



Application Notes for Pindrop Passport and Protect Solutions with Avaya Session Border Controller for Enterprise and Avaya Aura® Environment – Issue 1.0

Abstract

These Application Notes contain instructions for the Pindrop Passport and Protect solutions with Avaya Session Border Controller for Enterprise and Avaya Aura® environment to successfully interoperate.

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.

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

1. Introduction

These Application Notes contain instructions for the Pindrop Passport and Protect solutions (Pindrop) with Avaya Session Border Controller for Enterprise (Avaya SBCE) and Avaya Aura® environment to successfully interoperate.

Calls between a VoIP Service Provider and an Avaya Aura® environment are generally routed via an Avaya SBCE. Avaya SBCE has the ability to send the media for these calls using a SIPREC interface to Pindrop. Pindrop uses the SIPREC interface provided by an Avaya SBCE to receive SIPREC calls to identify whether the calls are fraudulent based upon the received media. During the compliance test, SIP signaling used TLS and media used SRTP.

2. General Test Approach and Test Results

The feature test cases were performed manually. Necessary user actions were done from the agent telephones to test different call scenarios for inbound and outbound calls from the Avaya Aura® environment.

The serviceability test cases were performed manually by disconnecting/reconnecting the network to Pindrop.

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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Consult the appropriate Avaya and third party documentation for the product

network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

Avaya recommends that 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. 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. Consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Pindrop used encryption capabilities.

2.1. Interoperability Compliance Testing

The interoperability Compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- Inbound calls to Avaya Aura® environment
- Outbound calls to VoIP Service Provider
- Proper transmissions of SIPREC calls to Pindrop
- SIP messaging between Avaya SBCE and Pindrop
- Media transmission to Pindrop
- Calls for scenarios involving internal, external, mute, hold, reconnect, conference, and transfer.

The serviceability testing focused on verifying the ability of Pindrop to recover from adverse conditions, such as disconnecting/reconnecting the network to Pindrop.

Although Pindrop supports TCP/TLS/UDP for SIP Signaling and RTP/SRTP for voice transmission, during the Compliance Testing, SIP signaling used TLS transport and SRTP was used for voice transmission. Note that sips URIs are not supported by Pindrop.

2.2. Test Results

All test cases were successfully executed with the exception of the following:

- By design, SIPREC calls to Pindrop do not include Called Party Number in the SIP signaling. A SigMa script was written during the compliance test to extract the number for an inbound and outbound calls and insert it into a custom SIP header.

2.3. Support

Technical support on Pindrop Passport and Protect solutions can be obtained through the following:

- **Phone:** 1-404-692-2757
- **Email:** www.pindropsecurity.com
- **Web:** support@pindropsecurity.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and Pindrop Passport and Protect solutions. All SIP traffic to and from VoIP service provider to Avaya Aura® environment was routed via Avaya SBCE. For these calls, SIPREC calls were sent to Pindrop. Avaya Aura® environment consisted of the following:

- Avaya Aura® Communication Manager
- Avaya Aura® Media Server
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Experience Portal
- Avaya G450 Gateway
- Avaya J100 and 9600 Series IP (SIP & H.323) Endpoints
- Avaya Digital Endpoints

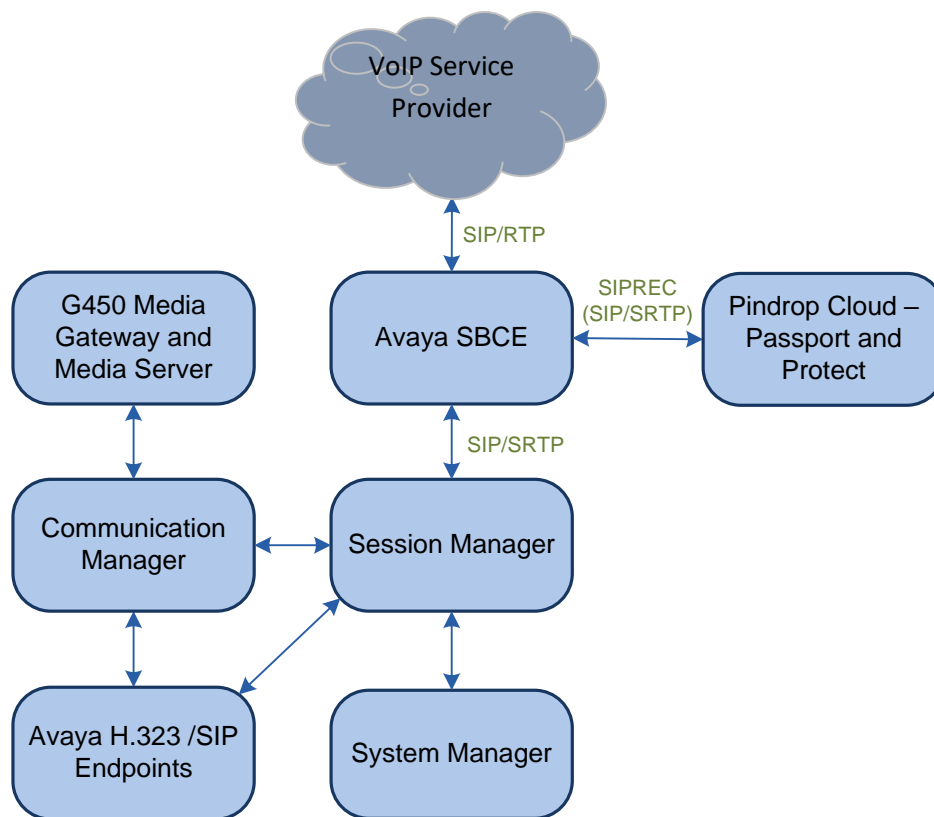


Figure 1: Test Configuration for Pindrop's Passport and Protect and Avaya Aura® Environment.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura [®] Communication Manager	8.1.1
Avaya Aura [®] Session Manager	8.1.1
Avaya Aura [®] System Manager	8.1.1
Avaya 9600 Series IP Deskphones	7.1.7 (SIP)
Avaya 9600 Series IP Deskphones	6.8.3 (H.323)
Avaya J100 Series IP Deskphones	6.8.3 (H.323)
Avaya J100 Series IP Deskphones	4.0.3 (SIP)
Avaya G450 Media Gateway	41.9.0
Avaya Aura [®] Experience Portal	7.2.3
Avaya Aura [®] Media Server	8.0.2
Avaya Session Border Controller for Enterprise	8.0.1.0-10-17555
Pindrop's Passport and Protect	April 2020 Cloud Platform

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure Pindrop successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Verify Avaya Aura® Communication Manager License

Enter the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an Avaya representative to make the appropriate changes.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	2400	1
Maximum Administered Remote Office Trunks:	12000	0
Max Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	36000	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	12000	10
Max Administered Ad-hoc Video Conferencing Ports:	12000	0
Max Number of DS1 Boards with Echo Cancellation:	688	0

5.2. Configure IP Node Names

All calls from and to Communication Manager are signalled over a SIP trunk to Session Manager. The signalling interface on Session Manager is provided by the SM100 security module. Use the **change node-names ip** command to add the **Name** and **IP Address** for the SIP security module of Session Manager. **sm81** and **10.64.110.212** was used in this example.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
aes81	10.64.110.215	
ams81	10.64.110.214	
cms19	10.64.110.225	
default	0.0.0.0	
procr	10.64.110.213	
procr6	::	
sm81	10.64.110.212	

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command to specify **G.711MU** and **G.729** codecs under **Audio Codec** where **n** is the codec set used in the configuration. Configure the **Media Encryption** and **Encrypted SRTCP** as shown below.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size (ms)
1: G.711MU      n          2          20
2: G.729      n          2          20
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
5:
```

5.4. Configure IP network Region

Use the **change ip-network-region n** command where **n** is the number of the network region used. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **yes**. For **Codec Set**, enter the codec set configured in **Section 5.3**. Set the **Authoritative Domain** to **avaya.com**. Retain the default values for the remaining fields.

```
change ip-network-region 1                               Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location:      Authoritative Domain: avaya.com
Name:          Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048      IP Audio Hairpinning? y
UDP Port Max: 3329
```


5.5. Configure SIP Trunk with Avaya Aura® Session Manager

To administer a SIP Trunk on Communication Manager, two intermediate steps are required, creation of a signaling group and trunk group.

5.5.1. Add Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** **sip**
- **Transport Method:** **tls**
- **Near-end Node Name:** **procr**
- **Far-end Node Name:** Session Manager node name from **Section 5.2**
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Network Region:** IP Network Region from **Section 5.4**
- **Far-end Domain:** **avaya.com**
- **DTMF over IP:** **rtp-payload (RFC2833)**
- **Direct IP-IP Audio Connections** **y**
- **IP Audio Hairpinning** **y**
- **Initial IP-IP Direct Media** **y**

```
add signaling-group 1                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? n                        Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM                Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n

Near-end Node Name: procr              Far-end Node Name: sml
Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                      Far-end Network Region: 1
                                      Far-end Secondary Node Name:

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
                                      RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3    IP Audio Hairpinning? y
Enable Layer 3 Test? y                Initial IP-IP Direct Media? y
```

5.5.2. Add SIP Trunk Group

Add the corresponding trunk group controlled by the above signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name (e.g. **SM Trunk**)
- **TAC:** An available trunk access code (e.g. **101**)
- **Service Type:** tie
- **Signaling Group:** Number of the signaling group added in **Section 5.5.1** (i.e. 1)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from licensed verified in **Section 5.1**)

```
add trunk-group 1                                     Page 1 of 5
TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
Group Name: SM Trunk                                COR: 1                 TN: 1             TAC: 101
Direction: two-way                                Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                  Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 1
                                                Number of Members: 10
```

Navigate to **Page 3** and change **Numbering Format** to **private**. Use default values for all other fields.

```
add trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n                                Measured: none
                                                Maintenance Tests? y
Numbering Format: private
                                                UI Treatment: shared
Maximum Size of UII Contents: 128
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
                                                Hold/Unhold Notifications? y
Modify Tandem Calling Number: no
```

5.6. Configure Route Patterns

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

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

5.7. Configure Private Numbering

Use the **change private-numbering 0** command to assign number presented by Communication Manager for calls leaving for Session Manager. Add an entry for the Extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields.

- **Ext Len:** Number of digits of the Extension i.e. **5**
- **Ext. Code:** Leading digits of the Extension number, i.e. **7**
- **Trk Group:** Leave it blank (meaning any trunk)
- **Private Prefix:** Enter a value a desired value or leave blank
- **Total CPN Len** Total number of digits i.e. **5**

Note that the value entered in **Private Prefix** will replace the agent's extensions value for outbound calls.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	5			5	Total Administered: 2	
5	7		12015551212	11	Maximum Entries: 540	

5.8. Configure ARS Analysis

This section shows a sample Auto Route Selection (ARS) entry used for routing calls with dialed digits beginning with **1555**. Use the **change ars analysis 1555** command to add an entry and specify routing of the calls to Session Manager. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **1555**
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e. **1**
- **Call Type:** **hnpa**

Note that additional entries may be added for different number destinations.

change ars analysis 1555							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
1555	11	11	1	hnpa		n	

5.9. Configure Feature Access Code

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS)**. In the test, **9** was used.

change feature-access-codes		Page 1 of 11
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

6. Configure Avaya Aura® Session Manager

All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL. A SIP trunk and routing needs to be configured for Communication Manager and Avaya SBCE.

6.1. Configure SIP Entities

Add two new SIP entities, one for Communication Manager and another one for Avaya SBCE

6.1.1. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Pindrop.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The procr address of Communication Manager.
- **Type:** “CM”
- **Location:** Select a preconfigured Location.
- **Time Zone:** Select the applicable time zone.

SIP Entity Details Commit Cancel Help ?

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

* **SIP Timer B/F (in seconds):**

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “sm81”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** “5061”
- **Connection Policy:** “trusted”

Entity Links

Override Port & Transport with DNS SRV: ☐

Add
Remove

1 Item
Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* sm81_cm81_5061_TLS	sm81	TLS	* 5061	cm81	* 5061	trusted

Select : All, None

SIP Responses to an OPTIONS Request

Add
Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit
Cancel

6.1.2. SIP Entity for Avaya SBCE

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya SBCE.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The internal SIP IP address of Avaya SBCE.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the 'SIP Entity Details' form in a web application. The left sidebar has 'Routing' selected, and 'SIP Entities' is highlighted. The form is titled 'SIP Entity Details' and has a 'General' tab. The form fields are:

- Name:** sbce81
- FQDN or IP Address:** 10.64.110.222
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** sbce81
- Location:** DevConnect
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4

There are 'Commit' and 'Cancel' buttons at the top right of the form.

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “sm81”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Avaya SBCE entity name from this section.
- **Port:** “5061”
- **Connection Policy:** “trusted”

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* sm81_sbce81_5061_TLS	sm81	TLS	* 5061	sbce81	* 5061	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

6.2. Configure Routing Policies

Add a new routing policy for routing calls to Communication Manager and Avaya SBCE.

6.2.1. Routing Policy for Communication Manager

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.1.1**.

Routing Policy Details

[Help ?](#)

CommitCancel

General

* Name:

cm81

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	CM	

6.2.2. Routing Policy for Avaya SBCE

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Avaya SBCE entity name from **Section 6.1.2**.

Routing Policy DetailsCommitCancelHelp ?

General

* Name:

sbce81

Disabled: ☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sbce81	10.64.110.222	SIP Trunk	

6.3. Configure Dial Patterns

Dial patterns needs to be configured for Session Manager to know where to route the calls.

6.3.1. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous **Section 6.2.1** (not shown). The configuration below shows calls to **1444xxxxxxx** were routed to Communication Manager.

Dial Pattern Details

[Help ?](#)

Commit

Cancel

General

* Pattern: 1444

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		cm81	0	<input type="checkbox"/>	cm81	

Select : All, None

6.3.2. Dial Pattern for Avaya SBCE

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Policies** created in previous **Section 6.2.2** (not shown). The configuration below shows calls to **1555xxxxxxx** were routed to Avaya SBCE.

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern:1555

* Min:11

* Max:11

Emergency Call:☐

SIP Domain:-ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 ItemFilter: Enable

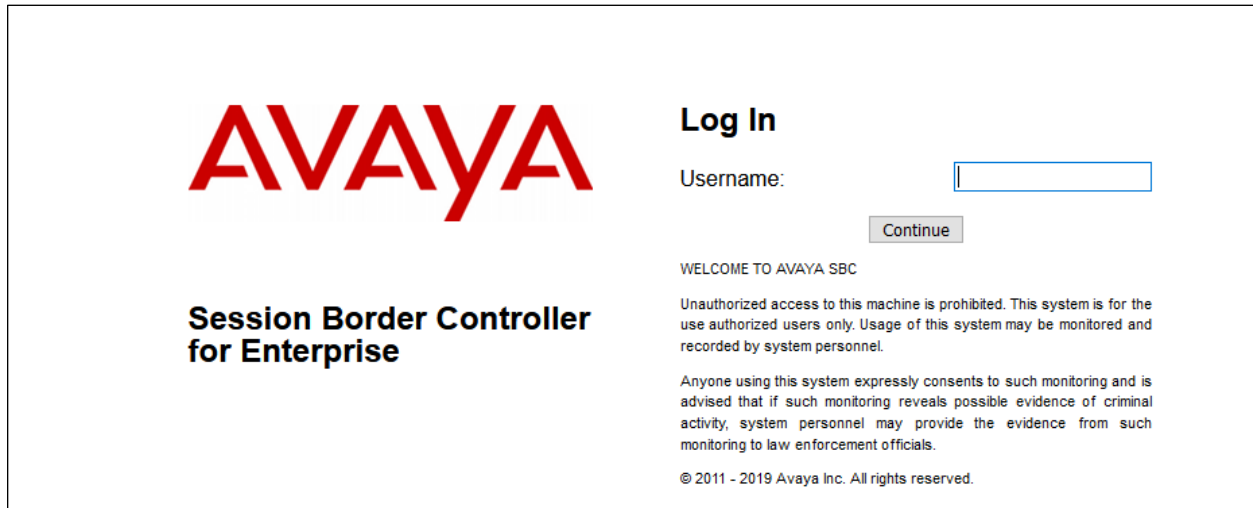
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect		sbce81	2	<input type="checkbox"/>	sbce81	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides SIP connectivity to VoIP Service Provider, Session Manager and a SIPREC server (Pindrop).

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The image shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, there is a "Log In" section. It includes a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access and monitoring, a consent statement, and a copyright notice: "© 2011 - 2019 Avaya Inc. All rights reserved."

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.

Device: sbce801 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS Dashboard

Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Dashboard

Information

System Time	03:14:48 PM MST	Refresh
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	12/19/2019 12:13:52 MST	
Failed Login Attempts	0	

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS

sbce801

Incidents (past 24 hours)

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

7.1. Define Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult References section for more information on this topic.

SigMa scripts were used to modify the following:

- Insert siprec-srs in the Request URI user part for INVITE and UPDATE to Pindrop
- Extract To header user part from incoming and outgoing INVITES and insert into a custom **x-To** header, which will be sent in the SIPREC calls to Pindrop.

7.1.1. Signaling Manipulation for Pindrop

To add a Signaling Manipulation rule, select **Configuration Profiles → Signaling Manipulation** from the left-hand menu. Add a new Signaling Manipulations Script and provide a name (not shown). Copy the script from **Appendix A** and insert.

Signaling Manipulation Scripts: siprec-srs

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

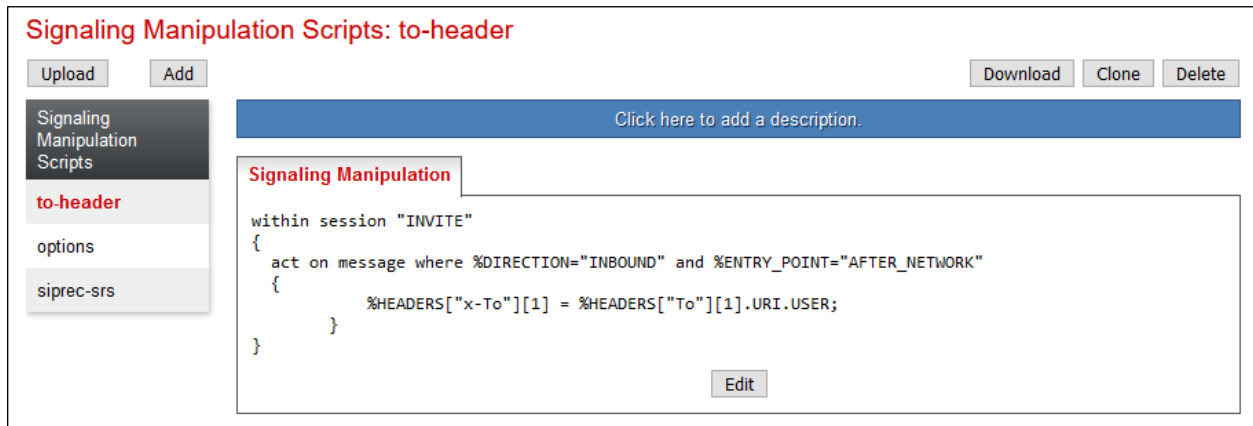
```
within session "ALL"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="INVITE"
    {
        %HEADERS["Request_Line"][1].URI.USER="siprec-srs";
    }

    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
    {
        %HEADERS["Request_Line"][1].URI.USER="siprec-srs";
    }
}
```

Edit

7.1.2. Signaling Manipulation for VoIP Service Provider and Session Manager

The following SigMa script was used to extract the Called Party Number for inbound and outbound calls.



Signaling Manipulation Scripts: to-header

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

```
within session "INVITE"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    {
      %HEADERS["x-To"][1] = %HEADERS["To"][1].URI.USER;
    }
  }
}
```

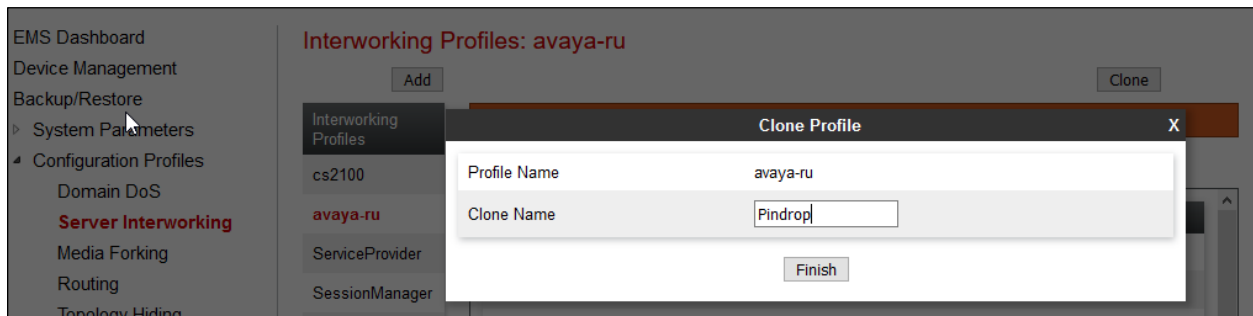
Edit

7.2. Define Server Interworking

An interworking profile is needed for supported SIP functionality for a SIP server. During Compliance Testing, a pre-configured profile was used for Session Manager and VoIP Service Provider, but the screen captures for those are shown in this section. Add Interworking profile for VoIP Service Provider, Pindrop and Session Manager.

7.2.1. Server Interworking profile for Pindrop

To add a Server Interworking profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. Screen captures for the profile are shown below. Select the **avaya-ru** profile and select **Clone**. Type in a **Clone Name** for Pindrop profile. Select **Finish** once done.



EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Interworking Profiles: avaya-ru

Add Clone

Interworking Profiles

cs2100

avaya-ru

ServiceProvider

SessionManager

Clone Profile

Profile Name avaya-ru

Clone Name Pindrop

Finish

7.2.2. Server Interworking profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. No changes were made to the cloned profile.

7.2.3. Server Interworking profile for VoIP Service Provider

VoIP Service Provider profile was also cloned from the same **avaya-ru** profile. No changes were made to the cloned profile.

7.3. Define SIP Servers

A SIP server definition is required for each server connected to the Avaya SBCE. Add SIP Servers for VoIP Service Provider, Pindrop and Session Manager.

7.3.1. SIP Server for Pindrop

To define a server, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up screen (not shown) and select **Next**. Note that for security purposes, Public IP Addresses have been changed to Private.

- **Server Type:** **Recording Server**
- **TLS Client Profile:** Select a TLS profile for authentication
- **IP Address / FQDN** SIP IP Address of Pindrop node
- **Port:** SIP Port of Pindrop node
- **Transport:** **TLS**

Note that TLS profiles were preconfigured and are not shown in this document. All TLS certificates used during the test were signed by System Manager.

The screenshot shows the 'Edit SIP Server Profile - General' dialog box. At the top, a blue banner states: 'Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.' The form contains the following fields:

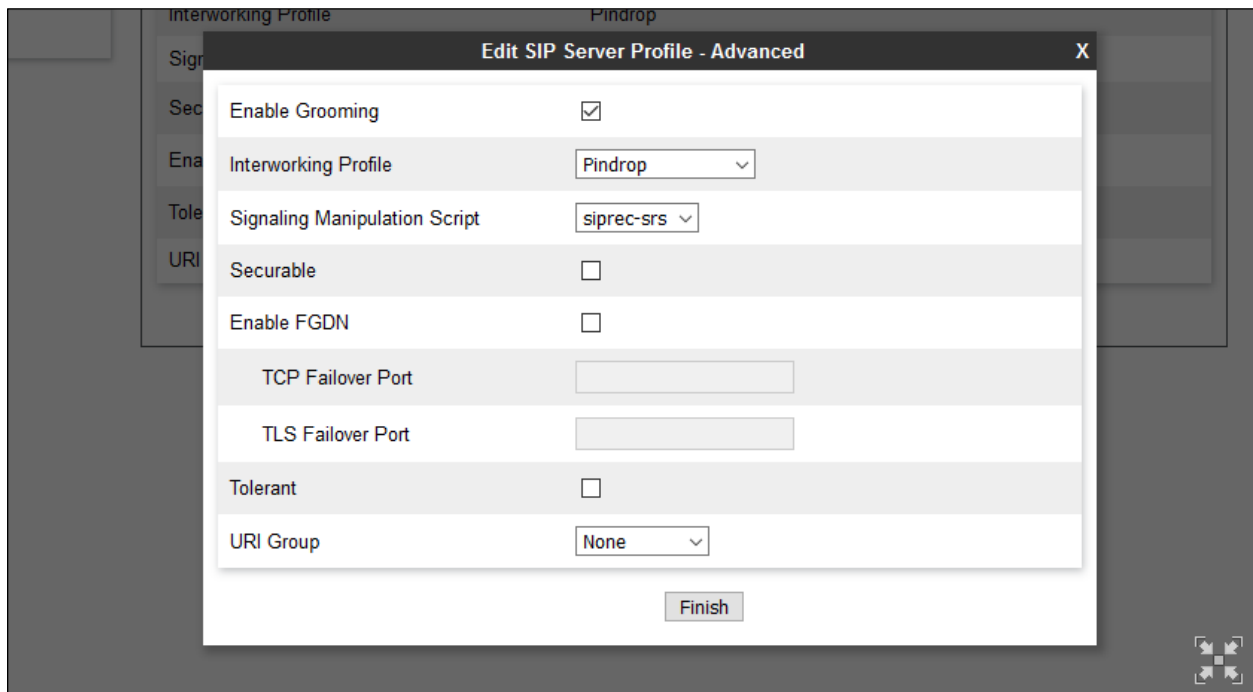
- Server Type:** Recording Server (dropdown)
- SIP Domain:** (empty text box)
- DNS Query Type:** NONE/A (dropdown)
- TLS Client Profile:** ClientTLS (dropdown)

Below these fields is an 'Add' button. At the bottom, there is a table with three columns: 'IP Address / FQDN', 'Port', and 'Transport'.

IP Address / FQDN	Port	Transport
10.64.101.207	5060	TLS

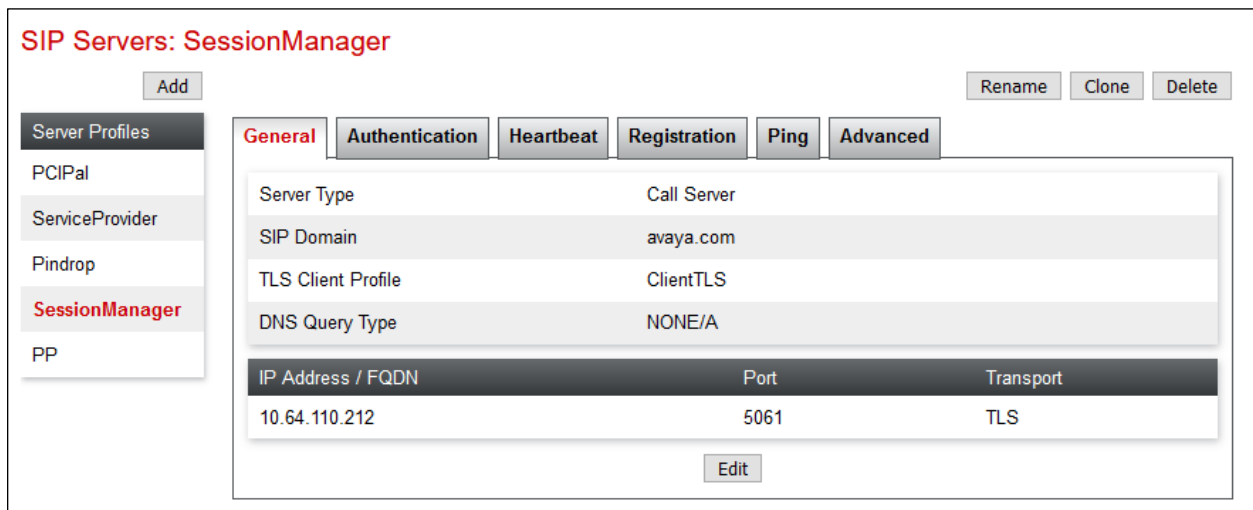
There is a 'Delete' link next to the table row and a 'Finish' button at the bottom center. In the background, the 'SIP Servers: Pindrop' page is visible with an 'Add' button and a sidebar menu containing 'Server Profiles', 'SessionManager', 'ServiceProvider', and 'Pindrop'.

Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for Pindrop from **Section 7.2.1** and select the **Signaling Manipulation Script** from **Section 7.1.1**, select **Finish**.



7.3.2. SIP Server for Session Manager

Session Manager SIP Server was preconfigured. The screen capture below shows the **General** tab:



All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile and Signaling Manipulation Script from **Section 7.2.2.** and **Section 7.1.2** was configured.

SIP Servers: SessionManager

Buttons: Add, Rename, Clone, Delete

Server Profiles: SessionManager, ServiceProvider, Pindrop

Tabs: General, Authentication, Heartbeat, Registration, Ping, **Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SessionManager
Signaling Manipulation Script	to-header
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None

Edit

7.3.3. SIP Server for VoIP Service Provider

VoIP Service Provider SIP Server was preconfigured. The screen capture below shows the **General** tab:

SIP Servers: ServiceProvider

Buttons: Add, Rename, Clone, Delete

Server Profiles: PCIPal, **ServiceProvider**, Pindrop, SessionManager, PP

Tabs: **General**, Authentication, Heartbeat, Registration, Ping, Advanced

Server Type	Trunk Server	
SIP Domain	avaya.com	
DNS Query Type	NONE/A	

IP Address / FQDN	Port	Transport
10.64.110.65	5060	UDP

Edit

All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile and Signaling Manipulation Script from **Section 7.2.3.** and **Section 7.1.2** was configured.

SIP Servers: ServiceProvider

Add

RenameCloneDelete

Server Profiles

SessionManager

ServiceProvider

Pindrop

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☐

Interworking ProfileServiceProvider

Signaling Manipulation Scriptto-header

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

Edit

7.4. Define Routing

Routing information is required for routing calls to all configured SIP Servers. The IP addresses and ports defined here will be used as the destination addresses for signalling.

7.4.1. Routing Profile for Pindrop

To define the Routing profile for Pindrop, navigate to **Configuration Profiles → Routing** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown). Pindrop **SIP Server Profile** was configured as shown below:

URI Group	Time of Day	Load Balancing	NAPTR	Transport	LDAP Server Profile	LDAP Base DN (Search)	Matched Attribute Priority	Alternate Routing	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	<input type="checkbox"/>	None	None	None	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Pindrop	10.64.101.207:5060 (UC)	None

7.4.2. Routing Profile for Session Manager

Routing Profile for Session Manager was preconfigured. Screen capture below shows the configured Routing Profile for Session Manager.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.64.110.212:5061	TLS

7.4.3. Routing Profile for VoIP Service Provider

Routing Profile for VoIP Service Provider was preconfigured. Screen capture below shows the configured Routing Profile for VoIP Service Provider.

Routing Profiles: ServiceProvider

Add

Rename

Clone

Delete

Routing Profiles

default

ServiceProvider

SessionManager

Pindrop

PCIPal

Click here to add a description.

Routing Profile

Update Priority

Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.64.110.65:5060	UDP	<div>EditDelete</div>

7.5. Define Media Rules

Media rules are used to define RTP 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. Note that during Compliance Testing calls to all the SIP Servers used the same Media Rules.

7.5.1. Media Rule for Pindrop

To define a new Media Rule, navigate to **Domain Policies → Media Rules**. Clone **default-low-med** rule and provide a **Clone Name** for the new Media Rule (not shown). Once added, select the newly added **Media Rule** and Edit the **Encryption** tab, configure as shown in the screen capture below:

Media Rules: Pindrop

Add Rename Clone Delete

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- Pindrop**
- RTP-SRTP

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

Audio Encryption

Preferred Formats	SRTP_AES_256_CM_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_32
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

7.5.2. Media Rule for VoIP Service Provider and Session Manager

Following screen capture displays the Media Rule used by VoIP Service Provider and Session Manager.

The screenshot shows the 'Media Rules: RTP-SRTP' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'Pindrop', and 'RTP-SRTP' (which is highlighted in red). Above the list is an 'Add' button. To the right of the sidebar is a main configuration area. At the top of this area is a blue bar with the text 'Click here to add a description.' Below this bar are four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab contains two sections: 'Audio Encryption' and 'Video Encryption'. The 'Audio Encryption' section has the following settings: 'Preferred Formats' (SRTP_AES_CM_128_HMAC_SHA1_32, SRTP_AES_CM_128_HMAC_SHA1_80, RTP), 'SRTP Context Reset on SSRC Change' (checkbox), 'Encrypted RTCP' (checkbox), 'MKI' (checkbox), 'Lifetime' (Any), and 'Interworking' (checkbox checked). The 'Video Encryption' section has 'Preferred Formats' (RTP) and 'Interworking' (checkbox checked). Below these sections is a 'Miscellaneous' section with 'Capability Negotiation' (checkbox). At the bottom right of the configuration area is an 'Edit' button.

Select the **Codec Prioritization** tab and **Edit**. Configure as shown in the screen capture below:

The screenshot shows the 'Media Rules: RTP-SRTP' configuration page, now with the 'Codec Prioritization' tab selected. The sidebar on the left is identical to the previous screenshot. The main configuration area has the 'Codec Prioritization' tab selected, showing 'Audio Codec' and 'Video Codec' sections. The 'Audio Codec' section has the following settings: 'Codec Prioritization' (checkbox checked), 'Allow Preferred Codecs Only' (checkbox), 'Transcode When Needed' (checkbox checked), 'Transrating' (checkbox), and 'Preferred Codecs' (PCMU (0) [T], telephone-event [D], G729 (18) [T]). The 'Video Codec' section has 'Codec Prioritization' (checkbox). At the bottom right of the configuration area is an 'Edit' button.

7.6. Define Signaling Rules

With Signaling Rules, definition of the action to be taken for each type of SIP-specific signaling request and response message can be specified. Actions that can be configured with Signaling Rules include Allow, Block, and Block with Response. When SIP signaling packets are received by the Avaya SBCE, the packets are parsed and pattern-matched against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

7.6.1. Define Signaling Rules for Pindrop

To add a Signaling Rule, navigate to **Domain Policies** → **Signaling Rules**. Clone **default** rule and provide a **Clone Name** for the new Signaling Rule (not shown). Once added, **Edit** the **UCID** tab and enable **UCID**.

Signaling Rules: Pindrop

Buttons: Add, Rename, Clone, Delete

Signaling Rules list: default, No-Content-Type..., INFOAllow, **Pindrop**

Configuration Panel (UCID tab active):

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
Click here to add a description.						
UCID <input checked="" type="checkbox"/>						
Node ID 4						
Protocol Discriminator 0x00						
<button>Edit</button>						

7.6.2. Define Signaling Rules for VoIP Service Provider and Session Manager

For VoIP Server Provider and Session Manager, **default** Signaling Rule were used.

7.7. Define Endpoint Policy Groups

Endpoint policy groups comprise a group of endpoint policy sets, all of which are specifically configured using a number of relevant parameters. Recently added Media Rule is associated with an Endpoint Policy Group.

7.7.1. Endpoint Policy Group for Pindrop

To add an Endpoint Policy Group, navigate to **Domain Policies → Endpoint Policy Groups**. Clone **default-low** group and provide a **Clone Name** for the new Endpoint Policy Group (not shown). Once added, **Edit** the newly cloned group and set the **Media Rule** to the Media Rule added in **Section 7.5.1** and **Signaling Rule** from **Section 7.6.1**. Select **Finish** once done.

The screenshot shows a web-based configuration interface with a sidebar on the left listing policy sets: default-med-enc, default-high, default-high, avaya-def-h, avaya-def-h, avaya-def-h, Pindrop (highlighted in red), and RTP-SRTP. A modal window titled 'Edit Policy Set' is open, displaying the following configuration:

Rule Type	Value
Application Rule	default
Border Rule	default
Media Rule	Pindrop
Security Rule	default-low
Signaling Rule	Pindrop
Charging Rule	None
RTCP Monitoring Report Generation	Off

A 'Finish' button is located at the bottom center of the modal. An 'Edit' button is visible in the background on the right side of the modal.

7.7.2. Endpoint Policy Group for VoIP Service Provider and Session Manager

Following screen capture displays the End Point Policy Group used by VoIP Service Provider and Session Manager.

Policy Groups: RTP-SRTP

Add

RenameCloneDelete

Policy Groups

default-lowdefault-low-encdefault-meddefault-med-encdefault-highdefault-high-encavaya-def-low...avaya-def-hig

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	RTP-SRTP	default-low	default	None	Off	Edit

7.8. Define Session Policy

A Session Policy needs to be defined for Pindrop. Navigate to **Domain Policies** → **Session Policies** and add a new Session Policy for Pindrop. The screen capture below shows the Session Policy configured during the Compliance test. Note that the configured **Routing Profile** was for Pindrop from **Section 7.4.1**

Session Policies: Pindrop

Add

RenameCloneDelete

Session Policies

default

MediaNoAnchor

Pindrop

Click here to add a description.

Media

Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input checked="" type="checkbox"/>
Recording Type	Full Time
Play Recording Tone	<input type="checkbox"/>
Call Termination on Recording Failure	<input type="checkbox"/>
Routing Profile	Pindrop
Video Recording	<input type="checkbox"/>
Media Server	<input type="checkbox"/>

Edit

7.9. Signaling Interface

Signaling Interface needs to be defined for each SIP Server and SIP Remote Workers for SIP signaling. Navigate to **Networks & Flows → Signaling Interface** to define a new Signaling Interface. During the Compliance Testing the following interfaces were defined. For security reasons, Public IP Addresses have been blacked out.

- SP: Signaling interface used by Service Provider to send and receive calls.
- Internal: Signaling interface used by Session Manager to send and receive calls.
- RW-Internal: Signaling interface used for SIP Remote Workers registrations and to send and receive calls towards Session Manager.
- RW-External: Signaling interface used for SIP Remote Workers registrations and to send and receive calls towards the internet.
- External: Signaling interface used by Avaya SBCE to send calls to Pindrop.

Signaling Interface							
Signaling Interface							
Add							
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
SP	10.64.110.223 SP (A2, VLAN 0)	5060	5060	---	None	Edit	Delete
Internal	10.64.110.222 Internal (A1, VLAN 0)	5060	5060	5061	ServerTLS	Edit	Delete
RW-Internal	10.64.110.220 Internal (A1, VLAN 0)	5060	5060	5061	ServerTLS	Edit	Delete
RW-External	██████████ External (B1, VLAN 0)	5060	5060	5061	ServerTLS	Edit	Delete
External	██████████ External (B1, VLAN 0)	5060	5060	5061	ServerTLS	Edit	Delete

7.10. Media Interface

Media Interface needs to be defined for each SIP Server and SIP Remote Workers to send and receive media (RTP or SRTP). Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined. For security reasons, Public IP Addresses have been blacked out.

- Internal: Interface used by Session Manager to send and receive media.
- SP: Interface used by Service Provider to send and receive media.
- RW-Internal: Interface used for SIP Remote Workers to send and receive media towards Session Manager.
- RW-External: Interface used for SIP Remote Workers to send and receive media towards the internet.
- External: Interface used by Avaya SBCE to send media to Pindrop.

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range		
Internal	10.64.110.222 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
SP	10.64.110.223 SP (A2, VLAN 0)	35000 - 40000	Edit	Delete
RW-Internal	10.64.110.220 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
RW-External	██████████ External (B1, VLAN 0)	35000 - 40000	Edit	Delete
External	██████████ External (B1, VLAN 0)	35000 - 40000	Edit	Delete

7.11. Server Flows

Server Flows combine the previously defined profiles for Pindrop/Session Manager and VoIP Service Provider. These End Point Server Flows allow calls to be routed to and from Pindrop/Session Manager/VoIP Service Provider. Navigate to **Network & Flows → End Point Flows → Server Flows**. The screen capture below displays the configured Server Flows. The screen capture below displays the Server flows used during the Compliance test.

End Point Flows

Subscriber Flows

Server Flows

SIP Server: Pindrop

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	PindropExternal	*	SP	External	Pindrop	default	View Clone Edit Delete
2	PindropInternal	*	Internal	External	Pindrop	default	View Clone Edit Delete
3	PindropRW	*	RW-Internal	External	Pindrop	default	View Clone Edit Delete

SIP Server: ServiceProvider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Outbound	*	Internal	SP	default-low	SessionManager	View Clone Edit Delete

SIP Server: SessionManager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	RWFlow	*	RW-External	RW-Internal	RTP-SRTP	default	View Clone Edit Delete
2	Inbound	*	SP	Internal	default-low	ServiceProvider	View Clone Edit Delete

7.12. Define Session Flow

A Session Flow needs to be defined for Pindrop. Navigate to **Network & Flows → Session Flows** and add a new Session Flow for Pindrop. The following Session Flow was configured during the Compliance test. Note that the configured **Session Policy** for Pindrop from **Section 7.8**.

Session Flows

Add

Modifications made to a Session Flow will only take effect on new sessions.

Hover over a row to see its description.

Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy	
1	Pindrop	*	*	*	*	Pindrop	Clone Edit Delete

8. Configure Advanced Options

Pindrop does not support SIPS URIs. In order for Avaya SBCE to disable SIPS URIs for SIP Servers configured with SRTP, AS-SIP mode needs to be enabled. When AS-SIP Mode is enabled Avaya SBCE supports SRTP over SIP towards the SIP trunks or call servers. Avaya SBCE converts the SIPS URIs to SIP URIs towards the SIP trunks or call servers. Navigate to **Network & Flows → Advanced Options → SIP Options** and enable **AS-SIP Mode** as shown below.

Advanced Options

Periodic Statistics

Feature Control

SIP Options

Network Options

Port Ranges

RTCP Monitoring

Load

Monitoring

Advanced SIP Options

DNS Caching

☒ Enabled

AS-SIP Mode

☒ Enabled

Only plain type URIs will be processed from the E911 group. Dial plan and regular expression type URIs are not supported here and will be ignored.

E911 Options

E911 URI Group

Emergency ▾

Maximum Concurrent Sessions

0

Leave as zero for unlimited

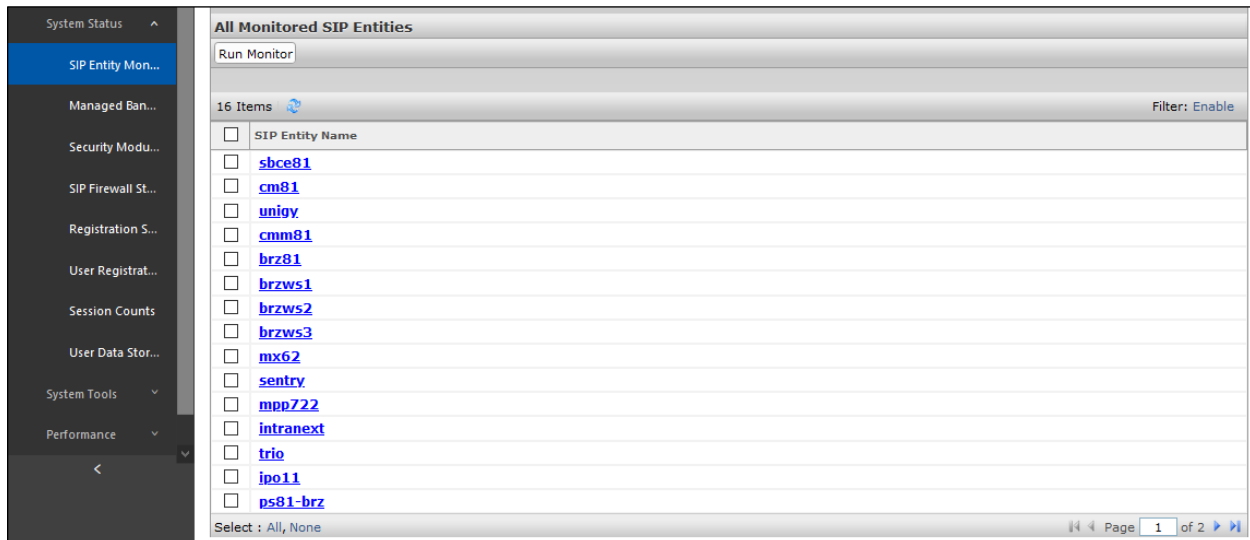
Save

9. Configure Pindrop's Passport and Protect Solutions

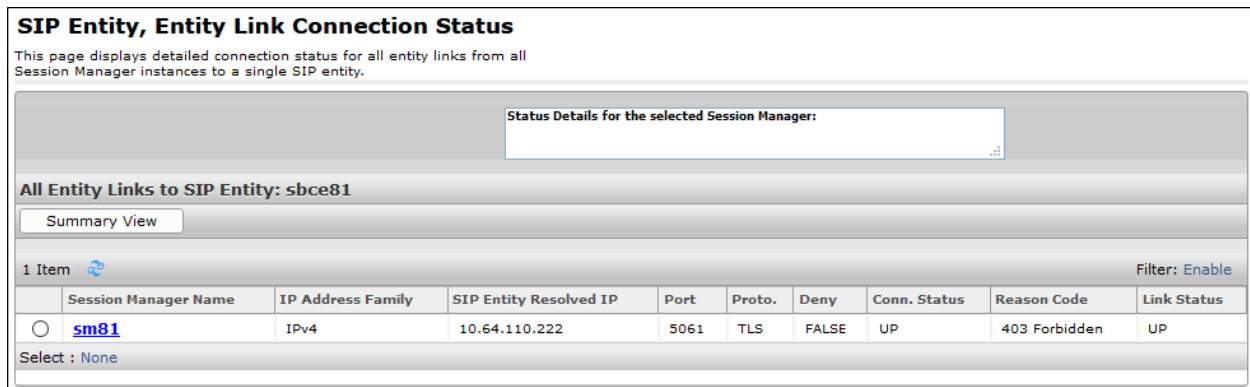
All configuration related to Pindrop is performed by Pindrop engineers and, thus, is not documented.

10. Verification Steps

To verify SIP connectivity to Avaya SBCE, via System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. Under the **All Monitored SIP Entities**, select the Avaya SBCE Entity.



Verify **Conn. Status** is **UP**.



Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
sm81	IPv4	10.64.110.222	5061	TLS	FALSE	UP	403 Forbidden	UP

Additionally, calls can be placed between VoIP Service Provider and Session Manager to verify SIPREC calls to Pindrop. The utility, `tracesbc`, can be run on Avaya SBCE to verify SIP messaging.

11. Conclusion

Pindrop Passport and Protect solutions were able to successfully interoperate with Avaya Aura® environment and Avaya Session Border Controller for Enterprise with the exception of the observation in **Section 2.2**.

12. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

[1] Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 5, November 2019.

[2] Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019.

[3] Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019

[4] Administering Avaya Session Border Controller for Enterprise, Release 8.0.x, Issue 4, August 2019.

Documentation related to Pindrop products can directly be obtained from Pindrop.

[5] Protect User Guide

[6] Passport User Guide

[7] Passport + Protect User Guide

13. Appendix A

SigMa script for Pindrop

```
within session "ALL"
{

    act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING" and %METHOD="INVITE"
    {
        %HEADERS["Request_Line"][1].URI.USER="siprec-srs";
    }

    act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING" and %METHOD="UPDATE"
    {
        %HEADERS["Request_Line"][1].URI.USER="siprec-srs";
    }
}
```

SigMa script for VoIP Service Provider and Session Manager

```
within session "INVITE"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
        %HEADERS["x-To"][1] = %HEADERS["To"][1].URI.USER;
    }
}
```

©2020 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.