



Avaya Solution & Interoperability Test Lab

Application Notes for VBrick Distributed Media Engine with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the steps required to integrate the VBrick Distributed Media Engine with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface.

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

1. Introduction

These Application Notes describe the steps required to integrate the VBrick Distributed Media Engine with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using a SIP interface.

The VBrick H.264 Distributed Media Engine (DME) simplifies delivery of high-definition video and other rich media content across multi-site enterprises and campus environments. The Distributed Media Engine, deployed centrally or at the network edge, is a single integrated platform that provides media redistribution, media transformation as well as video-on-demand content serving and storage.

The DME can deliver an optional Video Conference Streaming Gateway Module, enabling the DME to ingest video from popular videoconference systems and convert it for streaming. Each unit can support hundreds or thousands of users, concurrently delivering multiple streams of live and stored video content in a variety of formats. The DME's Video Conferencing Streaming Gateway Module can be invited into a video call by an individual video conference camera & codec or a multipoint control unit (MCU). Conversely, the Gateway Module can initiate a call into a conference. The DME ingests the video from the video conference system, converts the formats for streaming and delivers it across the VBrick ecosystem.

2. General Test Approach and Test Results

This goal of interoperability test plan was to test the ability of the VBrick Distributed Media Engine to interoperate with an Avaya telephony infrastructure. The Avaya components consisted of the following:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya video endpoints
 - Avaya Desktop Video Device (SIP)
 - Avaya one-X® Communicator (H.323)
 - Avaya one-X® Communicator (SIP)
 - Avaya 1010/1020 Video Conferencing System (SIP)
 - Avaya 1030/1040/1050 Video Conferencing System (SIP)

Compliance testing focused on point-to-point video calls and between the Avaya video endpoints and the VBrick DME, and live streaming of those calls. MCU video call scenarios were not tested.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by

DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of VBrick Distributed Media Engine with Session Manager.
- Video calls between VBrick Distributed Media Engine and Avaya one-X® Communicator (SIP and H.323 versions), the Avaya Desktop Video Device, and Avaya 1020 and 1050 Video Conference Systems.
- Voice calls between VBrick Distributed Media Engine and Avaya one-X® Communicator (SIP and H.323 versions), the Avaya Desktop Video Device, and Avaya 1020 and 1050 Video Conference Systems.
- G.711 and G.729 codec support.
- Caller ID display on.
- Audio mute on VBrick DME and Avaya endpoints for video and voice calls.
- Video mute from Avaya endpoints to VBrick DME.
- Proper system recovery after a restart of the VBrick DME and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following exception/observation:

- Video calls failed between Avaya one-X Communicator (H.323) and the VBrick DME. This issue has been identified within the VBrick DME and the fix will be in the upcoming release of the DME.

2.3 Support

For technical support on the VBrick Distributed Media Engine, contact VBrick Support via phone or website.

- **Phone:** (866) 827-4251
- **Web:** <http://www.vbrick.com/support/index.asp>

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Avaya Aura® Communication Manager running on an Avaya S8300D Server with a G450 Media Gateway.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager (used to configure Session Manager).
- Avaya video endpoints
 - Avaya Desktop Video Device (SIP)
 - Avaya one-X® Communicator (H.323)
 - Avaya one-X® Communicator (SIP)
 - Avaya 1010/1020 Video Conferencing System (SIP)
 - Avaya 1030/1040/1050 Video Conferencing System (SIP)

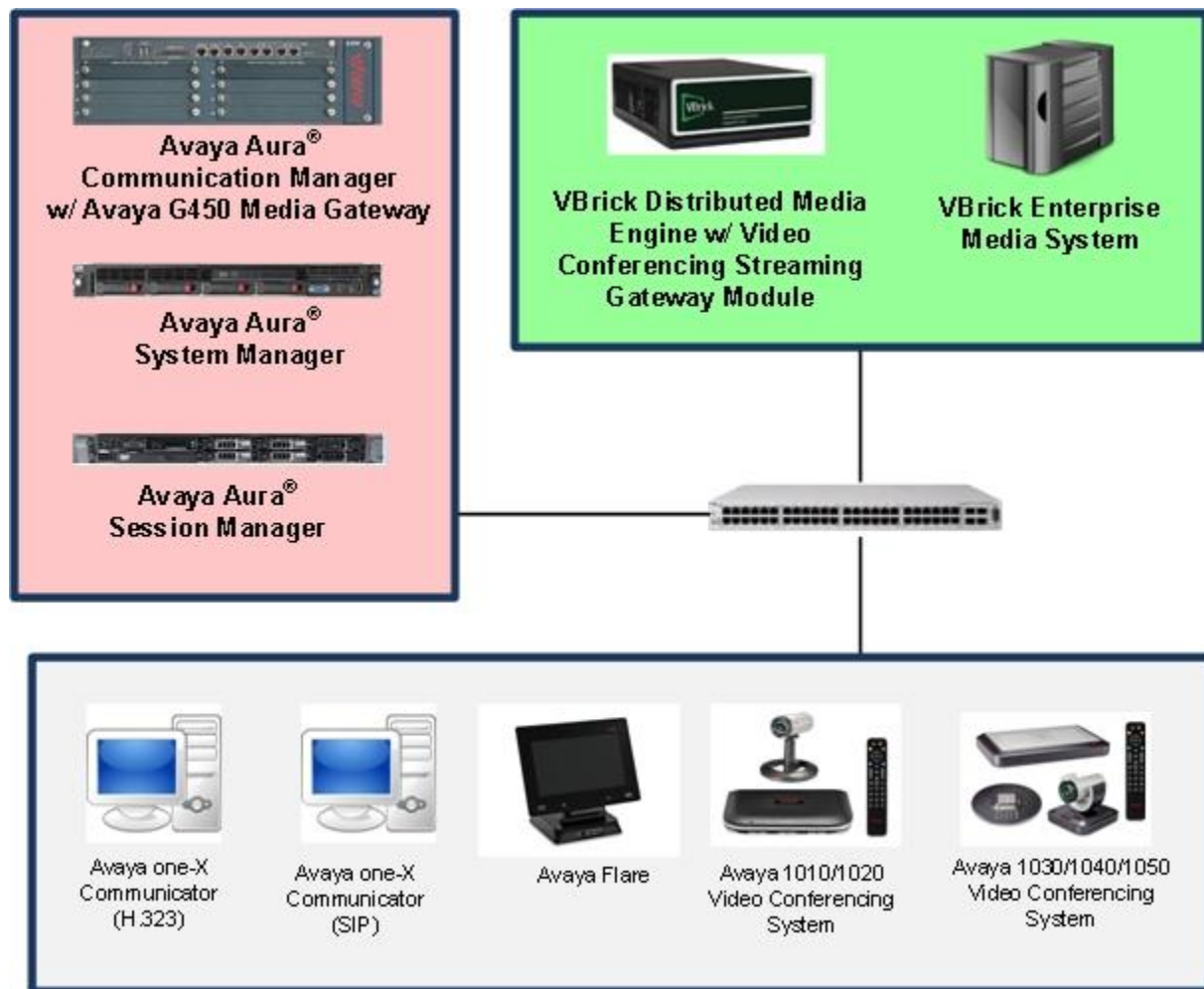


Figure 1: Avaya SIP Network with the VBrick Distributed Media Engine

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.2 SP2
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager 6.2 SP2
Avaya S8300D Server with an Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.2 (R016x.02.0.823.0-19926)
Avaya one-X® Communicator	6.1.5.07-SP5-37495
Avaya Desktop Video Device	1.1.1
Avaya 1020 Video Conference System	4.8.3 (26)
Avaya 1050 Video Conference System	4.8.3 (26)
VBrick Distributed Media Engine 7530: <ul style="list-style-type: none">• VBrick H.264 Distributed Media Engine• Video Conference Streaming Gateway Module	3.0.2

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Configure VBrick DME as an Off-PBX Station (OPS)
- Configure a SIP trunk between Communication Manager and Session Manager

Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials.

5.1 Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS), video capable endpoints, and SIP Trunk options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                          Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 409
Maximum Stations: 41000 51
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 19
Maximum Off-PBX Telephones - PBFMC: 41000 0
Maximum Off-PBX Telephones - PVFMC: 41000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0

(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options** form, verify that the number of video capable endpoints and SIP trunks supported by the system is sufficient.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	77
Maximum Concurrently Registered IP Stations:	18000	5
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:	18000	8
Maximum Video Capable IP Softphones:	18000	3
Maximum Administered SIP Trunks:	24000	180
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2 Configure SIP Trunk

In the **IP Node Names** form, assign a host name and IP address for the Session Manager SIP interface. Note the processor host name of Communication Manager. The host names will be used throughout the other configuration screens of Communication Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM_21_31	10.64.21.31	
default	0.0.0.0	
msgserver	10.64.21.41	
procr	10.64.21.41	
procr6	::	

(14 of 14 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
Name:		
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? 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		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to the VBrick DME. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown above. The default settings of the **IP Codec Set** form are shown below.

change ip-codec-set 1					Page	1 of	2
IP Codec Set							
Codec Set: 1							
Audio	Silence	Frames	Packet				
Codec	Suppression	Per Pkt	Size (ms)				
1: G.711MU	n	2	20				
2:							

Configure **Page 2** of the **IP Codec Set**, enable **Allow Direct-IP Multimedia**. Set **Maximum Call Rate for Direct-IP Multimedia** and **Maximum Call Rate for Priority Direct-IP Multimedia** to desired values or use the default values.

change ip-codec-set 1					Page	2 of	2
IP Codec Set							
Allow Direct-IP Multimedia? y							
Maximum Call Rate for Direct-IP Multimedia: 10240:Kbits							
Maximum Call Rate for Priority Direct-IP Multimedia: 10240:Kbits							
	Mode	Redundancy					
FAX	t.38-standard	0					
Modem	off	0					
TDD/TTY	US	3					
Clear-channel	n	0					

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Type **add signaling-group n** where n is the number of the signaling group. Configure the Signaling Group form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- Set the **Transport Method** field to *tls*.
- Set the **IP Video** field to *y*. This is an important setting required for video calls.
- Specify the processor of Communication Manager and the Session Manager SIP interface as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- Set the **Initial IP-IP Direct Media** field to *y*.
- The default values for the other fields may be used.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM		
Near-end Node Name: procr	Far-end Node Name: SM_21_31	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
Far-end Network Region: 1		
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate		
DTMF over IP: rtp-payload		
Session Establishment Timer(min): 3		
Enable Layer 3 Test? y		
H.323 Station Outgoing Direct Media? n		
Bypass If IP Threshold Exceeded? n		
RFC 3389 Comfort Noise? n		
Direct IP-IP Audio Connections? y		
IP Audio Hairpinning? n		
Initial IP-IP Direct Media? y		
Alternate Route Timer(sec): 20		

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to SIP endpoints. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*. Set the **Member Assignment Method** to *auto*. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: to SM_21_31	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: 50		

On **Page 3** of the trunk group form, set the **Numbering Format** field to *unk-pvt* (other configurations are possible). This field specifies the format of the calling party number sent to the far-end.

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: unk-pvt		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

Configure the **Private Numbering Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '5' whose calls are routed over any trunk group, including SIP trunk group "1", have the extension sent to the far-end for display purposes.

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

5.3 Configure Stations for VBrick Distributed Media Engine

The **station** and **off-pbx-telephone station-mapping** configuration shown in this section was automatically performed by creating the **User** in Session Manager as described in **Section 6.6**. In this section, simply verify the settings. Note that the **User** has to be added in Session Manager first before it can be viewed on Communication Manager. Alternatively, this configuration could have also been performed manually on Communication Manager. Two users were created, 53124 and 53125. User 53124, shown below, was created for incoming calls to the DME. User 53135, not shown, was created using the same steps for outgoing calls from the DME.

Use the **display station** command to view the station created for the VBrick Distributed Media Engine for incoming calls (i.e. station **53124**) and verify the settings in bold. Note that the **IP Video** field must be set to y.

display station 53124		Page 1 of 6
STATION		
Extension: 53124	Lock Messages? n	BCC: M
Type: 9630SIP	Security Code: 123456	TN: 1
Port: S00006	Coverage Path 1:	COR: 1
Name: DME - Incoming, VBrick	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19		
	Message Lamp Ext: 53124	
Display Language: english	Button Modules: 0	
Survivable COR: internal		
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? y	

Use the **display off-pbx-telephone station-mapping** command to view the mapping of the Communication Manager extensions (e.g., 53124) to the same extension configured in System Manager. Verify the field values shown. For the sample configuration, the **Trunk Selection** field is set to *aar* so that AAR call routing is used to route calls to Session Manager. AAR call routing configuration is not shown in these Application Notes. The **Configuration Set** value can reference a set that has the default settings.

display off-pbx-telephone station-mapping 53167							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
53124	OPS	-		53167	aar	1	

6. Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Application Sequence
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager
- Add SIP User

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials. The initial screen is displayed as shown below. The configuration in this section will primarily be performed under **Routing** and **Session Manager** listed within the **Elements** box.



Users	Elements	Services
<p>Administrators Manage Administrative Users</p> <p>Directory Synchronization Synchronize users with the enterprise directory</p> <p>Groups & Roles Manage groups, roles and assign roles to users</p> <p>User Management Manage users, shared user resources and provision users</p>	<p>B5800 Branch Gateway Manage B5800 Branch Gateway 6.2 elements</p> <p>Communication Manager Manage Communication Manager 5.2 and higher elements</p> <p>Conferencing Manage Conferencing Multimedia Server objects</p> <p>Inventory Manage, discover, and navigate to elements, update element software</p> <p>Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements</p> <p>Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging</p> <p>Presence Presence</p> <p>Routing Network Routing Policy</p> <p>Session Manager Session Manager Element Manager</p> <p>SIP AS 8.1 SIP AS 8.1</p>	<p>Backup and Restore Backup and restore System Manager database</p> <p>Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others</p> <p>Configurations Manage system wide configurations</p> <p>Events Manage alarms, view and harvest logs</p> <p>Licenses View and configure licenses</p> <p>Replication Track data replication nodes, repair replication nodes</p> <p>Scheduler Schedule, track, cancel, update and delete jobs</p> <p>Security Manage Security Certificates</p> <p>Templates Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway elements</p>

6.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

- **Name:** The authoritative domain name (e.g., *avaya.com*)
- **Type:** *sip*
- **Notes:** Descriptive text (optional).

Click **Commit**.

Since the sample configuration does not deal with any other domains, no additional domains need to be added.

AVAYA Avaya Aura® System Manager 6.2

Last Logged on at August 27, 2012 2:44 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing * **Home**

Home / Elements / Routing / Domains

Domain Management [Help ?](#)

Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.

1 Item Refresh Filter: Enable			
Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

* Input Required

6.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** A pattern used to logically identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the *.21 Subnet* location, which includes the Communication Manager and Session Manager. Click **Commit** to save the Location definition.

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Help ?

Location Details

Commit

Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth.
See Session Manager -> Session Manager Administration -> Global Settings

General

* Name:

.21 Subnet

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Audio Alarm Threshold:

80

%

* Latency before Audio Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.21.*	

Select : All, None

* Input Required

Commit

Cancel

6.3 Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and Communication Manager.

6.3.1 Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Notes :** Optional text.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain** The domain used for the enterprise (e.g., *avaya.com*).

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

[Routing](#) [Home](#)

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities**
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing / SIP Entities

[Help ?](#)

SIP Entity Details

[Commit](#) [Cancel](#)

General

* Name: SM_21_31

* FQDN or IP Address: 10.64.21.31

Type: Session Manager

Notes: local SM (subnet 21)

Location:

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

[Add](#) [Remove](#)25 Items | [Refresh](#)

Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AAM_21_72	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	Alliance	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	UDP	* 5060	Alliance	* 5060	Trusted
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_20_72	* 5061	Trusted
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_111	* 5061	Trusted

Select : All, None

< Previous | Page 1 of 5 | Next >

Port

TCP Failover port:

TLS Failover port:

[Add](#) [Remove](#)4 Items | [Refresh](#)

Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	
<input type="checkbox"/>	5063	TCP	avaya.com	

Select : All, None

SIP Responses to an OPTIONS Request

[Add](#) [Remove](#)0 Items | [Refresh](#)

Filter: Enable

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

* Input Required

[Commit](#) [Cancel](#)

6.3.2 Communication Manager

A SIP Entity must be added for the Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., C-LAN board) on the telephony system.
- **Type:** Select *CM*.
- **Notes :** Optional text.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

Routing

Home

Help ?

Commit

Cancel

SIP Entity Details

General

* Name:

CM_21_41

* FQDN or IP Address:

10.64.21.41

Type:

CM

Notes:

Evolution Server - 8300D

Adaptation:

Location:

.21 Subnet

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

both

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Add

Remove

1 Item

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
	SM_21_31	TLS	* 5061	CM_21_41	* 5061	Trusted

Select : All, None

SIP Responses to an OPTIONS Request

Add

Remove

0 Items

Refresh

Filter: Enable

	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--	-------------------------------	---------------------	-------

* Input Required

Commit


Cancel

6.4 Add Entity Link

The SIP trunk from Session Manager to Communication Manager is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the appropriate protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of Communication Manager.
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in Section 6.3.2 will be denied.*

Click **Commit** to save the Entity Link definition.

Avaya Aura® System Manager 6.2

Last Logged on at August 27, 2012 3:01 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Entity Links

Entity Links

Help ?

CommitCancel

1 Item RefreshFilter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	Trusted	Mike

* Input Required

CommitCancel

6.5 Define Communication Manager as Managed Element

Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

To define Communication Manager as a managed element, select **Elements→Inventory→Manage Elements** on the left and click on the **New** button (not shown) on the right. In the **New Elements** screen (not shown), select *Communication Manager* in the **Type** field.

In the **New Communication Manager** screen, fill in the following fields as follows:

In the *Application* tab:

- **Name:** Enter an identifier for Communication Manager.
- **Type:** *Communication Manager* was previously selected.
- **Node:** Enter the IP address of the administration interface for Communication Manager.



Avaya Aura® System Manager 6.2

Last Logged on at August 27, 2012 2:44 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Inventory ▾
Manage Elements
Upgrade Management
Collected Inventory
Manage Serviceability
Agents
Inventory Management
Synchronization
CS 1000 and CallPilot
Synchronization

Home / Elements / Inventory / Manage Elements

New Communication Manager

General * Attributes *

General ▾

* Name CM_21_41

* Type Communication Manager Reset

Description

* Node 10.64.21.41

Access Point ▾

Port ▾

*Required

Commit Cancel

In the *Attributes* tab:

- **Login / Password:** Enter the login and password used for administration access.
- **Is SSH Connection:** Enable SSH access.
- **Port:** Enter the port number for SSH administration access (5022).

Defaults can be used for the remaining fields. Click **Commit** to save the settings.



Inventory

Manage Elements

Upgrade Management

Collected Inventory

Manage Serviceability Agents

Inventory Management

Synchronization

CS 1000 and CallPilot Synchronization

Home / Elements / Inventory / Manage Elements

Inventory x Home

Help ?

New Communication Manager

Commit Cancel

General * Attributes *

SNMP Attributes ▾

* Version ☒ None ☐ V1 ☐ V3

Attributes ▾

* Login

Password

Confirm Password

Is SSH Connection ☒

* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

Enable Notifications ☐

*Required

Commit Cancel

6.6 Add SIP User

Add two SIP users for the VBrick Distributed Media Engine; one for incoming calls to the DME, and one for outgoing calls from the DME. The example screens below show the user created for incoming calls. The following configuration will automatically create the SIP station on Communication Manager.

To add new SIP users, navigate to **Users → User Management → Manage Users** from the left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **Identity** tab of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter <extension>@<sip domain> of the user (e.g., 53167@avaya.com).
- **Authentication Type:** Select *Basic*.
- **Password:** Enter the password which will be used to log into System Manager
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information when adding a new SIP user to the sample configuration.



User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

Home / Users / User Management / Manage Users

User ManagementHome

New User Profile

Commit & ContinueCommitCancel

Identity *Communication Profile *MembershipContacts

Identity

* Last Name: DME - Incoming

* First Name: VBrick

Middle Name:

Description:

* Login Name: 53124@avaya.com

* Authentication Type: Basic

* Password:

* Confirm Password:

Localized Display Name:

Endpoint Display Name:

Title:

Language Preference:

Time Zone:

Employee ID:

Department:

Company:

Address

Localized Names

*Required

Commit & ContinueCommitCancel

Enter values for the following required attributes for a new SIP user in the **Communication Profile** tab of the new user form.

- **Communication Profile Password:** Enter the password which will be used By the DME to register with Session Manager.
- **Confirm Password:** Re-enter the password from above.

Scroll down to the **Communication Address** section and select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.

AVAYA Avaya Aura® System Manager 6.2

Last Logged on at August 27, 2012 3:01 PM
Help | About | Change Password | Log off admin

User Management * Home

Home / Users / User Management / Manage Users

Help ?

New User Profile

Commit & Continue Commit Cancel

Identity * Communication Profile * Membership Contacts

Communication Profile

Communication Profile Password:
Confirm Password:

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 53124 @ avaya.com

Add Cancel

In the *Session Manager Profile* section, specify the Session Manager entity from **Section 6.3.1** for **Primary Session Manager**. Set the **Home Location** field to the **Location** configured in **Section 6.2**.

☒ **Session Manager Profile** ▼

* **Primary Session Manager** SM_21_31 ▼

Primary	Secondary	Maximum
18	0	18

Secondary Session Manager (None) ▼

Primary	Secondary	Maximum

Origination Application Sequence (None) ▼

Termination Application Sequence (None) ▼

Conference Factory Set (None) ▼

Survivability Server (None) ▼

* **Home Location** .21 Subnet ▼

In the **Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type** Select *Endpoint*.
- **Use Existing Stations:** If this field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select the *DEFAULT_9630SIP_CM_6_2* template.
- **Port:** Enter *IP*.

☒ **CM Endpoint Profile** ▼

* **System** CM_21_41 ▼

* **Profile Type** Endpoint ▼

Use Existing Endpoints ☐

* **Extension** 53124

* **Template** DEFAULT_9630SIP_CM_6_2 ▼

Set Type 9630SIP

Security Code ●●●●●●

* **Port** IP

Voice Mail Number

Preferred Handle (None) ▼

**Delete Endpoint on Unassign of
Endpoint from User or on Delete
User.** ☐

Override Endpoint Name ☒

Next, click on the **Endpoint Editor** button next to the **Extension** field. The following screen is displayed. In the **Feature Options** section, select **IP Video** and click the **Done** button to be returned to the previous screen. Click the **Commit** button to save the new SIP user profile.



[User Management](#) * [Home](#)

[Home](#) / [Users](#) / [User Management](#) / [Manage Users](#)

User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

Edit Endpoint

[Done](#) [Cancel](#)

[\[Save As Template\]](#)

[Help ?](#)

System	<input type="text" value="CM_21_41"/>	Extension	<input type="text" value="53124"/>
Template	<input type="text" value="DEFAULT_9630SIP_CM_6_2"/>	Set Type	<input type="text" value="9630SIP"/>
Port	<input type="text" value="IP"/>	Security Code	<input type="text" value="*****"/>
Name	<input type="text" value="DME - Incoming, VBrick"/>		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)	

<div>Active Station Ringing <input type="text" value="single"/></div> <div>MWI Served User Type <input type="text" value="Select"/></div> <div>Per Station CPN - Send Calling Number <input type="text" value="Select"/></div> <div>IP Phone Group ID <input type="text" value=""/></div> <div>Remote Soft Phone Emergency Calls <input type="text" value="Select"/></div> <div>LWC Reception <input type="text" value="spe"/></div> <div>AUDIX Name <input type="text" value=""/></div> <div>Speakerphone <input type="text" value="Select"/></div> <div>Short/Prefixed Registration Allowed <input type="text" value="Select"/></div> <div>EC500 State <input type="text" value="enabled"/></div>	<div>Auto Answer <input type="text" value="none"/></div> <div>Coverage After Forwarding <input type="text" value="system"/></div> <div>Display Language <input type="text" value="english"/></div> <div>Hunt-to Station <input type="text" value=""/></div> <div>Loss Group <input type="text" value="19"/></div> <div>Survivable COR <input type="text" value="internal"/></div> <div>Time of Day Lock Table <input type="text" value="Select"/></div> <div>Voice Mail Number <input type="text" value=""/></div>
---	--

Features

<input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting <input type="checkbox"/> Bridged Idle Line Preference <input checked="" type="checkbox"/> Coverage Message Retrieval <input type="checkbox"/> Data Restriction <input checked="" type="checkbox"/> Survivable Trunk Dest <input type="checkbox"/> Bridged Appearance Origination Restriction <input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Idle Appearance Preference <input type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy <input checked="" type="checkbox"/> Direct IP-IP Audio Connections <input type="checkbox"/> H.320 Conversion <input checked="" type="checkbox"/> IP Video <input type="checkbox"/> Per Button Ring Control
--	---

*Required

[Done](#) [Cancel](#)

6.7 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *Identity*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.



Session Manager * **Home**

Home / Elements / Session Manager / Session Manager Administration [Help ?](#)

Edit Session Manager

[Commit](#) [Cancel](#)

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name SM_21_31

Description

*Management Access Point Host Name/IP 10.64.21.30

*Direct Routing to Endpoints **Enable**

Security Module

SIP Entity IP Address 10.64.21.31

*Network Mask 255.255.255.0

*Default Gateway 10.64.21.1

*Call Control PHB 46

*QOS Priority 6

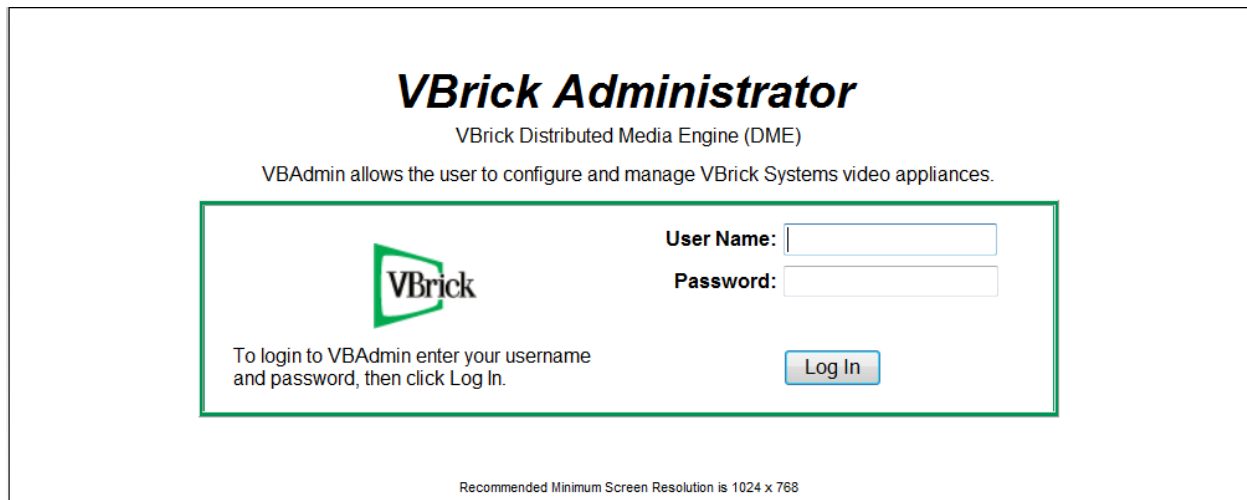
*Speed & Duplex **Auto**

VLAN ID

7. Configure VBrick Distributed Media Engine

The configuration of the VBrick Distributed Media Engine was performed via the VBrick DME's embedded web interface. Refer to reference [3] for additional information on configuring the DME.

From an internet browser, enter `https://<ip-addr>` in the URL field, where `<ip-addr>` is the VBrick DME's IP address. The following **Login** screen is displayed. Log into the system with the appropriate user name and password.



The image shows the VBrick Administrator login interface. At the top, the title "VBrick Administrator" is displayed in a large, bold, black font. Below it, the subtitle "VBrick Distributed Media Engine (DME)" is shown in a smaller font. A descriptive line states: "VAdmin allows the user to configure and manage VBrick Systems video appliances." The main login area is enclosed in a green rectangular border. On the left side of this area is the VBrick logo, which consists of a green square with a white 'V' and the word 'Brick' in black. To the right of the logo, there are two input fields: "User Name:" followed by a text box, and "Password:" followed by a text box. Below these fields is a "Log In" button with a blue gradient. To the left of the button, a small instruction reads: "To login to VAdmin enter your username and password, then click Log In." At the bottom of the entire interface, a small note states: "Recommended Minimum Screen Resolution is 1024 x 768".

After logging in, the Home screen is displayed as shown below.

The screenshot displays the VBrick DME 7530 VBAadmin web interface. On the left is a 'Configuration Menu' with options: Home, System Configuration (Network, Ports, Security, General, Streaming, Caching, Management SAP, Manage Configuration, Activate Feature), Input Configuration (Flash/RTSP Pull, Transport Stream In, RTP Playlists), Output Configuration, User Configuration, VC Gateway Configuration (Incoming Lines, Outgoing Lines, Defaults), Logging, Monitor, Maintenance, Diagnostics, Log Out, and Help. The main content area is titled 'VBrick Distributed Media Engine (VBDME) Status' and shows the following information:

- Status: Started Thu, 23. Aug 2012 06:25:37
- Current Time On Server: Mon, 27. Aug 2012 06:05:06
- Up Time: 3 days 23 hrs 39 min 28 sec
- Application Code Revision: 3.0.2 8/8/2012 6:01 p.m.
- RTMP Server Version: 3.0.2 Build 1315
- OS Registration Number: 3de7-6198-3deb-6360
- RTP CPU Load: 0.00%
- RTMP CPU Load: 0.00%
- Total CPU Load: 0.00%
- Current # of Connections: 2
- Current Throughput: 0 bps
- Multi Protocol Connections Count: 1
- Multi Protocol Max Count: 500
- RTP Connections Count: 1
- RTP Connections Max Count: 100
- Disk Usage: Used: 5120 MB (5%), Available: 103961 MB (95%)

The bottom status bar includes a 'Disable Server' button, the text 'Server is Running', and the IP address '10.64.21.24'.

To set up the DME to receive incoming calls, navigate to **VC Gateway Configuration → Incoming Lines**. The following screen is displayed. Click the appropriate **Edit** button to edit an existing incoming line, or a **New** button to create a new incoming line.

The screenshot shows the VBrick VBAAdmin interface. The sidebar menu on the left includes options like Home, System Configuration, Input Configuration, Output Configuration, User Configuration, VC Gateway Configuration (with sub-items Incoming Lines, Outgoing Lines, and Defaults), Logging, Monitor, Maintenance, Diagnostics, Log Out, and Help. The main content area is titled 'Incoming Lines' and features a 'Page Refresh Interval' dropdown set to 'Never'. Below this is a table with the following data:

Index	Line Name	State	Edit	Delete	Activate	Line	Record
1	IncomingLine1	disconnected	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Deactivate"/>		
2			<input type="button" value="New"/>				
3			<input type="button" value="New"/>				
4			<input type="button" value="New"/>				
5			<input type="button" value="New"/>				
6			<input type="button" value="New"/>				
7			<input type="button" value="New"/>				

Enter the following information on the **Incoming Line Details** screen:

- **Line Name** Enter desired name.
- **Line Identity** Specify *sip:user@<Session Manager IP address>*
- **Should Register** Check *Enabled*.
- **Line Authentication ID** Specify extension used by VBrick DME to register with Session Manager
- **Line Authentication Password** Specify the password used by VBrick DME to register with Session Manager
- **Re-enter Line Authentication Password** Specify the password used by VBrick DME to register with Session Manager

Default values may be used for the remaining fields. Click the **OK** button (not shown) at the bottom of the screen to save the changes.

The screenshot displays the VBrick VBAdmin interface for configuring an incoming line. The left sidebar shows the Configuration Menu with options like Home, System Configuration, Input Configuration, Output Configuration, User Configuration, VC Gateway Configuration, Logging, Monitor, Maintenance, Diagnostics, Log Out, and Help. The main area is titled 'Incoming Line Details' and contains the following fields:

- Line Name: incomingLine1
- Line Identity: sip:53124@10.64.21.31
- Should Register: ☒ Enabled
- Line Authentication ID: 53124
- Line Authentication Password: [masked]
- Re-enter Line Authentication Password: [masked]
- Never Hang Up: ☐ Enabled
- Maximum Call Time(min): 120
- Video Resolution: 704x480 @ 30fps at 512kbps
- P-Mode: ☒ standard ☐ override
- I-Frame Interval(sec): ☒ Enabled 5
- Audio Bit Rate: 32K
- Activate Line: ☒ Enabled
- Multicast RTP Relay: ☐ Enabled
- Record to VEMS: ☐ Enabled
- VEMS Mystro User: [blank] (If blank, then the default user id is used)
- VEMS Mystro Password: [blank]
- Re-enter VEMS Mystro Password: [blank]
- Automatic Record: ☐ Enabled
- Title: dme
- Description: [blank]

The status bar at the bottom indicates 'Server is Running' and the IP address '10.64.21.24'.

To set up the DME to initiate outgoing calls, navigate to **VC Gateway Configuration → Outgoing Lines**. The following screen is displayed. Click the appropriate **Edit** button to edit an existing outgoing line, or a **New** button to create a new outgoing line.

Configuration Menu

- Home
- System Configuration
- Input Configuration
- Output Configuration
- User Configuration
- VC Gateway Configuration
 - Incoming Lines
 - Outgoing Lines**
 - Defaults
- Logging
- Monitor
- Maintenance
- Diagnostics
- Log Out
- Help

VBAdmin DME 7530 dme-avaya

Outgoing Lines

Page Refresh Interval:

Index	Line Name	State	Edit	Delete	Line	Record
1	OutgoingLine1	not active	Edit	Delete	Call	
2			New			
3			New			
4			New			
5			New			
6			New			
7			New			

Enter the following information on the **Outgoing Line Details** screen:

- **Line Name** Enter desired name.
- **Line Identity** Specify *sip:user@<Session Manager IP address>*
- **Destination Identity** Specify *sip:user@<Session Manager IP address>* (this is the user to be called)
- **Should Register** Check *Enabled*.
- **Line Authentication ID** Specify extension used by VBrick DME to register with Session Manager
- **Line Authentication Password** Specify the password used by VBrick DME to register with Session Manager
- **Re-enter Line Authentication Password** Specify the password used by VBrick DME to register with Session Manager

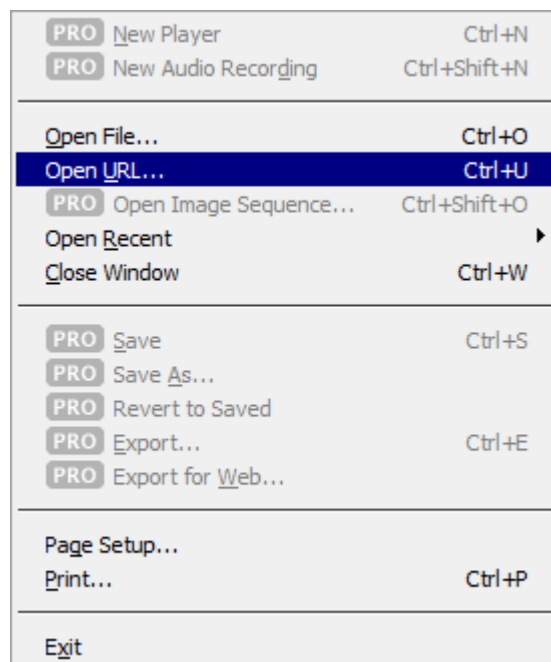
Default values may be used for the remaining fields. Click the **OK** button (not shown) at the bottom of the screen to save the changes.

The screenshot displays the VBrick VBAAdmin web interface for configuring an outgoing line. The left sidebar shows the Configuration Menu with options like Home, System Configuration, Input Configuration, Output Configuration, User Configuration, VC Gateway Configuration, Logging, Monitor, Maintenance, and Diagnostics. The main area is titled 'Outgoing Line Details' and contains 28 numbered fields for configuration. The fields are: 1. Line Name (OutgoingLine1), 2. Line Identity (sip:53125@10.64.21.31), 3. Destination Identity (sip:53102@10.64.21.31), 4. Should Register (checked Enabled), 5. Line Authentication ID (53125), 6. Line Authentication Password (masked), 7. Re-enter Line Authentication Password (masked), 8. Never Hang Up (unchecked), 9. Maximum Call Time(min) (120), 10. Video Resolution (704x480 @ 30fps at 512kbps), 11. P-Mode (radio buttons for standard and override), 12. I-Frame Interval(sec) (checked Enabled, 5), 13. Audio Bit Rate (32K), 14. Call Line (unchecked Enabled), 15. Multicast RTP Relay (unchecked Enabled), 16. Configure Multicast RTP Relay (unchecked Enabled), 17. Record to VEMS (unchecked Enabled), 18. VEMS Mystro User (blank), 19. VEMS Mystro Password (blank), 20. Re-enter VEMS Mystro Password (blank), 21. Automatic Record (unchecked Enabled), 22. Title (Outgoing Line 1), 23. Add Time Stamp (button). The bottom status bar shows 'Disable Server', 'Server is Running', and the IP address '10.64.21.24'.

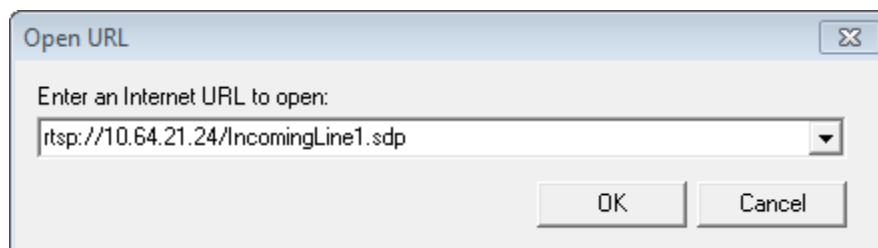
8. Verification Steps

This section provides the steps that may be performed to verify proper configuration of the VBrick Distributed Media Engine with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

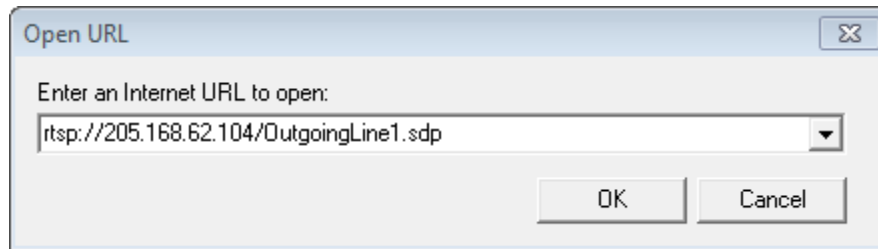
1. Place a video call from an Avaya endpoint to the VBrick DME. Verify that the call is successfully established with 2-way audio and video.
2. Place a video call from the VBrick DME to an Avaya endpoint. Verify that the call is successfully established with 2-way audio and video.
3. Repeat steps 1 and 2 above and while the each call is established, use QuickTime Player to view the streaming video call. Open QuickTime Player and select **File → Open URL....**



To view the stream of the call incoming to the DME, enter the following URL:
rtsp://<DME_IP>/<Line_Name>.sdp, where *<DME_IP>* is the IP address of the DME and *<Line_Name>* is the incoming line name.



To view the stream of the call outgoing from the DME, enter the following URL:
rtsp://<DME_IP>/<Line_Name>.sdp, where *<DME_IP>* is the IP address of the DME and *<Line_Name>* is the outgoing line name.



9. Conclusion

These Application Notes have described the administration steps required to integrate the VBrick Distributed Media Engine with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. VBrick Distributed Media Engine successfully registered with Session Manager and voice and video calls were established with Avaya one-X Communicator (SIP), Avaya Desktop Video Devices, and Avaya 1020 and 1050 video conference systems. All test cases passed with exceptions/observations noted in **Section 2.2**.

10. References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, July 2012, Document Number 03-300509.
- [2] *Administering Avaya Aura® Session Manager*, July 2012, Document Number 03-603324.

The following VBrick product documentation is available at <http://www.vbrick.com>.

- [3] *VBrick Distributed Media Engine, VBrick H.264 v3.0 DME Admin Guide*, May 2012, Document Number 4410-0294-0003.

©2012 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.