **0427** use **Routing Policy Name** as **SFR Inbound Calls** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by SFR.

AVAYA Aura® System Manager 8.0	Lusers ∨	🜲 🗮   admin
Home Routing		
Routing	Dial Pattern Details Commit Cancel	Help ?
Domains	General	
Locations	* Pattern: 0427	
Conditions	* Min: 4	
Adaptations 🗸 🗸	* Max: 10	
SIP Entities	SIP Domain: bvwdev.com 🗸	
Entity Links	Notes: SFR Inbound Calls	
Time Ranges	Originating Locations and Routing Policies	
Routing Policies	Add Remove	Filter: Enable
Dial Patterns ~	Originating Location Name         Originating Location         Routing Policy Name         Rank         Routing Policy Disabled         Routing Policy Destination	Routing Policy Notes
Regular Expressions	-ALL-         SFR Inbound Calls         0         CM8           Select : All, None	

Figure 52: Dial Pattern\_0427

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

ome Routing										
outing	^	Dial	Patte	rns						Hel
Domains		New	Edit	Delete	Dupl	licate More Actions	•			
Locations		38 It	ems 🥲							Filter: Enabl
Conditions			Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
			<u>0</u>	3	13				bvwdev.com	SFR Outbound Calls
Adaptations	~		0427	4	10				bvwdev.com	SFR Inbound Calls
202 - 20 March 19			17	2	36				bvwdev.com	SFR Outbound Calls
SIP Entities			18	2	36				bvwdev.com	SFR Outbound Calls
Entity Links			32	2	36				bvwdev.com	SFR Outbound Calls
Entity Links			33	2	36				bvwdev.com	SFR Outbound Calls
			805	3	36				bvwdev.com	SFR SIP Phones
Time Ranges										

**Figure 53: Dial Pattern List** 

# 7. Configure Avaya Session Border Controller for Enterprise

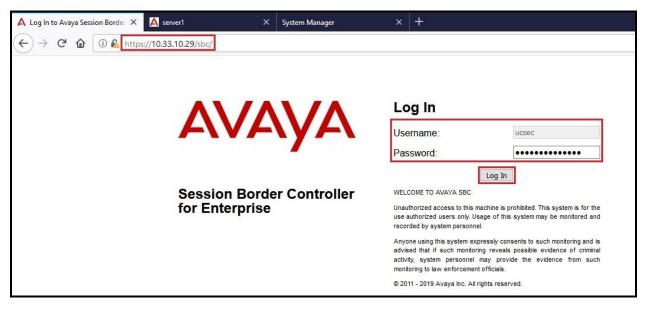
This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the SFR.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the SFR system resides on the Public side of the network.

**Note**: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

# 7.1. Log in to Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x/sbc/**" (where x.x.x.x is the management IP of the Avaya SBCE).



Enter the Username and Password and click on Log In button.

Figure 54: Avaya SBCE Login

Select **Device SBCE** and the **Dashboard** main page will appear as shown below.

Session Dorug	er Controller for	Enterprise			AVA	АУА
MS Dashboard	Dashboard					
evice Management	Information			Installed Devices		
ackup/Restore System Parameters	System Time	02:30:35 PM EDT	Refresh	EMS		
Configuration Profiles	Version	8.0.0.0-19-16991		SBCE		
Services	Build Date	Sat Jan 26 21:58:11 UTC 2019				
Domain Policies	License State	ØOK				
TLS Management	Aggregate Licensing Overages	0				
Network & Flows DMZ Services	Peak Licensing Overage Count	0				
Monitoring & Logging	Last Logged in at	04/30/2019 12:10:11 EDT				
	Failed Login Attempts	0				
	Active Alarms (past 24 hours)			Incidents (past 24 hours)		
	None found.			SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		
				SBCE: No Subscriber Flow Matched		

Figure 55: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

Device: SBCE 🗸 Alarms	Incidents Status 🛩 Lo	ogs 🗸 Diagnostics	Users				Settings 🗸	Help 🕚	<ul> <li>Log Out</li> </ul>
Session Bord	er Controller	for Enterpr	ise					A	VAYA
EMS Dashboard	Device Managem	nent							
Backup/Restore <ul> <li>System Parameters</li> </ul>	Devices Updates	SSL VPN Licensing	Key Bundles						
Configuration Profiles	Device Name	Management IP	Version	Status					
<ul><li>Services</li><li>Domain Policies</li></ul>	SBCE	10.33.10.29	8.0.0.0-19-16991	Commissioned	Reboot	Shutdown	Restart Application Vie	ew Edit	Uninstall

Figure 56: Avaya SBCE Device Management

The System Information screen shows General Configuration, Device Configuration, Network Configuration, DNS Configuration and Management IP(s) information provided during installation and corresponds to Figure 1.

			System Information: SBCE			х
General Configu	ration		Device Configuration	Dynamic License Alloc	ation ——	
Appliance Name	SBCE		HA Mode No Two Bypass Mode No		Min License Allocation	Max License Allocation
Box Type Deployment Mode			Two Bypass Mode No	Standard Sessions		Allocation 0
Deployment wou	e Ploxy			Advanced Sessions	0	0
				Scopia Video Sessions	0	0
				CES Sessions	0	0
						53 191
				Transcoding Sessions	0	0
				CLID	() <del></del> -)	
				Encryption Available: Yes		
			L			
Network Configu	iration	Public IP	Network Prefix or Subnet Mas	k Gateway		Interface
10.10.98.111		10,10,98,111	255.255.252.224	10.10.98.97		B1
10.10.98.123		10.10.98.123	255.255.255.224	10.10.98.97		B1
10.10.98.14		10.10.98.14	255.255.255.192	10.10.98.1		A1
10.10.98.34		10.10.98.34	255.255.255.192	10.10.98.1		A1
DNS Configuration	on		Management IP(s)			
Primary DNS	10.10.98.60		IP #1 (IPv4) 10.33.10.29			
Secondary DNS			1			
DNS Location	DMZ					
DNS Client IP	10.10.98.111					

Figure 57: Avaya SBCE System Information

# 7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

#### 7.2.1. Configure Server Interworking Profile - Avaya Site

Server Interworking profile allows administrator to configure and manage various SIP call server specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Configuration Profiles**  $\rightarrow$  **Server Interworking** 

- Select avaya-ru in Interworking Profiles
- Click Clone
- Enter Clone Name: SMVM and click Finish (not shown)
- Select **SMVM** in **Interworking Profiles**
- Select General tab and click Edit button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that Session Manager server interworking profile (named: SMVM) was added.

Device: SBCE ∽ Alarms I	ncidents Status 🛩 Log	s♥ Diagnostics Users		Settings 🗸 Help 🖌 Log O
Session Borde	r Controller f	or Enterprise		AVAYA
EMS Dashboard Device Management	Interworking Profile Add	es: SMVM		Rename Clone Delete
Backup/Restore System Parameters	Interworking Profiles		Click here to add a description.	
Configuration Profiles     Domain DoS     Server Interworking	cs2100 avaya-ru	General Timers Privacy URI Ma	nipulation Header Manipulation Advance	ed
Media Forking Routing	SMVM	Hold Support 180 Handling	NONE	
Topology Hiding Signaling Manipulation		180 Handling	None	
URI Groups		182 Handling 183 Handling	None	
SNMP Traps Time of Day Rules		Refer Handling	No	
FGDN Groups Reverse Proxy Policy		URI Group Send Hold	None	
Services Domain Policies		Delayed Offer	Yes	
TLS Management		3xx Handling	No	
Network & Flows		Diversion Header Support	No	
DMZ Services		Delayed SDP Handling	No	
Monitoring & Logging		Re-Invite Handling	No	
		Prack Handling	No	
		Allow 18X SDP	No	
		T.38 Support	Yes	
		URI Scheme	SIP	
		Via Header Format	RFC3261	
			Edit	

#### Figure 58: Server Interworking – Avaya site

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

#### 7.2.2. Configure Server Interworking Profile – SFR SIP Trunk Site

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Server Interworking  $\rightarrow$  Add

- Enter **Profile Name**: **SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)
- Select **SP4** in **Interworking Profiles**
- Select **General** tab and click **Edit** button
- Check **T.38 Support** option and click **Finish** (not shown)

The following screen shows that SFR server interworking profile (named: SP4) was added.

Device: SBCE Υ Alarms Ir	ncidents Status 🛩 Lo	gs ✔ Diagnostics Users		Settings 🗸 Help 🖌 Log Ou
Session Border	r Controller	for Enterprise		AVAYA
MS Dashboard Device Management Backup/Restore System Parameters	Interworking Profi	les: SP4	Click here to add a description.	Rename Clone Delete
Configuration Profiles	cs2100	General Timers Privacy URI	Manipulation Header Manipulation Advance	ed
Server Interworking Media Forking Routing Topology Hiding Signaling Manipulation URI Groups SNMP Traps Time of Day Rules FGDN Groups Reverse Proxy Policy Services Domain Policies TLS Management Network & Flows DMZ Services Monitoring & Logging	SMVM SP4 SP5	General         Hold Support         180 Handling         181 Handling         182 Handling         183 Handling         183 Handling         Refer Handling         URI Group         Send Hold         Delayed Offer         βxx Handling         Diversion Header Support         Delayed SDP Handling         Re-Invite Handling         Prack Handling         Allow 18X SDP	NONE None None None None No No No Yes No No No No No No No No No No No No No	
		T.38 Support URI Scheme	Yes	
		Via Header Format	RFC3261	

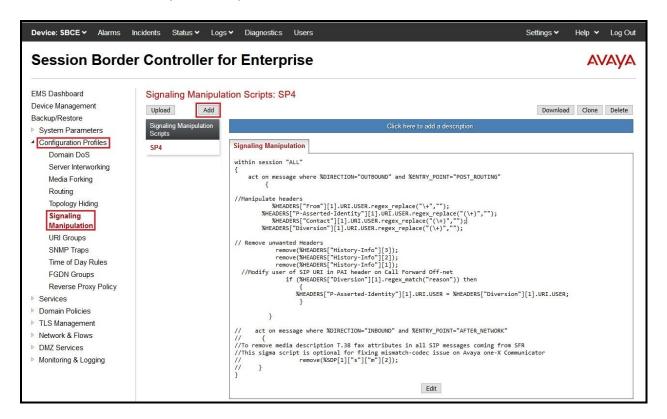
#### Figure 59: Server Interworking – SFR SIP Trunk site

### 7.2.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Signaling Manipulation  $\rightarrow$  Add

- Enter script **Title**: **SP4**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
  - Manipulate the SIP headers for outbound calls
  - Remove un-wanted headers
  - Modify user of SIP URI in PAI header on off-net call forward
  - Remove media description T.38 fax attributes in all SIP messages coming from SFR (See Section 2.2 for details)
  - Click **Save** (not shown)



**Figure 60: Signaling Manipulation** 

**Note:** See **Appendix B** in **Section 13** for the reference of this signaling manipulation (SigMa) script.

### 7.2.4. Configure Server – Avaya Site

The **SIP Servers** screen contains six tabs: **General**, **Authentication**, **Heartbeat**, **Registration**, **Ping** and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select Services  $\rightarrow$  SIP Servers  $\rightarrow$  Add

#### Enter Profile Name: SMVM

On **General** tab, enter the following:

- Server Type: Select Call Server
- **TLS Client Profile**: Select **AvayaSBCClient**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- IP Address/FQDN: 10.33.10.43 (Session Manager IP Address)
- Port: 5061
- Transport: TLS
- Click **Finish** (not shown)

Device: SBCE ~ Alarms	Incidents Status 🗸 Log	s♥ Diagnostics Users		Settings 🗸 Help 🖌 Log Out
Session Bord	er Controller f	or Enterprise		AVAYA
EMS Dashboard Device Management Backup/Restore IP System Parameters	SIP Servers: SMV	M General Authentication Heart	beat Registration Ping Advanced	Rename Clone Delete
<ul> <li>Configuration Profiles</li> <li>Services</li> <li>SIP Servers</li> <li>LDAP</li> </ul>	SMVM	Server Type TLS Client Profile DNS Query Type	Call Server AvayaSBCClient NONE/A	
RADIUS Domain Policies TLS Management Network & Flows		IP Address / FQDN 10.33.10.43	Port 5061 Edit	Transport TLS
<ul> <li>DMZ Services</li> </ul>			Luit	

Figure 61: SIP Server – General - Avaya site

On the **Advanced** tab:

- Enable Grooming box is checked
- Select **SMVM** for **Interworking Profile** (see Section 7.2.1)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced			
Enable D	oS Protection							
Enable G	Grooming							
Interwork	ing Profile		SMV	/M				
Signaling	Manipulation Scrip	t	None	e				
Securabl	e							
Enable F	GDN							
Tolerant								
URI Grou	p		None	9				
				Edi	t			

Figure 62: SIP Server – Advanced - Avaya site

#### 7.2.5. Configure Server – SFR SIP Trunk

From the menu on the left-hand side, select Services  $\rightarrow$  SIP Servers  $\rightarrow$  Add

#### Enter **Profile Name: SP4**

On **General** tab, enter the following:

- Server Type: Select Trunk Server
- IP Address/FQDN: 192.168.129.46 (SFR signaling server IP address)
- Port: 5060
- Transport: UDP
- Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Log	s♥ Diagnostics Users		Settings 🗸 Help 🖌 Log
Session Bord	er Controller f	or Enterprise		AVAY
EMS Dashboard Device Management Backup/Restore IP System Parameters	SIP Servers: SP4 Add Server Profiles	General Authentication H	leartbeat Registration Ping Advanced	Rename Clone Delet
<ul> <li>Configuration Profiles</li> <li>Services</li> <li>SIP Servers</li> </ul>	SMVM SP4	Server Type DNS Query Type	Trunk Server NONE/A	
LDAP RADIUS		IP Address / FQDN 192.168.129.46	Port 5060	Transport UDP
<ul> <li>Domain Policies</li> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>			Edit	

Figure 63: SIP Server – General – SFR site

On **Heartbeat** tab, enter the following:

- Check Enable Heartbeat
- Select Method: OPTIONS
- Set Frequency: 60 seconds
- Input From URI: ping@10.10.98.14 (Avaya SBCE public interface IP address)
- Input **To URI**: **ping@192.168.129.46** (SFR signaling server IP address)

able Heartbeat	
Method	OPTIONS
Frequency	60 seconds
From URI	ping@10.10.98.14
To URI	ping@192.168.129.46

Figure 64: SIP Server – Heartbeat – SFR site

On the **Advanced** tab, enter the following:

- Interworking Profile: SP4 (see Section 7.2.2)
- Signaling Manipulation Script: SP4 (see Section 7.2.3)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping Advanced
Enable D	oS Protection			1
Enable G	Grooming			J
Interwork	ing Profile		SP4	24
Signaling	Manipulation Scrip	t	SP4	14
Securabl	е			1
Enable F	GDN			Į
Tolerant				1
URI Grou	p		None	ne
				Edit

Figure 65: SIP Server – Advanced – SFR site

### 7.2.6. Configure Routing – Avaya Site

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server Addresses and resolution methods, next hop routing information, and packet transport types.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing and click Add as highlighted below.

Enter Profile Name: SP4\_To\_SMVM and click Next button (Not Shown)

- Select Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1
- SIP Server Profile: SMVM (see Section 7.2.4)
- Next Hop Address: 10.33.10.43:5061 (TLS) (Session Manager IP address)
- Click Finish

Device: SBCE 🗸 Alarms In								Help 🖌 Log Out
Session Border	Controller fo	or Enterp	orise					AVAYA
EMS Dashboard Device Management Backup/Restore System Parameters Configuration Profiles Domain DoS	Routing Profiles: SI Add Routing Profiles default	P4_To_SMVM	_	Routing Profil	Click here to add a description. Ie		Renam	e Clone Delete
Server Interworking Media Forking	URI Group	* ~	2		Time of Day	default v		Add
Routing Topology Hiding	Load Balancing	Priority	~		NAPTR			Delete
Signaling Manipulation	Transport	None 🗸			LDAP Routing			
URI Groups SNMP Traps	LDAP Server Profile	None 🗸			LDAP Base DN (Search)	None $\sim$		
Time of Day Rules	Matched Attribute Priority				Alternate Routing	$\checkmark$		
FGDN Groups	Next Hop Priority				Next Hop In-Dialog			_
Reverse Proxy Policy Services	Ignore Route Header							
Domain Policies								
TLS Management	ENUM				ENUM Suffix			_
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> </ul>								Add
<ul> <li>Monitoring &amp; Logging</li> </ul>	Priority / Weight 1	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profi	ile Next Hop Address		Transport None v	

Figure 66: Routing to Session Manager

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 64 of 105 SFRCMSMSBCE80

#### 7.2.7. Configure Routing – SFR SIP Trunk Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing and click Add as highlighted below.

Enter Profile Name: SMVM\_To\_SP4 and click Next button (not shown)

- Load Balancing: Priority
- Check Next Hop Priority
- Click **Add** button to add a Next-Hop Address
- Priority/Weight: 1
- Server Configuration: SP4 (see Section 7.2.5)
- Next Hop Address: 192.168.129.46:5060 (UDP) (SFR signaling server IP address)
- Click Finish

Device: SBCE - Alarms Ind	cidents Status 🛩 Logs	<ul> <li>Diagnostics</li> </ul>	Users				Settings 🗸	Help 🗸	Log Out
Session Border	Controller fo	or Enterp	orise					A۱	/AYA
EMS Dashboard Device Management Backup/Restore System Parameters Configuration Profiles Domain DoS Server Interworking	Routing Profiles: SN Add Routing Profiles default SP4_To_SMVM	NVM_To_SP4			Slick here to add a description.		Rename	Clone	Add
Media Forking Routing Topology Hiding	URI Group	* v		Routing Profil	e Time of Day NAPTR	default ~	2	×	Delete
Signaling Manipulation URI Groups SNMP Traps	Transport LDAP Server Profile	None ~	•		LDAP Routing	None V			
Time of Day Rules FGDN Groups Reverse Proxy Policy	Matched Attribute Priority Next Hop Priority				Alternate Routing Next Hop In-Dialog				
<ul> <li>Services</li> <li>SIP Servers</li> <li>LDAP</li> </ul>	Ignore Route Header								
RADIUS <ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	ENUM				ENUM Suffix			Add	
<ul> <li>Network &amp; Flows</li> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	Priority / Weight 1	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profi	le Next Hop Address 192.168.129.46:5060		Transport None ~	Delete	

Figure 67: Routing to SFR SIP Trunk

### 7.2.8. Configure Topology Hiding

The **Topology Hiding** screen allows an administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Topology Hiding

- Select default in Topology Hiding Profiles
- Click Clone
- Enter Clone Name: SP4\_To\_SMVM and click Finish (not shown)
- Select **SP4\_To\_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **To**,
  - In the Criteria column select IP/Domain
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev.com**
- For the Header **Request-Line**,
  - In the Criteria column select IP/Domain
  - In the Replace Action column select: Overwrite
  - In the **Overwrite Value** column: **bvwdev.com** Note: bvwdev.com is SIP Domain of enterprise
- For the Header **From**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev.com**

Device: SBCE ~ Alarms		ogs∨ Diagnostics User for Enterprise			Settings V Help V I	
EMS Dashboard		Profiles: SP4 To SM				
Device Management	Add	1			Rename Clone I	Delete
Backup/Restore	Topology Hiding		Click	here to add a description.		
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> </ul>	Profiles			11110 15 242 2 222 mg pilotti		
Domain DoS	default	Topology Hiding				
Server Interworking	cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value	
Media Forking	SP4_To_SMVM	Referred-By	IP/Domain	Auto		
Routing		То	IP/Domain	Overwrite	bvwdev.com	
Topology Hiding		Request-Line	IP/Domain	Overwrite	bwwdev.com	
Signaling Manipulation		From	IP/Domain	Overwrite	bwwdev.com	
URI Groups SNMP Traps		Record-Route	IP/Domain	Auto		
Time of Day Rules		SDP	IP/Domain	Auto		
FGDN Groups		Via	IP/Domain	Auto		
Reverse Proxy Policy		Refer-To	IP/Domain	Auto		
Services		Reter-10	IP/Domain	Auto		

#### Figure 68: Topology Hiding To Session Manager

HV; Reviewed: SPOC 6/5/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 66 of 105 SFRCMSMSBCE80 From the menu on the left-hand side, select **Global Profiles**  $\rightarrow$  **Topology Hiding** 

- Select default in Topology Hiding Profiles
- Click Clone
- Enter Clone Name: SMVM\_To\_SP4 and click Finish (not shown)

Session Borde	r Controller f	or Enterprise	÷		AVAYA
EMS Dashboard	Topology Hiding P	rofiles: SMVM To SI	24		
Device Management	Add				Rename Clone Delete
Backup/Restore System Parameters	Topology Hiding Profiles		Clic	k here to add a description.	
Configuration Profiles	default	Topology Hiding			
Domain DoS Server Interworking	cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value
Media Forking	SP4_To_SMVM	Referred-By	IP/Domain	Auto	-
Routing	SMVM To SP4	То	IP/Domain	Auto	
Topology Hiding		Request-Line	IP/Domain	Auto	
Signaling Manipulation		From	IP/Domain	Auto	
URI Groups SNMP Traps		Record-Route	IP/Domain	Auto	
Time of Day Rules		SDP	IP/Domain	Auto	
FGDN Groups		Via	IP/Domain	Auto	
Reverse Proxy Policy		Refer-To	IP/Domain	Auto	
Services					

Figure 69: Topology Hiding To SFR

# 7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or an administrator can create a custom domain policy.

### 7.3.1. Create Application Rules

Application rules define the type of SBC-based Unified Communication (UC) applications Avaya SBCE protects. You can also determine the maximum number of concurrent voice and video sessions that your network can process before resource exhaustion.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Application Rules** 

- Select **default** from **Application Rules** and click **Clone** button:
- Enter Clone Name (e.g., SIP-Trunk) and click Finish (not shown)
- Click on **SIP-Trunk** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
  - Check In and Out
  - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
  - Leave the **CDR Support** field at **Off** and the **RTCP Keep-Alive** field unchecked (**No**)

Device: SBCE 🛩 Alarms	Incidents Status 🗸 Log	s♥ Diagnostics Users		Settings 🛩 Help 🛩 Log Out
Session Bord	er Controller f	or Enterprise		Αναγα
EMS Dashboard Device Management	Application Rules:	SIP-Trunk		Rename Clone Delete
Backup/Restore   System Parameters  Configuration Profiles	Application Rules default	Application Rule	Click here to add a description.	
<ul> <li>Services</li> <li>Domain Policies</li> <li>Application Rules</li> <li>Border Rules</li> </ul>	default-trunk default-subscriber-low default-subscriber-high	Application Type Audio	In Out Maximum Conc	urrent Sessions Maximum Sessions Per Endpoint 2000
Media Rules Security Rules Signaling Rules	default-server-low default-server-high	Video Miscellaneous		
Charging Rules End Point Policy Groups Session Policies	SIP-Trunk RW_AR	CDR Support RTCP Keep-Alive	Off No Edit	

Click on **Finish** (not shown)

**Figure 70: Application Rule** 

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

### 7.3.2. Create Media Rules

Media Rules allow one to define media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Media Rules** 

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name**: **SMVM** Click **Finish** (not shown)
- Select SMVM under Media Rules to Edit

The Encryption tab indicates that RTP and SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80 encryption was used as **Preferred Formats** for Audio Encryption.

Device: SBCE 🛩 Alarms	Incidents Status - Logs	<ul> <li>Diagnostics Users</li> </ul>		Settings 🗸 Help 🖌 Log Out
Session Borde	er Controller fo	or Enterprise		Αναγα
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Media Rules: SMVI Add Media Rules default-low-med		Click here to add a description.	Rename Clone Delete
<ul> <li>Services</li> <li>Domain Policies</li> <li>Application Rules</li> <li>Border Rules</li> <li>Media Rules</li> <li>Security Rules</li> <li>Signaling Rules</li> <li>Charging Rules</li> <li>End Point Policy</li> </ul>	default-low-med-enc default-high default-high-enc avaya-low-med-enc SMVM SP4	Audio Encryption Preferred Formats Encrypted RTCP MKI Lifetime Interworking	RTP_AES_CM_128_HMAC	<u>SHA1_80</u>
Groups Session Policies > TLS Management > Network & Flows > DMZ Services > Monitoring & Logging		Video Encryption Preferred Formats Interworking Miscellaneous Capability Negotiation	RTP	

Figure 71: Media Rule 1

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Media Rules** 

• Select the **default-low-med** rule, click **Clone**. Enter **Clone Name**: **SP4** Click **Finish** (not shown)

Session Bord		gs • Diagnostics Users		Settings • Help • Log Ou
EMS Dashboard Device Management	Media Rules: SP4			Rename Clone Delete
Backup/Restore System Parameters	Media Rules		Click here to add a description.	
Configuration Profiles	default-low-med	Encryption Codec Prioriti	zation Advanced QoS	
Domain Policies	default-low-med-enc default-high	Audio Encryption		
Application Rules Border Rules	default-high-enc	Preferred Formats	RTP	
Media Rules	avaya-low-med-enc	Interworking		
Security Rules	SMVM	Video Encryption		
Signaling Rules Charging Rules	SP4	Preferred Formats	RTP	
End Point Policy		Interworking		
Groups Session Policies		Miscellaneous		
TLS Management		Capability Negotiation		
Network & Flows			Edit	
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>				

Figure 72: Media Rule 2

#### 7.3.3. Create Signaling Rules

In the reference configuration, Signaling Rules are used to filter various SIP headers.

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules** 

- Select the **default** rule, click **Clone**. Enter **Clone Name**: **SIP-Trunk**. Click **Finish** (not shown)
- Select SIP-Trunk under Signaling Rules
- Select the Signaling QoS tab and click on Edit button
- Verify that **Enabled** is selected
- Select **DCSP**
- Select Value = EF
- Click Finish (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Log	s♥ Diagnostics (	Users			Set	tings 🗸	Help 🗸	Log Out
Session Bord	er Controller f	or Enterpri	ise					AV	/AYA
EMS Dashboard Device Management Backup/Restore	Signaling Rules: S Add Signaling Rules	IP-Trunk		Click b	ere to add a description		Rename	Clone	Delete
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> <li>Services</li> </ul>	default No-Content-Type-Ch	General Requests	s Responses	Request Headers	Response Headers		UCID		
Domain Policies     Application Rules	SIP-Trunk	Signaling QoS 🗹 QoS Type DSCP							
Border Rules Media Rules Security Rules		DSCP		EF	Edit				
Signaling Rules Charging Rules									

Figure 73: Signaling Rule

### 7.3.4. Create Endpoint Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): Application, Border, Media, Signaling, Security, Charging and RTCP Monitoring Report Generation, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of Avaya SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **End Point Policy Groups** 

- Select Add.
- Enter Group Name: SMVM
  - Application Rule: SIP-Trunk (See in Section 7.3.1)
  - Border Rule: default
  - Media Rule: SMVM (See in Section 7.3.2)
  - Security Rule: default-low
  - Signaling Rule: SIP-Trunk (See in Section 7.3.3)
- Select **Finish** (not shown)

Device: SBCE V Alarms	Incidents Status 🛩 Log	ıs <b>∨</b> Diagn	nostics Use	rs				Settings	✓ Help Y	<ul> <li>Log Out</li> </ul>
Session Bord	er Controller f	or Ent	terprise	9					4	VAYA
EMS Dashboard Device Management	Policy Groups: SM	IVM						Re	ename Clone	e Delete
Backup/Restore <ul> <li>System Parameters</li> </ul>	Policy Groups				Click	here to add a desc	ription.			
Configuration Profiles	default-low				Hover ov	er a row to see its o	lescription.			
Services	default-low-enc									
Domain Policies	default-med	Policy Gro	oup							
Application Rules Border Rules	default-med-enc	_								Summary
Media Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Security Rules	default-high-enc	1	SIP-Trunk	default	SMVM	default-low	SIP-Trunk	None	Off	Edit
Signaling Rules	avaya-def-low-enc									
Charging Rules End Point Policy	avaya-def-high-subsc									
Groups	avaya-def-high-server									
Session Policies	SMVM									
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	SP4									
DMZ Services	SMVM_RW									

#### Figure 74: Endpoint Policy 1

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups** 

- Select Add.
- Enter Group Name: SP4
  - Application Rule: SIP-Trunk (See in Section 7.3.1)
  - Border Rule: default
  - Media Rule: SP4 (See in Section 7.3.2)
  - Security Rule: default-low
  - Signaling Rule: SIP-Trunk (See in Section 7.3.3)
- Select **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🛩 Logs	S V Diagno	ostics User	s				Settings	¥ He	elp 🗸	Log Out
Session Bord	er Controller fo	or Ent	erprise	9						AV	AYA
EMS Dashboard Device Management Backup/Restore	Policy Groups: SP4	1						Re	name	Clone	Delete
<ul> <li>System Parameters</li> <li>Configuration Profiles</li> </ul>	Policy Groups default-low				a na si	here to add a desc					
<ul> <li>Services</li> <li>Domain Policies</li> <li>Application Rules</li> </ul>	default-low-enc default-med	Policy Gro	up		Hover ov	er a row to see its o	lescription.				
Border Rules Media Rules	default-med-enc default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Gen		mmary
Security Rules Signaling Rules Charging Rules	default-high-enc avaya-def-low-enc	1	SIP-Trunk	default	SP4	default-low	SIP-Trunk	None	Off		Edit
End Point Policy Groups Session Policies	avaya-def-high-subsc avaya-def-high-server										
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	SMVM										
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	SMVM_RW										

**Figure 75: Endpoint Policy 2** 

## 7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

## 7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Network & Flows** → **Network Management**.

- Select **Networks** tab and click the **Add** button to add a network for the outside interface as follows:
  - Name: Network\_A1
  - Default Gateway: 10.10.98.1
  - Subnet Mask: 255.255.255.192
  - Interface: A1 (This is the Avaya SBCE outside interface)
  - Click the Add button to add the IP Address for inside interface: 10.10.98.14
  - Click the **Finish** button to save the changes

Device: SBCE - Alarms	Incidents Status 🛩 Logs	✓ Diagnostics Users		Settings 🛩	Help 🖌 Log Out
Session Borde	er Controller fo	or Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles > Services	Network Managem	ent			Ada
<ul> <li>Domain Policies</li> </ul>	Name	Gateway Subnet Ma Length			
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	Network_B1		Add Network		X Edit Delete
Network Management Media Interface Signaling Interface End Point Flows Session Flows	Network_A1	Name Default Gateway Network Prefix or Subnet Mask Interface	Network_A1 10.10.98.1 255.255.192 A1 ~		Edit Defete
Advanced Options <ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>			blic IP Gateway Or e IP Address Use Default Finish		

#### Figure 76: Network Management – Outside Interface

From the menu on the left-hand side, select **Network & Flows** → **Network Management**.

- Select **Networks** tab and click **Add** button to add a network for the inside interface as follows:
  - Name: Network\_B1
  - Default Gateway: 10.10.98.97
  - Subnet Mask: 255.255.255.224
  - Interface: B1 (This is the Avaya SBCE inside interface)
  - Click the Add button to add the IP Address for outside interface: 10.10.98.111
  - Click the **Finish** button to save the changes

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🕯	<ul> <li>Diagnostics Users</li> </ul>		Settings 🗸	Help 👻 Log Out
Session Borde	r Controller fo	r Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters	Network Manageme	nt			
Configuration Profiles					Add
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name	Gateway Subnet Length	: Mask / Prefix Interface	IP Address	
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	Network_B1		Add Network		X Edit Delete
Network	Network_A1	Name	Network_B1		Edit Delete
Management Media Interface		Default Gateway	10.10.98.97		
Signaling Interface		Network Prefix or Subnet Mask	255.255.255.224		
End Point Flows Session Flows		Interface	B1 ~		
Advanced Options				Add	T
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>		IP Address	Public IP Gateway Ove	rride	
- workening & Logging		10.10.98.111	Use IP Address Use Default	Delete	
			Finish		

Figure 77: Network Management – Inside Interface

From the menu on the left-hand side, select Network & Flows → Network Management

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

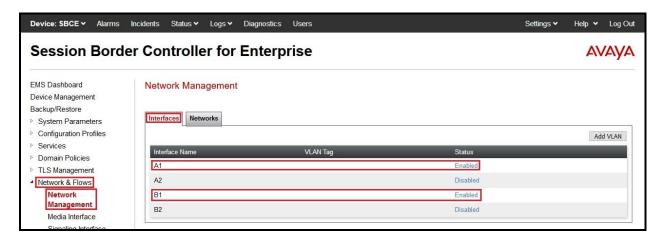


Figure 78: Network Management – Interface Status

## 7.4.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for inside port.

From the menu on the left-hand side, **Device Specific Settings**  $\rightarrow$  **Media Interface** 

- Select the **Add** button and enter the following:
- Name: OutsideMedia
- IP Address: Select Network\_A1 (A1,VLAN0) and 10.10.98.14 (External IP address toward SFR)
- Port Range: 35000 40000
- Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - Name: InsideMedia
  - IP Address: Select Network\_B1 (B1,VLAN0) and 10.10.98.111 (Internal IP address toward Session Manager)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)

Device: SBCE - Alarms	Incidents Status 🗸 Logs 🕯	<ul> <li>Diagnostics</li> </ul>	Users	Settings 🗸	Help 🗸	Log Out
Session Borde	er Controller fo	r Enterp	rise		A	VAYA
EMS Dashboard	Media Interface					
Device Management						
Backup/Restore						
System Parameters	Media Interface					
Configuration Profiles						Add
Services			Media IP			
Domain Policies	Name		Network	Port Range		
TLS Management	OutsideMedia		10.10.98.14 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Network & Flows Network Management	InsideMedia		10.10.98.111 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Media Interface						
Signaling Interface						

**Figure 79: Media Interface** 

## 7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
  - Name: OutsideUDP
  - IP Address: Select Network\_A1 (A1,VLAN0) and 10.10.98.14 (External IP address toward SFR)
  - UDP Port: 5060
  - Click **Finish** (not shown)

From the menu on the left-hand side, select Network & Flows → Signaling Interface

- Select the **Add** button and enter the following:
  - Name: InsideTLS
  - IP Address: Select Network\_B1 (B1,VLAN0) and 10.10.98.111 (Internal IP address toward Session Manager)
  - TLS Port: 5061
  - **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
  - Click **Finish** (not shown)

**Note**: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as SFR used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

Device: SBCE ∽ Alarms	Incidents Status 🛩 Logs	<ul> <li>Diagnostics</li> </ul>	Users				Settin	ıgs 🗸	Help 🗸	Log Out
Session Borde	er Controller fo	or Enterp	rise						AV	/AYA
EMS Dashboard Device Management Backup/Restore > System Parameters > Configuration Profiles	Signaling Interface									
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Name	Signaling II Network	P	TCP Port	UDP Port	TLS Port	TLS Profile	-		Add
TLS Management	OutsideUDP	10.10.98.1 Network_A1 (		-	5060		None		Edit	Delete
<ul> <li>Network &amp; Flows</li> <li>Network Management</li> <li>Media Interface</li> </ul>	InsideTLS	10.10.98.11 Network_B1 (				5061	AvayaSBCServer		Edit	Delete
Signaling Interface End Point Flows										

**Figure 80: Signaling Interface** 

## 7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and apply a policy.

#### 7.4.4.1 Create End Point Flows – SMVM Flow

From the menu on the left-hand side, select Network & Flows → End Point Flows

- Select the Server Flows tab
- Select Add, enter Flow Name: SMVM Flow
  - Server Configuration: SMVM (see Section 7.2.4)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: OutsideUDP (see Section 7.4.3)
  - Signaling Interface: InsideTLS (see Section 7.4.3)
  - Media Interface: InsideMedia (see Section 7.4.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SMVM (see Section 7.3.4)
  - Routing Profile: SMVM To SP4 (see Section 7.2.7)
  - Topology Hiding Profile: SP4\_To\_SMVM (see Section 7.2.8)
  - Leave other parameters as default
  - Click Finish

Device: SBCE 🛩 Alarms Ir								
Session Border	r Controll	er for Enterpris	e				AVA	yа
EMS Dashboard Device Management Backup/Restore ▹ System Parameters	End Point Flo							
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>			Add Flow	×			Add	
Domain Policies	Modifications m	Flow Name	SMVM Flow					
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	SIP Server: S	SIP Server Profile	SMVM ~			_	_	
Network Management	Update	URI Group	* ~					
Media Interface Signaling Interface	Priority Flov	Transport	* ~	Profi				
End Point Flows Session Flows	1 SM	Remote Subnet	*	·o_S	SP4 View	Clone E	dit Delete	
Advanced Options	2 SM	Received Interface	OutsideUDP ~	`o_5	SP5_AS View	Clone E	Edit Delete	
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	3 SM	Signaling Interface	InsideTLS ~		View	Clone E	dit Delete	
Monitoring & Logging	SIP Server: S	Media Interface	InsideMedia 🗸					
	Priority Flov	Secondary Media Interface	None ~	ing	Profile			
	1 SP2	End Point Policy Group	SMVM ~	-	SMVM View	01000		
		Routing Profile	SMVM_To_SP4 ~	_10_	_SIVIVIM View			
	SIP Server: S	Topology Hiding Profile	SP4_To_SMVM V			_	_	
	Priority Flov	Signaling Manipulation Script	None ~	ing	Profile			
	1 SP	Remote Branch Office	Any ~	_To_	_SMVM View	Clone E	dit Delete	
	SIP Server: S	Link Monitoring from Peer						
	Priority Flow		Finish	ing	Profile			See 2

#### Figure 81: End Point Flow 1

HV; Reviewed: SPOC 6/5/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved. 79 of 105 SFRCMSMSBCE80

#### 7.4.4.2 Create End Point Flows – SFR SIP Trunk Flow

From the menu on the left-hand side, select Network & Flows → End Point Flows

- Select the Server Flows tab
- Select Add, enter Flow Name: SP4 Flow
  - Server Configuration: SP4 (see Section 7.2.5)
  - URI Group: \*
  - Transport: \*
  - Remote Subnet: \*
  - Received Interface: InsideTLS (see Section 7.4.3)
  - Signaling Interface: OutsideUDP (see Section 7.4.3)
  - Media Interface: OutsideMedia (see Section 7.4.2)
  - Secondary Media Interface: None
  - End Point Policy Group: SP4 (see Section 7.3.4)
  - Routing Profile: SP4\_To\_SMVM (see Section 7.2.6)
  - Topology Hiding Profile: SMVM\_ To\_SP4 (see Section 7.2.8)
  - Leave other parameters as default
  - Click Finish

Device: SBCE 🛩 Alarms Ir	ncidents Status 🗸	Logs 🗸 Diagnostics	Users		Settings 🗸	Help 🖌 L	.og Out
Session Border	r Controll	er for Enterp	rise			AVA	ŊА
EMS Dashboard Device Management Backup/Restore System Parameters	End Point Flo						
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>			Add Flow	x		Add	
Domain Policies	Modifications m	Flow Name	SP4 Flow				
<ul> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>		SIP Server Profile	SP4 V				-
Network Management	SIP Server: S	URI Group	* ~				
Media Interface Signaling Interface	Priority Flow	Transport	* v	Profile	_		
End Point Flows	1 SM	Remote Subnet	*	o SP4	View Clo	ne Edit Delete	
Session Flows Advanced Options	2 SM	Received Interface	InsideTLS ~	_			
DMZ Services	3 SM	Signaling Interface	OutsideUDP v	w		ne Edit Delete	
Monitoring & Logging		Media Interface	OutsideMedia 🗸		View Cit		
	SIP Server: S	Secondary Media Interface	None ~		_		
	Priority Flow	End Point Policy Group	SP4 V	ing Profil	•		
	1 SP4	Routing Profile	SP4_To_SMVM V	_To_SM\	M View Clo	ne Edit Delete	
	SIP Server: S	Topology Hiding Profile	SMVM_To_SP4 v				3
	Priority Flow	Signaling Manipulation Script	None	ing Profil			
	1 SPE	Remote Branch Office	Any 🗸	_To_SM\	M View Clo	ne Edit Delete	
	SIP Server: S	Link Monitoring from Peer					
	Priority Flov		Finish	ing Profil			

Figure 82: End Point Flow 2

HV; Reviewed: SPOC 6/5/2019

Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

# 8. SFR SIP Trunk Configuration

SFR is responsible for the configuration of SFR SIP Trunk Service. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. SFR will provide the customer necessary information to configure the SIP connection between Avaya SBCE and SFR. SFR also provides the SFR SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between SFR SIP Trunk and the enterprise is a static IP Address configuration.

## 9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

- 1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- 2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- 3. Verify that the user on the PSTN can end an active call by hanging up.
- 4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

- 1. Communication Manager: Enter the following commands using the Communication Manager System Access Terminal (SAT) interface.
  - **list trace station** <extension number> Traces calls to and from a specific station.
  - **list trace tac** <trunk access code number> Trace calls over a specific trunk group.
  - **status station** <extension number> Displays signaling and media information for an active call on a specific station.
  - **status trunk-group** <trunk-group number> Displays trunk-group state information.
  - **status signaling-group** <signaling-group number> Displays signaling-group state information.
- 2. Session Manager:
  - Call Routing Test The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to Elements → Session Manager → System Tools → Call Routing Test. Enter the requested data to run the test.
  - **traceSM** Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
- 3. Avaya SBCE: Debug logging can be started in two different ways:
  - GUI of the SBC: Monitoring & Logging → Debugging. Check on Debug option
    - SIP only: enable LOG\_SUB\_SIPCC subsystem under SSYNDI process.
    - CALL PROCESSING: enable all subsystems under SSYNDI process.
    - The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
  - **Command Line Interface**: Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Session Manager and Avaya Session Border Controller for Enterprise to SFR. This solution successfully passed compliance testing via the Avaya DevConnect Program.

## 11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at: <u>http://support.avaya.com/</u>

#### Avaya Aura® Session Manager/System Manager

- [1] Administering Avaya Aura<sup>®</sup> Session Manager, Release 8.0.1, Issue 3, December 2018
- [2] Administering Avaya Aura® System Manager, Release 8.0.1, Issue 6, January 2019

## Avaya Aura<sup>®</sup> Communication Manager

[3] Administering Avaya Aura ®Communication Manager, Release 8.0.1, Issue 3, December 2018

## Avaya Phones

- [4] Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323, Issue 2, March 2018
- [5] Installing and Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones SIP, Issue 3, March 2018
- [6] Avaya one-X® Communicator Release 6.2 SP13 Release Notes, Issue 1.0, February 2019
- [7] Avaya Equinox® Client (Windows) Release 3.5.5 (Feature Pack) Release Notes, Issue 1.1, April 2019

#### Avaya Session Border Controller for Enterprise

[8] Avaya Session Border Controller for Enterprise 8.0 Release Notes, Release 8.0.0.0, Issue 1 November 2018

#### IETF (Internet Engineering Task Force) SIP Standard Specifications

[9] RFC 3261 SIP: Session Initiation Protocol, <u>http://www.ietf.org/</u>

Product documentation for SFR SIP Trunking may be found at: https://www.sfrbusiness.fr/

# 12. Appendix A – Remote Worker Configuration

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet, access through the Avaya SBCE to Session Manager on the private enterprise. It builds on the Avaya SBCE configuration described in previous sections of this document.

In the reference configuration, an existing Avaya SBCE is provisioned to access the SFR SIP Trunk Services (see **Section 2.1** of this document). The Avaya SBCE also supports Remote Worker configurations, allowing remote SIP endpoints (connected via the public Internet) to access the private enterprise.

Supported endpoints are Avaya 96x1 SIP Deskphones, Avaya one- $X^{\text{®}}$  Communicator SIP softphone and Avaya Equinox<sup>TM</sup> for Windows SIP softphone.

Note: In the compliance testing, only Avaya one- $X^{\mathbb{B}}$  Communicator SIP softphone was used to test as the remote worker.

Standard and Advanced Session Licenses are required for the Avaya SBCE to support Remote Workers. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

## 12.1. Network Management on Avaya SBCE

The following screen shows the **Network Management** of the Avaya SBCE. The Avaya SBCE is configured with two "outside" IP Addresses assigned to physical interface A1, and two "inside" IP Addresses assigned to physical interface B1.

**Note**: A SIP Entity in Session Manager was not configured for the Avaya SBCE's internal IP Address used for Remote Worker. This keeps the Remote Worker interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.

These are the IP Addresses used in the reference configuration:

- **10.10.98.14** is the Avaya SBCE "outside" IP address previously provisioned for SIP Trunking with SFR (see Section 7.4.1)
- **10.10.98.34** is the new Avaya SBCE "outside" IP address for Remote Worker access to Session Border Controller
- **10.10.98.111** is the Avaya SBCE "inside" IP address previously provisioned for SIP Trunking with Session Manager (see Section 7.4.1)
- **10.10.98.123** is the new Avaya SBCE "inside" IP address for Remote Worker access to Session Manager

From the menu on the left-hand side, select Network & Flows → Network Management

- Enter the above **IP** Addresses and Gateway Addresses for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column accordingly

Session Bord	er Controller	for Enterpris	se			AVAY
EMS Dashboard	Network Manage	ement				
Device Management	3					
ackup/Restore						
System Parameters	Interfaces Network	(S				
Configuration Profiles						Add
Services			Subnet Mask / Prefix			
Domain Policies	Name	Gateway	Length	Interface	IP Address	
TLS Management	Network_B1	10.10.98.97	255.255.255.224	B1	10.10.98.111, 10.10.98.123	Edit Delete

#### Figure 83: Network Management

On the **Interfaces** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the SFR SIP Trunk access in **Section 7.4.1**.

Device: SBCE - Alarms	Incidents Status 🛩 Logs 🛩 Dia	gnostics Users	S	ettings 🗸 🛛 Help 👻 Log Out
Session Bord	er Controller for Er	nterprise		Αναγα
EMS Dashboard Device Management Backup/Restore > System Parameters	Network Management			
<ul> <li>Configuration Profiles</li> <li>Services</li> </ul>				Add VLAN
<ul> <li>Services</li> <li>Domain Policies</li> </ul>	Interface Name	VLAN Tag	Status	
<ul> <li>TLS Management</li> </ul>	A1		Enabled	
<ul> <li>Network &amp; Flows</li> </ul>	A2		Disabled	
Network	B1		Enabled	
Management Media Interface Signaling Interface	B2		Disabled	

**Figure 84: Network Interface Status** 

## 12.2. Media Interface on Avaya SBCE

From the menu on the left-hand side, select **Device Specific Settings**  $\rightarrow$  **Media Interface** 

- Select the **Add** button and enter the following:
  - Name: OutsideMedRW
  - **IP Address**: Select **Network\_A1 (A1, VLAN0)** and **10.10.98.34** (External IP address toward Remote Worker phones)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
  - Name: InsideMedRW
  - **IP Address**: Select **Network\_B1 (B1, VLAN0)** and **10.10.98.123** (Internal IP address toward Session Manager)
  - Port Range: 35000 40000
  - Click **Finish** (not shown)

Session Borde	er Controller for Ent	erprise		AVAY
EMS Dashboard Device Management Backup/Restore	Media Interface			
System Parameters Configuration Profiles	Media Interface			Add
Services Domain Policies	Name	Media IP Network	Port Range	
TLS Management	OutsideMedia	10.10.98.14 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Network & Flows Network Management	InsideMedia	10.10.98.111 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
Media Interface Signaling Interface	OutsideMedRW	10.10.98.34 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
End Point Flows	InsideMedRW	10.10.98.123 Network B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

#### Figure 85: Media Interface

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (**Section 12.8.1**), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

## 12.3. Signaling Interface on Avaya SBCE

The following screen shows the Signaling Interface settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

Select the Add button to create Signaling Interface OutsideSIGRW using the parameters:

- IP Address: Select Network\_A1 (A1, VLAN0) and 10.10.98.34 (External IP address toward Remote Worker phones)
- TLS Port: 5061
- **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

Select the Add button to create Signaling Interface InsideSIGRW using the parameters:

- IP Address: Select Network\_B1 (B1, VLAN0) and 10.10.98.123 (Internal IP address toward Session Manager)
- TLS Port: 5061
- **TLS Profile:** AvayaSBCServer. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use

Session Borde	er Controller for	Enterprise					AN	/AY
EMS Dashboard	Signaling Interface							
Device Management	0 0							
Backup/Restore								
System Parameters	Signaling Interface							
Configuration Profiles								Add
Services	Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Domain Policies	Name	Network	ΙCΡ Ροπ	UDP Port	ILS Port	ILS Profile		
TLS Management	OutsideUDP	10.10.98.14 Network A1 (A1, VLAN 0)	532	5060		None	Edit	Delete
<ul> <li>Network &amp; Flows</li> </ul>		10.10.98.111			5061		Edit	
Network Management	InsideTLS	Network_B1 (B1, VLAN 0)			5061	AvayaSBCServer	Edit	Delete
Media Interface Signaling Interface	OutsideSIGRW	10.10.98.34 Network_A1 (A1, VLAN 0)			5061	AvayaSBCServer	Edit	Delete
End Point Flows	InsideSIGRW	10.10.98.123			5061	AvayaSBCServer	Edit	Delete

#### • Click on **Finish** (not shown)

## **Figure 86: Signaling Interface**

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (**Section 12.8.1**), and in the Remote Worker Server Flow (**Section 12.8.2.1**). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

## 12.4. Routing Profile on Avaya SBCE

The Routing Profile **To\_SMVM\_RW** is created for routing the SIP traffic from Remote Worker to Session Manager via Avaya SBCE.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing  $\rightarrow$ Add

Enter Profile Name: To\_SMVM\_RW (not shown)

- Load Balancing: Priority
- Check Next Hop Priority
- Click Add button to add a Next-Hop Address
- Priority/Weight: 1
- SIP Server Profile: SMVM
- Next Hop Address: 10.33.10.43:5061 (TLS) (IP address of Session Manager)
- Click Finish

The Routing Profile **To\_SMVM\_RW** is used in the Subscriber Flows (Section 12.8.1).

Device: SBCE 🛩 Alarms Ir					Help 🖌 Log Out
Session Border	r Controller fo	r Enterprise			AVAYA
EMS Dashboard Device Management Backup/Restore > System Parameters Configuration Profiles Domain DoS Server Interworking	Routing Profiles: To Add Routing Profiles default SP4_To_SMVM	SMVM_RW Routing Profile Update Priority	Click here to add a description.	Renam	e Clone Delete
Media Forking Routing	SMVM_To_SP4	Ini	Routing Profile		x
Topology Hiding Signaling Manipulation URI Groups	URI Group Load Balancing	* v	Time of Day NAPTR	default 🗸	)elete
SNMP Traps Time of Day Rules	Transport	None V	LDAP Routing LDAP Base DN (Search)	None ~	
FGDN Groups Reverse Proxy Policy Services	Matched Attribute Priority		Alternate Routing		
<ul> <li>Domain Policies</li> <li>TLS Management</li> <li>Network &amp; Flows</li> </ul>	Next Hop Priority		Next Hop In-Dialog		
<ul> <li>DMZ Services</li> <li>Monitoring &amp; Logging</li> </ul>	ENUM		ENUM Suffix		
	Priority / Weight 1	LDAP Search LDAP Search Regex Pattern Regex Result	SIP Server Profile Next Hop Address SMVM  I 10.33.10.43:5061 (TL Back Finish	Transport S) V	Add

Figure 87: Remote Worker Routing to Session Manager

The Routing Profile **default\_RW** is created for routing SIP traffic from Session Manager to Remote Worker via Avaya SBCE.

From the menu on the left-hand side, select Configuration Profiles  $\rightarrow$  Routing  $\rightarrow$ Add Enter Profile Name: default\_RW

- Check Load Balancing: DNS/SRV
- **NAPTR** box is checked
- Click **Finish**

The Routing Profile default\_RW is used in the Remote Worker Server Flow in Section 12.8.2.1.

Device: SBCE - Alarms In	cidents Status ❤ Logs	<ul> <li>Diagnostics</li> </ul>	Users				Settings 🗸	Help 🐱	Log Out
Session Border	Controller fo	r Enterp	rise					AV	AYA
		fault_RW	irise Stoup Time of Day default	Load Baland DNS/SRV/ Routing Profile	Auto-Detect	ss default > None >			Delete
	Click the Add buttor	1 to add a Next-F	Hop Address.						
				Back Fini	ish				

Figure 88: Remote Worker Default Routing

## 12.5. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya one-X Communicator is used as the User Agent.

From the menu on the left-hand side, select **System Parameters**  $\rightarrow$  **User Agents** Click **Add** button to add the user agent:

- Enter Name: Avaya one-X Communicator
- Enter Regular Expression: Avaya one-X Communicator.\*
- Click on **Finish** (not shown)



Figure 89: User Agents for Remote Worker

The following abridged output of Session Manager trace shows the details of an INVITE from an Avaya one-X Communicator. The User-Agent shown in this trace will match User Agent **one-X Communicator** shown above with a **Regular Expression** of "**Avaya one-X Communicator**.". In this expression, ".\*" will match anything listed after the user agent name.

INVITE sip: 001613XXX7497@bvwdev.com SIP/2.0 From: sip:8052@bvwdev.com;tag=-59f03c7f529fb7c152aa3fd4\_F0950710.10.98.79 To: sip: 00161613XXX7497@bvwdev.com CSeq: 24 INVITE Call-ID: 18\_a7e80-49279ea452aa365c\_I@10.10.98.79 Contact: <<u>sip:8052@10.10.98.79:5061;transport=tls;subid\_ipcs=3784557512</u>>;+avaya-cm-line=1 Allow:INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRA CK Supported: eventlist, 100rel, replaces, vnd.avaya.ipo **User-Agent: Avaya one-X Communicator**/6.2.13.2 (Engine GA-2.2.0.178; Windows NT 6.2, 32-bit) Max-Forwards: 70 Via: SIP/2.0/TLS 10.10.98.79:62151;branch=z9hG4bK18\_a7e80-312c149e52aa3fe8\_I09507 Accept-Language: en Content-Type: application/sdp Content-Length: 440

## Figure 90: Output of trace for User Agent

Note: The User Agent is defined in its associated Subscriber Flows in Section 12.8.1.

## 12.6. Application Rules on Avaya SBCE

The following section describes Application Rule **RW\_AR**, used in this Remote Worker setting. In a typical customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions.

From the menu on the left-hand side, select **Domain Policies**  $\rightarrow$  **Application Rules** 

- Select default from Application Rules and click Clone button:
- Enter Clone Name (e.g., RW\_AR) and click Finish (not shown)
- Click on **RW\_AR** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
  - Check In and Out
  - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
  - Leave the **CDR Support** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**)
  - Click on **Finish** (not shown)

Device: SBCE 🛩 Alarms	Incidents Status 🗸 Logs	s∨ Diagnostics Users				Settings 🗸	• Help •	<ul> <li>Log Out</li> </ul>
Session Borde	er Controller fo	or Enterprise					A	VAYA
EMS Dashboard	Application Rules: F	RW AR						
Device Management	Add	Man da - O Martin				Rena	ame Clone	e Delete
Backup/Restore ▶ System Parameters	Application Rules		Click h	ere to a	add a description.			
Configuration Profiles	default	Application Rule						
Services	default-trunk			201				
Domain Policies	default-subscriber-low	Application Type	In	Out	Maximum Concurrent Sessions	Maximum	Sessions Per	Endpoint
Application Rules	default-subscriber-high	Audio			2000	2000		
Border Rules Media Rules	default-server-low	Video			100	10		
Security Rules	default-server-high	Miscellaneous						
Signaling Rules	SIP-Trunk	CDR Support	Off					
Charging Rules		RTCP Keep-Alive	No					
End Point Policy Groups	RW_AR				Edit			
Session Policies		L		_				

#### Figure 91: Remote Worker Application Rule

Note: The rule RW\_AR is assigned to the End Point Policy Groups in Section 12.7.

## 12.7. End Point Policy Groups on Avaya SBCE

A new End Point Policy Groups is defined for Remote Worker: SMVM\_RW.

To create the new **SMVM\_RW** group, click on **Add**. Enter the following:

- Enter a name (e.g., **SMVM\_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Enter the following:
  - Application Rule = RW\_AR (see Section 12.6)
  - Border Rule = default
  - Media Rule = SMVM (see Section 7.3.2)
  - Security Rule = default-low
  - Signaling Rule = SIP-Trunk (see Section 7.3.3)
- Click on **Finish** (not shown)

The End Point Policy Group **SMVM\_RW** is used in the Subscriber Flow **Avaya one-X Communicator** in **Section 12.8.1** and Remote Worker Server Flow in **Section 12.8.2.1**.

Device: SBCE 🗸 Alarms	Incidents Status 🛩 Log	js <b>∨</b> Diagr	nostics Use	s				Settings	s∨ Help∖	<ul> <li>Log Out</li> </ul>
Session Bord	er Controller f	or En	terprise	9					A	VAYA
EMS Dashboard Device Management Backup/Restore	Policy Groups: SM	IVM_RW						R	ename Clone	Delete
System Parameters	Policy Groups				Click	here to add a desc	ription.			
Configuration Profiles	default-low				Hover ov	er a row to see its c	lescription			
Services	default-low-enc						loosinpiton.			
Domain Policies	default-med	Policy Gr	oup							
Application Rules Border Rules	default-med-enc		-							Summary
Media Rules	default-high	Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
Security Rules	default-high-enc	1	RW_AR	default	SMVM	default-low	SIP-Trunk	None	Off	Edit
Signaling Rules	avaya-def-low-enc	-	icor_rue	deladit	ONIVIN	deladir low	on Hunt	None	01	Eur
Charging Rules	avaya-def-high-subsc									
End Point Policy Groups	,									
Session Policies	avaya-def-high-server									
TLS Management	SMVM									
Network & Flows	SP4									
DMZ Services	SMVM RW									
Monitoring & Logging										

Figure 92: Remote Worker End Point Policy

## 12.8. End Point Flows on Avaya SBCE

## 12.8.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent one-X Communicator** that was created in **Section 12.5**. The below subscriber flow is configured for Remote Worker to access Session Manager via Avaya SBCE.

From the menu on the left-hand side, select Network & Flows  $\rightarrow$  End Point Flows On the Subscriber Flows tab, click on the Add button and enter the following:

- Enter a Flow Name (e.g., Avaya one-X Communicator)
- **URI Group** = \* (default)
- User Agent = Avaya one-X Communicator (see Section 12.5)
- **Source Subnet** = \* (default)
- Via Host = \* (default)
- **Contact Host** = \* (default)
- Signaling Interface = OutsideSIGRW (see Section 12.3)

Click on Next (not shown) and the Profile window will open (not shown). Enter the following:

- Source = Subscriber
- Methods Allowed Before REGISTER = Leave as default
- Media Interface = OutsideMedRW (see Section 12.2)
- Received Interface = None.
- End Point Policy Group = SMVM\_RW (see Section 12.7)
- Routing Profile = To\_SMVM\_RW (see Section 12.4)
- TLS Client Profile = None
- Signaling Manipulation Script = None
- **Presence Server Address** = Leave as blank

Click on **Finish** (not shown).

EMS Dashboard End Point Flows	
Jevice Management	
Surface Surface Subscriber Flows Server Flows	
System Falameters	 
Configuration Profiles	Add
Services Modifications made to an End-Point Flow will only take effect on new registrations or re-registrations	
Domain Policies TLS Management Hover over a row to see its description.	
TLS Management Hover over a row to see its description. Network & Flows	
Network Management Priority Flow Name URI Group Source Subnet User Agent End Point Policy Group	
	dit Delete

#### Figure 93: Remote Worker Subscriber Flows – 1

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

	View Flow: Avay	a one-X Communicator		X	
Criteria ———		Optional Settings			
Flow Name	Avaya one-X Communicator	TLS Client Profile	None		
URI Group	*	Signaling Manipulation Script	None		
User Agent	Avaya one-X Communicator				
Source Subnet	*				
Via Host	*				
Contact Host	*				
Signaling Interface	OutsideSIGRW				
Profile		criber			
Methods Allowed B					
User Agent	Avay	a one-X Communicator			
Media Interface	Outsi	OutsideMedRW			
Secondary Media Interface		None			
End Point Policy Group SM		M_RW			
		To_SMVM_RW			
Routing Profile	To_S				

## Figure 94: Remote Worker Subscriber Flows – 2

## 12.8.2. Server Flow on Avaya SBCE

The new Remote Worker Server Flow (**SMVM\_RemoteWorker**) is configured for the SIP traffic flow from Session Manager to Remote Worker via Avaya SBCE. Two existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and SP4 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

## 12.8.2.1 Remote Worker Server Flow

From the menu on the left-hand side, select **Device Specific Settings**  $\rightarrow$  **Endpoint Flows** Select the **Server Flows** tab and click the **Add** button (not shown) to enter the following:

- Name = SMVM\_RemoteWorker
- Server Configuration = SMVM (see Section 7.2.4)
- **URI Group** = \* (default)
- **Transport** = \* (default)
- **Remote Subnet** = \* (default)
- Received Interface = OutsideSIGRW (see Section 12.3)
- Signaling Interface = InsideSIGRW (see Section 12.3)
- Media Interface = InsideMedRW (see Section 12.2)
- Secondary Media Interface = None
- End Point Policy Group = SMVM\_RW (see Section 12.7)
- Routing Profile = default\_RW (see Section 12.4)
- **Topology Hiding Profile** = **None** (default)
- **Signaling Manipulation Script = None** (default)
- **Remote Branch Office** = **Any** (default)
- Link Monitoring from Peer = uncheck (default)

Click **Finish** (not shown).

	View Flow: SM	/M_RemoteWorker	
Criteria ———		Profile	
Flow Name	SMVM_RemoteWorker	Signaling Interface	InsideSIGRW
Server Configuration	SMVM	Media Interface	InsideMedRW
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SMVM_RW
Remote Subnet	.*)	Routing Profile	default_RW
Received Interface	OutsideSIGRW	Topology Hiding Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 95: Remote Worker Server Flow

## 12.8.2.2 Trunking Server Flow

Two existing Trunking Server Flows (SMVM Flow in Section 7.4.4.1 and SP4 Flow in Section 7.4.4.2) are also used for Remote Worker.

	Vie	w Flow: SP4 Flow	
Criteria ———		Profile	
Flow Name	SP4 Flow	Signaling Interface	OutsideUDP
Server Configuration	SP4	Media Interface	OutsideMedia
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SP4
Remote Subnet	*	Routing Profile	SP4_To_SMVM
Received Interface	InsideTLS	Topology Hiding Profile	SMVM_To_SP4
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

Figure 96: Trunking Server Flow – SP4 Flow

Criteria ———		Profile	
Flow Name	SMVM Flow	Signaling Interface	InsideTLS
	CORRECTION CONTRACTOR		
Server Configuration	SMVM	Media Interface	InsideMedia
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	SMVM
Remote Subnet	*	Routing Profile	SMVM_To_SP4
Received Interface	OutsideUDP	Topology Hiding Profile	SP4_To_SMVM
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	

#### Figure 97: Trunking Server Flow – SMVM Flow

HV; Reviewed: SPOC 6/5/2019 Solution & Interoperability Test Lab Application Notes ©2019 Avaya Inc. All Rights Reserved.

## 12.9. System Manager

# 12.9.1. Modify Session Manager Firewall: Elements $\rightarrow$ Session Manager $\rightarrow$ Network Configuration $\rightarrow$ SIP Firewall

Select Rule Sets as Rule Set for SMVM, click Edit button

Session Manager       SIP Firewall Configuration         Dashboard       Create, configure and assign SIP Firewall Rule Sets to Session Managers         Session Manager Admin       Global Settings         Global Settings       New ©Duplicate redit	Hel
Global Settings     Image: Communication Profile	
Communication Profile 7 Items 🌮	
/ Items ag	
Network Configuration A Rule Sets Type Assigned Count Avaya Provided Description	
BSM 6.3.2.0         BSM         Q         Yes         Avaya provided Rule Set for BSM	
Failover Groups D BSM 6.3.8.0 BSM 0 Default Avaya provided Rule Set for BSM	
BSM 6.3.4.0         BSM         Q         Yes         Avaya provided Rule Set for BSM	
Local Host Name R D SM 6.3.2.0 SM 0 Yes Avaya provided Rule Set for SM	
SM 6.3.8.0 SM 0 Default Avaya provided Rule Set for SM	
Remote Access	

Figure 98: Session Manager – SIP Firewall Configuration - Rules

On Whitelist tab, select New

- In the Key field, select Remote IP Address
- In the Value field, enter internal Avaya SBCE IP address used for Remote Worker (10.10.98.123 as defined in Section 12.1)
- In the Mask field, enter the appropriate mask (e.g., 255.255.255.255)
- **Enabled** box is checked
- Select Commit

AVAYA Aura® System Manager 8.0	Users v 🖌 Elements v 🗢 Services v   Widgets v Shortcuts v	Search	📕   admin
Home Session Manager	Session Manager		
Session Manager ^	Rule Set		Help ?
Session Manager Admi	Edit or view SIP Firewall Rule Set whitelist, blacklist, and rules.  *Name Rule Set for SMVM  Description		
Global Settings	*SM Type SM		
Communication Profile	Rules Blacklist Whitelist		
Network Configuration ^	New Delete		
Failover Groups	Key Value	Mask	
Local Host Name R	Remote IP Address v         10.10.98.123	255.255.255.255	]
Remote Access	Select : All, None		
SIP Firewall			

Figure 99: Session Manager – SIP Firewall Configuration - Whitelist

# 12.9.2. Disable PPM Limiting: Elements $\rightarrow$ Session Manager $\rightarrow$ Session Manager Administration

Select the Session Manager Instance named bvwasm2, and select Edit

Aura® System Manager 8.0	isers 🗸 📕 Elements 🗸 🌣 Services 🗸 🕴 Widge	ts v Shortcuts v	Search 🐥 🗏	∎   admin
Home Session Manager	Session Manager			
Session Manager	Session Manager Administration			Help ?
Dashboard	This page allows you to administer Session Manager instances a their global settings.	and configure		
Session Manager Admi	Session Manager Instances Branch Session Mana	ger Instances		
Global Settings	Session Manager Instances           New         View         Edit         Delete			
Communication Profile				Share Track In
Network Configuration ^	1 Item 📚 Name License Mode Primary Communicatio	n Profiles Secondary Communication Profiles	H Maximum Active Communication Profiles	ilter: Enable Description
Failover Groups	bywasm2     Normal     1	0	1	
Local Host Name R	Select : None			

## Figure 100: Session Manager – Edit Instance

The Session Manager View screen is displayed. Scroll down to the Personal Profile Manager (PPM) – Connection Settings section.

- Uncheck the Limited PPM Client Connection and PPM Packet Rate Limiting options
- Select **Commit** (not shown)

Personal Profile Manager (PPM) - Connection Settings 👻	
Limited PPM Client Connection	
*Maximum Connection per PPM Client 3	
PPM Packet Rate Limiting	
*PPM Packet Rate Limiting Threshold 200	

#### Figure 101: Session Manager – Disable PPM limit

## 12.10. Remote Worker Client Configuration

The following screen illustrates Avaya one- $X^{\otimes}$  Communicator administration settings for the Remote Worker, used in the reference configuration (note that some screen formats may differ from endpoint to endpoint).

## SIP Global Settings Screen

Launch to Avaya one-X<sup>®</sup> Communicator settings and click on Telephony under Accounts. Select Using as SIP Enter Extension and Password Click Add button to add a server into Server List Enter Proxy Server as 10.10.98.34 (see Section 12.1). Set Transport Type: TLS and Port: 5061. Click OK to submit the changes.

Set the **Domain** to **bvwdev.com**.

The other fields are default. Click **OK** to submit the settings.

Avaya one-X® Communicator Login		General Settings					? ×	
Please log In: Extension: 8052 Password: ••••••		Accounts Telephony Login	Telephony Using: O H.323 O SIP					
			Messaging IM and Presence Security	Extension: Password:	8052			
				Server List:				
	ceive calls using Computer ÷		Devices and Services Outgoing Calls					
		Log In	Phone Numbers Dialing Rules			Add	Remove	
			Audio	Domain:	bvwdev.co	m		
			Video	Mode:	Proxied		\$	
			Public Directory Preferences	Avaya Environment: Auto			٥	
			Desktop Integration Hot Keys	Failback Policy:	Auto		\$	
				Registration Policy:	Simultaneo	us	\$	
			Network Advanced	Add Server				
				Proxy Server 10.10.98.34				
				Transport Type TLS + Port 5061				
				Port is optional. If r will be used (TLS=5	061).	the defa	ult	
			Auto-configure			6	DK Ca	incel

Figure 102: Avaya one-X Communicator - Settings

# 13. Appendix B - SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.2.3**.

```
within session "ALL"
  act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
     {
//Manipulate headers
      %HEADERS["From"][1].URI.USER.regex_replace("\+","");
    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\+)","");
      %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
    %HEADERS["Diversion"][1].URI.USER.regex_replace("(\+)","");
// Remove unwanted Headers
      remove(%HEADERS["History-Info"][3]);
      remove(%HEADERS["History-Info"][2]);
      remove(%HEADERS["History-Info"][1]);
 //Modify user of SIP URI in PAI header on Call Forward Off-net
        if (%HEADERS["Diversion"][1].regex match("reason")) then
          %HEADERS["P-Asserted-Identity"][1].URI.USER =
%HEADERS["Diversion"][1].URI.USER;
          }
     }
// act on message where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK"
//
//To remove media description T.38 fax attributes in all SIP messages coming from SFR
//This sigma script is optional for fixing mismatch-codec issue on Avaya one-X Communicator
          remove(%SDP[1]["s"]["m"][2]);
//
//
    }
}
```

#### ©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>®</sup> and <sup>TM</sup> 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 <u>devconnect@avaya.com</u>.