



Application Notes for ScoreData ScoreFast™ with Avaya Aura® Application Enablement Services, Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes contain interoperability instructions for ScoreData ScoreFast™ with Avaya Aura® Application Enablement Services, Avaya Aura® Communication Manager and Avaya Aura® Session Manager 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 any 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

This document contains a sample configuration that was used for interoperability compliance testing between ScoreData ScoreFast™ (ScoreFast) and Avaya products.

ScoreFast is a Predictive Analytic solution that utilizes data retrieved from Avaya to make intelligent routing decisions. ScoreFast utilizes the following Avaya interfaces:

- AES – TSAPI Interface – Query agent state for logged on agents.
- AES – SMS Interface – Retrieve Manage objects information from Communication Manager.
- Session Manager – SIP Interface (TCP) – Route calls to and from Session Manager.

Incoming calls to contact centers are routed to ScoreFast via Session Manager SIP Trunk (TCP). ScoreFast performs intelligent routing decision and routes the call back to an agent on Communication Manager via Session Manager (via SIP REFER). ScoreFast uses the SMS interface to retrieve information about station extensions, skills and agents. Once agents are logged on, it uses the TSAPI interface to query agent states.

Note that, ScoreFast utilizes the data retrieved from Avaya Call Management System to make intelligent routing decisions, but during the compliance test, a predetermined set of data was used to make such intelligent decisions. As such, Avaya Call Management System was not used during the compliance test.

2. General Test Approach and Test Results

Interoperability testing contained functional tests that tested the following interfaces/products:

- Avaya Aura® Application Enablement Services – TSAPI Interface
- Avaya Aura® Communication Manager – SMS Interface
- Avaya Aura® Session Manager – SIP Interface

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

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

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

For the testing associated with these Application Notes, the interface between AES and ScoreFast used SSL interface. SIP Interface between Session Manager and ScoreFast did not utilize a secure interface.

2.1. Interoperability Compliance Testing

During Interoperability Compliance testing, call center call routing scenarios were tested. Scenarios tested ScoreFast's ability to:

- Route calls to and from Session Manager.
- Failback scenarios where ScoreFast is unavailable, calls are routed to contact center agents based on vector configuration.
- Deliver calls to single skill and multi-skill agents.
- Query Communication Manager objects via SMS.
- Query agent states via TSAPI.

Serviceability tests such as network failure and server reboots were also tested. Please note that performance testing or load testing were not part of this test effort.

2.2. Test Results

All planned test cases were completed and passed.

2.3. Support

Support for ScoreFast can be obtained via following means:

Email: info@scoredata.com

Phone: +1-408-300-2560

Web: www.scoredata.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and ScoreFast.

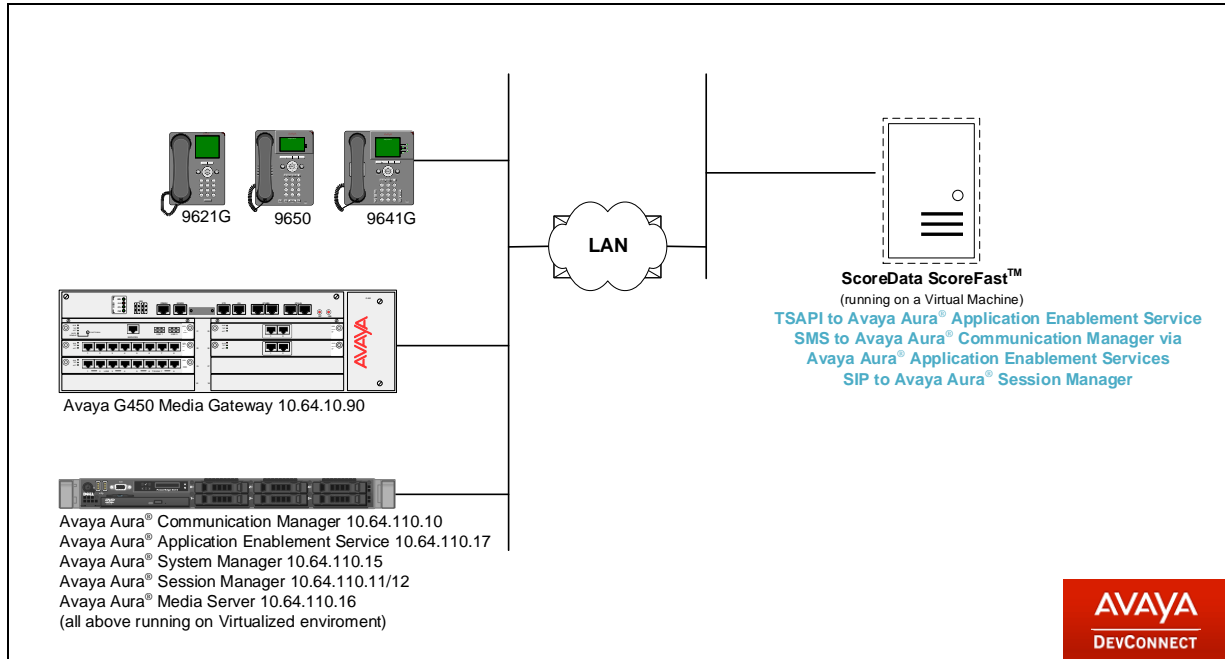


Figure 1: Test Configuration

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	7.1.3 R017x.01.0.532.0 Build 24515
Avaya G450 Media Gateway	37.19.0
Avaya Aura® Application Enablement Services	7.1.3.0.1.7-0
Avaya Aura® System Manager	7.1.3.0.037763
Avaya Aura® Session Manager	7.1.3.0.713014
Avaya Aura® Media Server	v.7.8
ScoreData ScoreFast™ running on Windows Server 2016 Standard.	2.0

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure ScoreFast successfully with Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

The table below shows a sample call center data that was used during compliance testing.

Station	Agent	Hunt Group/Extension	VDN	Vector
50001	2001	1/23001	22035	35
50002	2002			
52001	2003			

Table 1: Sample Data

5.1. Configure Stations

Use **add station *n*** command to add a station, where *n* is an available station extension.

Configure the station as follows, on Page 1:

- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**

These stations are used by contact center agents to log on to Avaya IP Deskphones.

add station 50001		Page	1 of	5
STATION				
Extension: 50001	Lock Messages? n	BCC: 0		
Type: 9641	Security Code: *	TN: 1		
Port: IP	Coverage Path 1:	COR: 1		
Name: H.323 Station 1	Coverage Path 2:	COS: 1		
	Hunt-to Station:	Tests? y		
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 50001			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Button Modules: 0			
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? y			
	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			

One Page 4, under **BUTTON ASSIGNMENTS**, add **auto-in**, **aux-work**, **after-call** and **manual-in** as shown below:

add station 50001		Page	4 of	5
STATION				
SITE DATA				
Room:		Headset? n		
Jack:		Speaker? n		
Cable:		Mounting: d		
Floor:		Cord Length: 0		
Building:		Set Color:		
ABBREVIATED DIALING				
List1:	List2:	List3:		
BUTTON ASSIGNMENTS				
1: call-appr	5: auto-in	Grp:		
2: call-appr	6: aux-work	RC: Grp:		
3: call-appr	7: after-call	Grp:		
4:	8: manual-in	Grp:		
voice-mail				

5.2. Configure Hunt Group

Use **add hunt-group *n*** command to add a hunt group, where ***n*** is an available hunt group. On Page 1:

- In the **Group Name** field, enter a descriptive name.
- Set **ACD, Queue, Vector** to **y**.
- Enter an available **Group Extension**

add hunt-group 1	HUNT GROUP	Page 1 of 4
Group Number: 1	ACD? y	
Group Name: Skill 1	Queue? y	
Group Extension: 23001	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

On Page 2, set **Skill** to **y** and **Measured** to **both**.

add hunt-group 1	HUNT GROUP	Page 2 of 4
Skill? y	Expected Call Handling Time (sec): 20	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: both		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec): 1	After Xfer or Held Call Drops? n	

5.3. Configure Agents

Use **add agent-loginID *n*** to add an agent, where *n* is an available agent id. On Page 1:

- In the **Name** field, type in a descriptive name
- Enter password in **Password** and **Password (enter again)**

add agent-loginID 2001		Page 1 of 2
AGENT LOGINID		
Login ID: 2001	AAS? n	
Name: SD Agent 1	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
Attribute:	AUDIX Name for Messaging:	
LoginID for ISDN/SIP Display? n		
Password:		
Password (enter again):		
Auto Answer: station		
AUX Agent Remains in LOA Queue: system	MIA Across Skills: system	
AUX Agent Considered Idle (MIA): system	ACW Agent Considered Idle: system	
Work Mode on Login: system	Aux Work Reason Code Type: system	
Logout Reason Code Type: system		
Maximum time agent in ACW before logout (sec): system		

On Page 2, set skill number and skill level in **SN** and **SL** fields. Skill number is the hung group that was added in previous section.

agent-loginID 2001		Page 2 of 2		
AGENT LOGINID				
Direct Agent Skill:		Service Objective? n		
Call Handling Preference: skill-level		Local Call Preference? n		
SN	RL SL	SN	RL SL	
1: 35	1	16:	31:	46:
2:		17:	32:	47:
3:		18:	33:	48:
4:		19:	34:	49:
5:		20:	35:	50:
6:		21:	36:	51:
7:		22:	37:	52:
8:		23:	38:	53:
9:		24:	39:	54:
10:		25:	40:	55:
11:		26:	41:	56:
12:		27:	42:	57:
13:		28:	43:	58:
14:		29:	44:	59:
15:		30:	45:	60:
15:				

5.4. Configure Vectors

Use **change vector *n*** to configure a Vector, where *n* is an available Vector number. For test scenarios, Vector 35 was used during compliance test. Note the extension configured in the **route-to** step, 888200. 8 is aar feature access code and 88200 is configured to route to ScoreFast via aar (not shown). Vector was configured as follows:

```
change vector 35                                     Page 1 of 6
                                                    CALL VECTOR

Number: 35                      Name: SD Vector
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 wait-time      2      secs hearing ringback
02 goto step      6      if available-agents in skill 1st      = 0
03 goto step      6      if P      >      0
04 set      P      = none      ADD      1
05 route-to      number 888200      with cov n if unconditionally
06 queue-to      skill 1st pri m
07 stop

Press 'Esc f 6' for Vector Editing
```

Following variables were configured during compliance test.

```
change variables                                     Page 1 of 39
                                                    VARIABLES FOR VECTORS

Var Description      Type      Scope Length Start Assignment      VAC
A      Adjunct Route Digits      collect L      16      1
B      Adjunct Route Flag      collect P      1      1
C
D
E
F
G
H
I
J
K
L
M
N
O
P      SD      collect P      1      1
Q
R
```

5.5. Configure VDN

Use **add vdn *n*** to add a vdn, where *n* is an available vdn extension. On Page 1:

- In the **Name** field, enter a descriptive name
- In the **Destination** field, set **Vector Number** to the vector configured earlier in this document. i.e., Vector Number 35.
- Set 1st Skill* to the Hunt Group from **Section 5.3**

add vdn 22035	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 22035	
Name*: SD VDN 1	
Destination: Vector Number	35
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	Report Adjunct Calls as ACD*? n
VDN of Origin Annc. Extension*:	
1st Skill*: 35	
2nd Skill*:	
3rd Skill*:	
SIP URI:	

5.6. Configure AES connection

Use **change ip-services** command to add an entry for AES. On Page 1,

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.

change ip-services					Page	1 of	3
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the actual hostname obtained from the AES server.
- In the **Password** field, type a password to be administered on AES.
- In the **Enabled** field, type **y**.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes	*	y	in use		
2:						

5.7. Configure CTI Link

Use **add cti-link *n*** command, where *n* is an available CTI link number.

- In the **Extension** field, type in an available extension number
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 69999		
Type: ADJ-IP		
Name: AES CTI Link		COR: 1

5.8. Configure SMS User

ScoreFast uses the SMS interface to retrieve objects information from Communication Manager. An SMS user needs to be created as such. User profile 18 was used for SMS User. This profile is one of the default profiles.

list user-profiles		
USER PROFILES		
Profile	Extended Profile	User Profile Name
0	n	services super-user
1	n	services manager
2	n	business partner
3	n	services
16	n	call center manager
17	n	snmp
18	n	customer super-user
19	n	customer non-super-user

Log onto Communication Manager System Management Interface via a browser, <http://<IP-Address>>, where IP-Address is the IP Address of Communication Manager. Navigate to **Administration → Server (Maintenance) → Administrator Accounts**, and select **Add Logon → Privileged User**.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes the Avaya logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". Below this, a red banner indicates the current section is "Administration". The left sidebar lists various system management categories: Alarms, SNMP, Diagnostics, Server, Server Configuration, Server Upgrades, and Data Backup/Restore. The main content area is titled "Administrator Accounts" and contains the following text: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups." Below this text, a "Select Action:" section offers several options: "Add Login" (selected), "Privileged Administrator" (selected), "Unprivileged Administrator", "SAT Access Only", "Web Access Only", "CDR Access Only", "Business Partner Login (dadmin)", "Business Partner Craft Login", and "Custom Login". Further down, there are four radio button options: "Change Login", "Remove Login", "Lock/Unlock Login", and "Add Group", each followed by a "Select Login" or "Select Group" dropdown menu. At the bottom of the form are "Submit" and "Help" buttons. The top right corner of the interface shows "This Server: acm".

Type in a desired **Login Name**, Select **prof18** for **Additional Groups**, set **Linux shell** to **/opt/ecs/bin/autosat** and type in password in **Enter password or key** and **Re-enter password or key**.

AVAYA

Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Help Log Off
Administration

Administration / Server (Maintenance)
This Server: acm

Alarms

Current Alarms

SNMP

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

IPSI Firmware Upgrades

IPSI Version

Download IPSI Firmware

Download Status

Activate IPSI Upgrade

Activation Status

Data Backup/Restore

Backup Now

Administrator Accounts -- Change Login

This page allows you to edit an administrator login.

[Click to Change](#)

Login name	<input type="text" value="ScoreData"/>
<input type="checkbox"/> Primary group	<input type="text" value="susers"/>
<input type="checkbox"/> Additional groups (profile)	<input type="text" value="prof18"/>
<input type="checkbox"/> Linux shell (/sbin/nologin for no shell)	<input type="text" value="/opt/ecs/bin/autosat"/>
Home directory	<input type="text" value="/var/home/ScoreData"/>
<input type="checkbox"/> Lock this account	<input type="checkbox"/>
<input type="checkbox"/> SAT Limit	<input type="text" value="none"/>
<input type="checkbox"/> Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
<input checked="" type="checkbox"/> Enter password	<input type="password" value="*****"/>
Re-enter password	<input type="password" value="*****"/>
Force password change on next login	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>The user will not be forced to change the password on next login. To enable this behavior, enter a new password and select the Yes option.</small>

6. Configure Avaya Aura® Application Enablement Services

Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for ScoreFast.

6.1. Configure User

All administration is performed by web browser, <https://<aes-ip-address>/>

A user needs to be created for ScoreFast to communicate with AES. Navigate to **User Management → User Admin → Add User**.

Fill in **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set the **CT User** to **Yes**, and **Apply**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message with system details. A red navigation bar contains links for 'User Management | User Admin | Add User' and 'Home | Help | Logout'. On the left, a sidebar menu lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is titled 'Add User' and contains a form with the following fields: 'User Id' (ScoreData), 'Common Name' (ScoreData), 'Surname' (ScoreData), 'User Password' (masked with dots), 'Confirm Password' (masked with dots), 'Admin Note' (empty), 'Avaya Role' (None), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), 'CT User' (Yes), 'Department Number' (empty), and 'Display Name' (empty). A note at the top of the form states 'Fields marked with * can not be empty.'

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**.

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> acqueon	acqueon	NONE	NONE
<input type="radio"/> fil	fil	NONE	NONE
<input type="radio"/> interop	interop	NONE	NONE
<input checked="" type="radio"/> ScoreData	ScoreData	NONE	NONE

[Edit](#) [List All](#)

Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.

Edit CTI User

User Profile:

User ID: ScoreData
Common Name: ScoreData
Worktop Name: NONE
Unrestricted Access: ☒

Call and Device Control:

Call Origination/Termination and Device Status: None

Call and Device Monitoring:

Device Monitoring: None
Calls On A Device Monitoring: None
Call Monitoring: ☐

Routing Control:

Allow Routing on Listed Devices: None

[Apply Changes](#) [Cancel Changes](#)

6.2. Configure Communication Manager Switch Connections

To add links to the Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **acm71** for this test environment:

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm71	Yes	30	1

Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding AESVCS connection in Communication Manager.

Connection Details - cm71

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☐

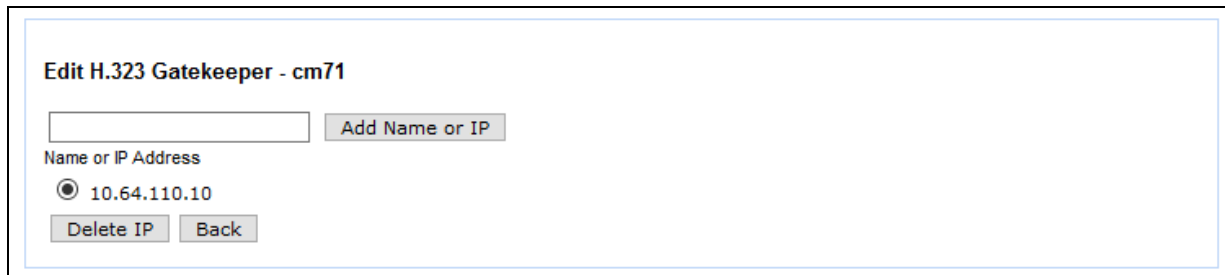
Processor Ethernet ☒

Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN IP Address** (es) for TSAPI message traffic.

Edit Processor Ethernet IP - cm71

Name or IP Address	Status
10.64.110.10	In Use

Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen capture above) to configure the **procr** or **CLAN** IP Address (es).



Edit H.323 Gatekeeper - cm71

Add Name or IP

Name or IP Address

☒ 10.64.110.10

Delete IP **Back**

6.3. Configure TSAPI Link

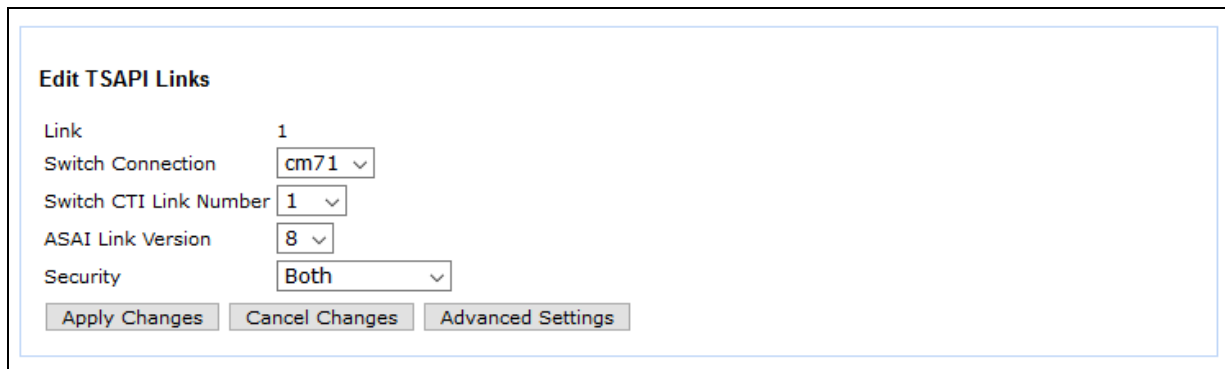
Navigate to the **AE Services → TSAPI → TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

Click **Apply Changes**.

Configuration shown below was previously configured.



Edit TSAPI Links

Link 1

Switch Connection cm71 ▾

Switch CTI Link Number 1 ▾

ASAI Link Version 8 ▾

Security Both ▾

Apply Changes **Cancel Changes** **Advanced Settings**

6.4. Obtain Tlink

Navigate to **Security** → **Security Database** → **Tlinks**. Take a note of the Tlink that will be used by ScoreFast to connect.

Tlinks

Tlink Name

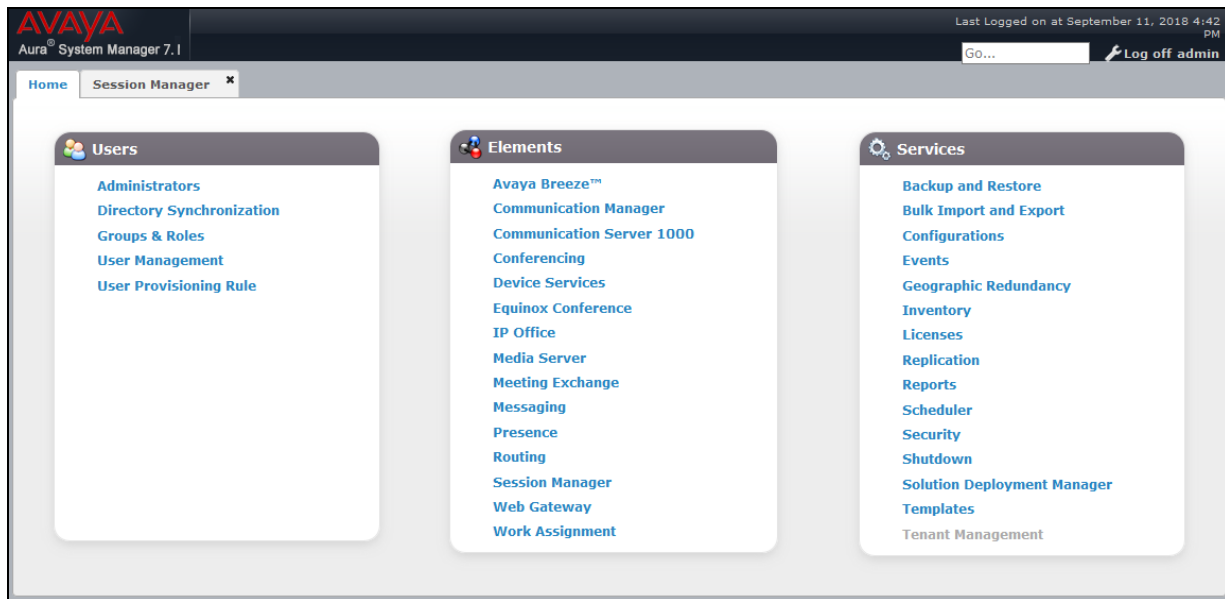
☐ AVAYA#CM71#CSTA#AES

☒ AVAYA#CM71#CSTA-S#AES

Delete Tlink

7. Configure Avaya Aura® Session Manager

Configuration of Session Manager is performed via System Manager. Log onto System Manager Web console using appropriate credentials.



7.1. Add SIP Entity and Entity Links

To add a SIP Entity for ScoreFast, navigate to **Elements → Routing → SIP Entities → New**.

- Type in a **Name**.
- Type in the IP Address of ScoreFast in **FQDN or IP Address**.
- Scroll down and configured the Entity link as shown below. Note the SIP Entity 1 and SIP Entity 2 Ports; they will be used when configuring Scorefast.

AVAYA
Aura® System Manager 7.1

Last Logged on at September 11, 2018 4:42 PM
Go... Log off admin

Home Session Manager * Routing *
Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: scoredata

* FQDN or IP Address: 10.64.110.154

Type: SIP Trunk

Notes:

Adaptation:

Location: DevConnect

Time Zone: America/Denver

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

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"/>	* asm_scoredata_5060_TCP	asm	TCP	* 5060	scoredata	* 5060	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

7.2. Add Routing Policy

Continuing from above, select **Routing Policies** in the left pane and select **New**.

- Type in a **Name**
- Select the **Select** button; select the ScoreFast SIP Entity created above (not shown)

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.1', and a 'Last Logged on at September 11, 2018 4:42 PM' status. Below the navigation bar, there are tabs for 'Home', 'Session Manager', and 'Routing'. The 'Routing' tab is active, and the left sidebar shows a tree view with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains a 'General' section with fields for 'Name' (scoredata), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is a 'SIP Entity as Destination' section with a 'Select' button and a table showing the selected entity 'scoredata' with FQDN or IP Address '10.64.110.154' and Type 'SIP Trunk'.

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
scoredata	10.64.110.154	SIP Trunk	

7.3. Add Dial Pattern

Continuing from above, select **Dial Patterns** in the left pane and select **New** to add a new Dial Pattern.

- Enter the dial pattern for aar routed digits from **Section 5.4**.
- Select **Add** and configure the Routing Policy from previous section.

AVAYA
Aura® System Manager 7.1

Last Logged on at September 11, 2018 4:42 PM
Go... Log off admin

Home Session Manager x Routing x

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 88200

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

Add Remove

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"/>	DevConnect		scoredata	0	<input type="checkbox"/>	scoredata	

Select : All, None

8. Configure ScoreData ScoreFast™

Configuration for ScoreFast is performed on the server it is installed on. During the compliance test, this configuration was performed by a ScoreData Engineer. During the compliance test, ScoreFast was installed on a Windows Server 2016 Standard Virtual Machine.

Below is a list of components that should be installed and configured to implement ScoreFast.

- SD-CTI
 - SD_SMSAPI
 - SD_TMACServer
 - SD_CtiServer
- SD-SIP
 - SD_TSIPServer

8.1. Installation

Copy the ScoreData provided package folder to an application folder. And open “install.bat” file and change the path to application folder root path.

```
sc create "SD _CtiServer" binPath= "C:\Program
Files\Tetherfi\Tetherfi_TSAPIServer\TetherfiCTIServer.exe"

sc create "SD _SMSAPI" binPath= "C:\Program
Files\Tetherfi\Tetherfi_SMSAPI\SMSAPIWinService.exe"

sc create "SD _TMACServer" binPath= "C:\Program
Files\Tetherfi\Tetherfi_TMACServer\AMACWebServerWin.exe"

sc create "SD _TSIPServer" binPath= "C:\Program
Files\Tetherfi\Tetherfi_SipProxy\Tetherfi_SipProxy.exe"
```

Then execute “install.bat” from the ScoreData provided package, in administrator mode. After installation, make all services to auto start and set recovery option to restart (not shown).

8.2. Password encryption

To encrypt passwords, use “ConfigurationProviderT.exe” from SD_SMSAPI folder.

To Encrypt, open command prompt and navigate to folder where you have copied “ConfigurationProviderT.exe”. Execute below command:

```
ConfigurationProviderT.exe <password>
```

8.3. SMSAPI Configuration

Go to SD_SMSAPI application folder and open “SMSAPI_Data.json” file and configure values accordingly.

- tmc.conf.aesIp – IP Address of AES.
- tmc.conf.cmIp – IP Address of Communication Manager.
- tmc.conf.cmUser – SMS User name from **Section 5.8**.
- tmc.conf.cmPassword – SMS User password from **Section 5.8** (use ConfigurationProviderT.exe to encrypt).
- tmc.conf.appPath – Path to SMS API folder (use \\ instead of \).
- tmc.conf.aesUsername – AES TSAPI User name from **Section 6.1**.
- tmc.conf.aesPassword – AES TSAPI User password from **Section 6.1** (use ConfigurationProviderT.exe to encrypt)
- tmc.conf.aesLink – AES Tlink from **Section 6.4**
- tmc.conf.aesTls – TLS version for AES SMS Services (Tls, Tls11, Tls12)
- tmc.conf.listenerPort – SMS API listener port (no need to change. Keep 50000)

Open “tmc.config” and configure correct application paths (not shown).

Sample:

```
{
  "tmc.conf.aesIp": "10.64.110.17",
  "tmc.conf.cmIp": "10.64.110.10:5022",
  "tmc.conf.cmUser": "scoredata",
  "tmc.conf.cmPassword":
  "OJFKp5m4Aa0ZNylUlGc3KLY6pxrD/3JG4wYzMgmvBp136fB7fHYoTIDke34XQv36J
  FLQyVPkMoNrgcprIDJW0Q==",
  "tmc.conf.appPath": "C:\\Program Files\\Tetherfi\\Tetherfi_SMSAPI",
  "tmc.conf.aesUsername": "scoredata",
  "tmc.conf.aesPassword":
  "M6DikXL5cHd6bjnYcUEb+orufG63sw7AwZB3A9iVVBwUIRe2jQvcyUDWo+NiB4rvp
  H25k1sfNi/nMicyaESJrQ==",
  "tmc.conf.aesLink": " AVAYA#CM71#CSTA-S#AES",
  "tmc.conf.aesTls": "Tls12",
  "tmc.conf.listenerPort": "50000"
}
```

8.4. TMAC Server Configuration

Go to SD_TMACServer application folder and open “TMAC_ScoreData.json” file. Configure values accordingly.

- tmc.conf.aesUsername – AES TSAPI User name from **Section 6.1**.
- tmc.conf.aesPassword – AES TSAPI User password from **Section 6.1** (use ConfigurationProviderT.exe to encrypt)
- tmc.conf.aesLink – AES Tlink from **Section 6.4**
- tmc.conf.appPath – TMAC Server application folder (use \\ instead of \)
- tmc.conf.logPath – TMAC Server agent logs path (use \\ instead of \ and folder should be present)
- tmc.conf.listenerPort - TMACServer listener port (no need to change. Keep 50000)
- tmc.conf.ctiserverwspport – CTI Server listen port (no need to change. Keep 1337)
- tmc.conf.scoredataapi – ScoreData Score API URL
- tmc.conf.scoredatatokenapi – ScoreData Token API URL
- tmc.conf.scoredatatimeout – Timeout for score data connection in milliseconds
- tmc.conf.scoredatausername – ScoreData API authorization username
- tmc.conf.scoredatapassword – ScoreData API authorization password (use ConfigurationProviderT.exe to encrypt)

Open “tmc.config” and configure correct application paths (not shown).

Sample:

```
{
  "tmc.conf.aesUsername": "scoredata",
  "tmc.conf.aesPassword":
  "M6DIkXL5cHd6bjnYcUEb+orufG63sw7AwZB3A9iVVBwUIRe2jQvcyUDWo+NiB4rvp
  H25k1sfNi/nMicyaESJrQ==",
  "tmc.conf.aesLink": " AVAYA#CM71#CSTA-S#AES",
  "tmc.conf.appPath": "C:\\Program Files\\Tetherfi\\Tetherfi_TMACServer",
  "tmc.conf.logPath": "C:\\Program
  Files\\Tetherfi\\Logs\\Tetherfi_TMACServer\\AgentLogs",
  "tmc.conf.listenerPort": "50000",
  "tmc.conf.ctiserverwspport": "1337",
  "tmc.conf.scoredataapi": "https://console.scoredata.com/agent/v1/",
  "tmc.conf.scoredatatokenapi": "http://console.scoredata.com/api/token/",
  "tmc.conf.scoredatatimeout": "50000",
  "tmc.conf.scoredatausername": "tetherfi",
  "tmc.conf.scoredatapassword":
  "hCDSZw9TOpVDfMqSJZp4e+OmeNqb5bFzg4CUKaLMJvutFeJfy/TN//2HFjcfSTbil+rB
  4rKvye7q7kFl9cDx6Q==",
}
```

8.5. CTI Server Configuration

Go to SD_CtiServer application folder and open “TetherfiTSAPIServer.exe.config”.

Change below value to include correct application path.

```
<add key="Log4NetConfigFile" value="ApplicationPath\Log4Net.config"/>
```

8.6. TSIP Server configuration

Go to SD_TSIPServer application folder and open “TSIP_Data.json” and configure values accordingly.

- tmc.conf.ProxyPort – SIP Entity 2 Port from **Section 7.1**.
- tmc.conf.ProxyLocalIP – IP Address of ScoreFast server.
- tmc.conf.SipDomain – IP Address of Session Manager.
- tmc.conf.SipServerIp – IP Address of Session Manager.
- tmc.conf.SipServerPort – SIP Entity 1 Port from **Section 7.1**.
- tmc.conf.WSPort – local port which TSIP proxy listen on (don’t change. Keep 27005)
- tmc.conf.SipUserList – TSIP call ports should be configured here. Based on the number of calls you want to handle using the TSIP Server, it should be configured here (100-110 means 10 ports)
- tmc.conf.AppPath – Application path of TSIP Server (use \\ instead of \)
- tmc.conf.LogPath – Log path of TSIP server (use \\ instead of \)
- tmc.conf.WcfPort – TSIP Server listen port (don’t change, keep 50000)
- tmc.conf.scoredataapi – ScoreData Score API URL
- tmc.conf.scoredatatokenapi – ScoreData Token API URL
- tmc.conf.scoredatatimeout – Timeout for score data connection in milliseconds
- tmc.conf.scoredatausername – ScoreData API authorization username
- tmc.conf.scoredatapassword – ScoreData API authorization password (use ConfigurationProviderT.exe to encrypt)

Open “tmc.config” and configure correct application paths (not shown).

Sample:

```
{
  "tmc.conf.ProxyPort": "5060",
  "tmc.conf.ProxyLocalIP": "10.64.110.154",
  "tmc.conf.SipDomain": "10.64.150.17",
  "tmc.conf.SipServerIp": "10.64.150.17",
  "tmc.conf.SipServerPort": "5060",
  "tmc.conf.WSPort": "27005",
  "tmc.conf.SipUserList": "100-110",
  "tmc.conf.AppPath": "C:\\Program Files\\Tetherfi\\Tetherfi_SipProxy",
  "tmc.conf.LogPath": "C:\\Program Files\\Tetherfi\\Logs\\Tetherfi_SipProxy",
  "tmc.conf.WcfPort": "50000",
  "tmc.conf.scoredataapi": "https://console.scoredata.com/agent/v1/",
  "tmc.conf.scoredatatokenapi": "http://console.scoredata.com/api/token/",
  "tmc.conf.scoredatatimeout": "50000",
  "tmc.conf.scoredatausername": "tetherfi",
  "tmc.conf.scoredatapassword":
    "hCDSZw9TOpVDfMqSJZp4e+OmeNqb5bFzg4CUKaLMJvutFeJfy/TN//2HFjcfSTbil+rB4rK
    vye7q7kFl9cDx6Q==",
}
```

8.7. Service Start order

Via services.msc, restart the services in following order:

1. SD_SMSAPI
2. SD_CtiServer
3. SD_TMACServer
4. SD_TSIPServer

9. Verification Steps

- Via a SAT terminal, verify that AES is **Enabled** and **listening** using the **status aesvcs interface** command.

```
status aesvcs interface
```

AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
procr	yes	2	listening

- Verify via SAT terminal, the Service State between Communication Manager and the AES is **established**, using the **status aesvcs cti-link** command.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	8	no	aes	established	225	225

- Via System Manager, **Session Manager → System Status → SIP Entity Monitoring → ScoreFast SIP Entity**, verify Conn. Status and Link Status is **UP**.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: scoredata

Summary View

1 Item

Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	asm	IPv4	10.64.110.154	5060	TCP	FALSE	UP	200 OK	UP

Select : None

Via AES OAM, **TSAPI Service Summary → Status and Control → TSAPI Service Summary → User Status**, verify the user created in **Section 6.1** for ScoreFast is connected.

CTI User Status
☐ Enable page refresh every seconds
CTI Users
Open Streams 1
Closed Streams 0
Open Streams

Name	Time Opened	Time Closed	Tlink Name
scoredata	Wed 05 Sep 2018 05:29:26 PM MDT		AVAYA#CM71#CSTA-S#AES

10. Conclusion

ScoreData ScoreFast™ was able to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager. All executed test cases were passed.

11. Additional References

This section references the product documentation relevant for these Application Notes.

- [1] Administering Avaya Aura® Communication Manager, Release 7.1.3, Issue 7, May 2018.
- [2] Administering Avaya Aura® Session Manager, Release 7.1.3, Issue 5, July 2018.
- [3] Administering and Maintaining Avaya Aura® Application Enablement Services, Release 7.1.3, Issue 5, May 2018.

Documentation related to ScoreFast™ can be directly obtained from ScoreData.

©2018 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.