



Avaya Solution & Interoperability Test Lab

Application Notes for Uptivity Discover with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Uptivity Discover to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing. Uptivity Discover is a call recording solution.

In the compliance testing, Uptivity Discover used the Telephony Services Application Programming Interface and Device, Media, and Call Control interfaces from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and capture the media associated with the monitored agents for call recording with the Service Observing method.

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 configuration steps required for Uptivity Discover to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing. Uptivity Discover is a call recording solution.

In the compliance testing, Uptivity Discover used the Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) interfaces from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and capture the media associated with the monitored agents for call recording.

The TSAPI interface is used by Uptivity Discover to monitor skill groups and agent stations on Avaya Aura® Communication Manager. The DMCC interface is used by Uptivity Discover to register virtual IP softphones, and for adding virtual IP softphones to active calls using the Service Observing method.

When there is an active call at the monitored agent, Uptivity Discover is informed of the call via event reports from the TSAPI interface. Uptivity Discover starts the call recording by using the Service Observing feature from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Discover application, the application automatically requests monitoring on skill groups and agent stations and performs device queries using TSAPI, and registers the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent station with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Discover.

The verification of tests included use of Discover logs for proper message exchanges, and use of Discover web interface for proper logging and playback of calls.

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

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Discover:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC physical devices services and monitoring services to activate Service Observing for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

All test cases were executed, and there was one observation on Discover. With the non-instancing recording script, multiple simultaneous calls at the agent are lumped into one recording entry. Furthermore, for a call that was dropped during a server Ethernet disruption, the recording will be lumped with subsequent calls to the agent, and terminated by either the maximum silence or maximum duration detection.

2.3. Support

Technical support on Discover can be obtained through the following:

- **Phone:** (888) 922-5526, option 2
- **Email:** support@uptivity.com
- **Web:** <http://uptivity.com/support>

3. Reference Configuration

Discover can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Discover monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Supervisor	45000
Agent Station	45001, 45002
Agent ID	45881, 45882

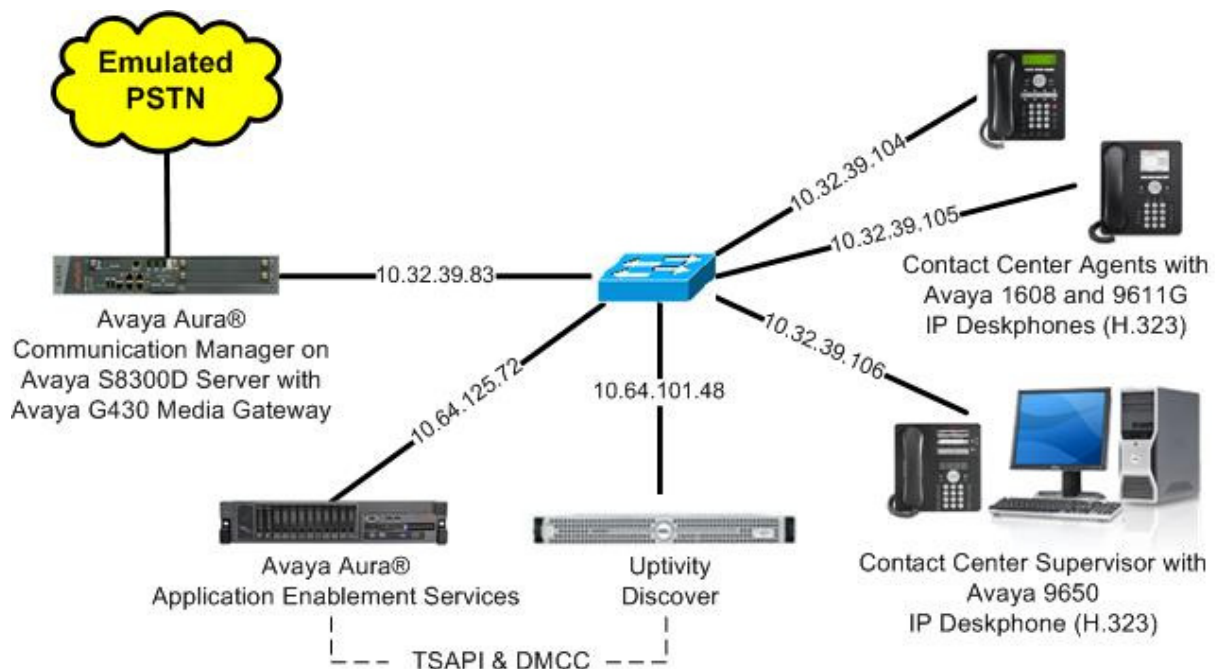


Figure 1: Compliance Testing Configuration

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 on Avaya S8300D Server with Avaya G430 Media Gateway	6.3.2 (R016x.03.0.124.0-21053)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya 1608 IP Deskphone (H.323)	1.340B
Avaya 9611G IP Deskphone (H.323)	6.3037
Avaya 9650 IP Deskphone (H.323)	3.210A
Uptivity Discover on Windows Server 2008 <ul style="list-style-type: none">Web Player (CallCopy.Web.dll)cc_cticore.exeAvaya TSAPI Windows Client (csta32.dll)Avaya DMCC .NET (ServiceProvider.dll)	5.2 R2 Standard 5.2.67.11142 5.2.0.2849 6.1.0.396 4.2.47.0

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Administer feature access codes
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	Computer Telephony Adjunct Links?	y	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n			
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y	
ATM WAN Spare Processor?	n	DS1 MSP?	y	

Navigate to **Page 6**, and verify that the **Service Observing (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page	6 of	11
CALL CENTER OPTIONAL FEATURES				
Call Center Release: 6.0				
ACD?	y	Reason Codes?	y	
BCMS (Basic)?	y	Service Level Maximizer?	n	
BCMS/VuStats Service Level?	y	Service Observing (Basic)?	y	
BSR Local Treatment for IP & ISDN?	y	Service Observing (Remote/By FAC)?	y	
Business Advocate?	n	Service Observing (VDNs)?	y	
Call Work Codes?	y	Timed ACW?	y	
DTMF Feedback Signals For VRU?	y	Vectoring (Basic)?	y	
Dynamic Advocate?	n	Vectoring (Prompting)?	y	

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                     Page 1 of 3
                                         CTI LINK
CTI Link: 1
Extension: 40001
  Type: ADJ-IP
                                         COR: 1
  Name: AES CTI Link
```

5.3. Administer System Parameters Features

Use the “change system-parameters features” command, and navigate to **Page 11**. Set **Service Observing Warning Tone** to the needed setting per customer requirements, and enable **Allow Two Observers in Same Call**, as shown below.

```
change system-parameters features                 Page 11 of 20
                                         FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
    Expert Agent Selection (EAS) Enabled? y
    Minimum Agent-LoginID Password Length:
    Direct Agent Announcement Extension:          Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
    Converse First Data Delay: 0          Second Data Delay: 2
    Converse Signaling Tone(msec): 100    Pause (msec): 70
    Prompting Timeout(secs): 10
    Interflow-qpos EWT Threshod: 2
    Reverse Star/Pound Digit For Collect Step? n
    Available Agent Adjustments for BSR? n
    BSR Tie Strategy: 1st-found
    Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
    Service Observing: Warning Tone? n    or Conference Tone? n
    Service Observing Allowed with Exclusion? n
    Allow Two Observers in Same Call? y
```


5.4. Administer Feature Access Codes

Enter the “change feature-access-codes” command, and navigate to **Page 5**. Set **Service Observing Listen Only Access Code** to an available access code, and make a note of the value to be used later to configure Discover.

```
change feature-access-codes                                     Page 5 of 10

                                FEATURE ACCESS CODE (FAC)
                                Call Center Features

AGENT WORK MODES
    After Call Work Access Code: *14
        Assist Access Code:
        Auto-In Access Code: *11
        Aux Work Access Code:
        Login Access Code: *10
        Logout Access Code: *15
        Manual-in Access Code: *12

SERVICE OBSERVING
    Service Observing Listen Only Access Code: *19
    Service Observing Listen/Talk Access Code:
    Service Observing No Talk Access Code:
    Service Observing Next Call Listen Only Access Code:
    Service Observing by Location Listen Only Access Code:
    Service Observing by Location Listen/Talk Access Code:

AACC CONFERENCE MODES
    Restrict First Consult Activation:      Deactivation:
    Restrict Second Consult Activation:     Deactivation:
```

5.5. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the class of restriction (COR) number used for integration with Discover. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “y”, as shown below. For the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

```
change cor 2                                                  Page 1 of 23

                                CLASS OF RESTRICTION

COR Number: 2
COR Description:

FRL: 0
Can Be Service Observed? y
Can Be A Service Observer? y
Time of Day Chart: 1
Priority Queuing? n
Restriction Override: none
Restricted Call List? n

APLT? y
Calling Party Restriction: none
Called Party Restriction: none
Forced Entry of Account Codes? n
Direct Agent Calling? n
Facility Access Trunk Test? n
Can Change Coverage? n
```

5.6. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

change station 45001	Page 1 of 4	
STATION		
Extension: 45001	Lock Messages? n	BCC: 0
Type: 9611	Security Code: 45001	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 2
Name: G430 Station #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 45001	
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	

Repeat this section to administer all agent stations from **Section 3**. In the compliance testing, two agent stations were administered as shown below.

list station 45001 count 2							
STATIONS							
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack
45001	S00000	G430 Station #1			1	2	
	1608		no			1	1
45002	S00008	G430 Station #2			1	2	
	9611		no			1	1

5.7. Administer Virtual IP Softphones

Add a virtual IP softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “4624”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** “y”

```

add station 45991

```

Page 1 of 5

STATION		
Extension: 45991	Lock Messages? n	BCC: 0
Type: 4624	Security Code: 45991	TN: 1
Port: IP	Coverage Path 1:	COR: 2
Name: Discover Virtual #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y

STATION OPTIONS

Loss Group: 19	Time of Day Lock Table:
	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 45991
Display Language: english	Mute Button Enabled? y
Survivable GK Node Name:	Expansion Module? n
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default
	Customizable Labels? Y

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, two virtual IP softphones were administered as shown below, to allow for simultaneous recording of two monitored agents in **Section 3**.

```

list station 45991 count 2

```

STATIONS							
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack
45991	S00036	Discover Virtual #1				2	
	4624		no			1	1
45992	S00039	Discover Virtual #2				2	
	4624		no			1	1

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Obtain Tlink name
- Administer Discover user
- Enable ports

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a central login box with the text "Please login here:". Inside the box are two input fields labeled "Username" and "Password", and two buttons labeled "Login" and "Reset". At the bottom of the page, a red horizontal bar is followed by the copyright notice: "Copyright © 2009-2013 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user status block. The user status block displays: "Welcome: User", "Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20", "Number of prior failed login attempts: 0", "HostName/IP: aes_125_72/10.64.125.72", "Server Offer Type: VIRTUAL_APPLIANCE_ON_SP", "SW Version: 6.3.1.0.19-0", "Server Date and Time: Tue Nov 19 07:58:28 MST 2013", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home", "Help", and "Logout" links. On the left is a dark sidebar menu with options: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list: "• AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "• Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "• High Availability - Use High Availability to manage AE Services HA.", "• Licensing - Use Licensing to manage the license server.", "• Maintenance - Use Maintenance to manage the routine maintenance tasks.", "• Networking - Use Networking to manage the network interfaces and ports.", "• Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "• Status - Use Status to obtain server status informations.", "• User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "• Utilities - Use Utilities to carry out basic connectivity tests.", and "• Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the main content area, a note states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."


6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected. The top header and user status block are identical to the previous screenshot. The red navigation bar now shows "Licensing" as the active page. The sidebar menu is the same, but "Licensing" is expanded, showing sub-options: "WebLM Server Address", "WebLM Server Access" (highlighted in blue), and "Reserved Licenses". The main content area is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" with a bullet point "• WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" with a bullet point "• WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" with a bullet point "• Reserved Licenses".

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.


Web License Manager (WebLM v6.3)
Help | About | Change Password

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
Uninstall license
Server properties
Manage users
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity
License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" table with one link configured. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	6	Both

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 0**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area contains a form with the following fields: "Link" (set to 2), "Switch Connection" (set to S8300D), "Switch CTI Link Number" (set to 1), "ASAI Link Version" (set to 6), and "Security" (set to Unencrypted). At the bottom of the form are "Apply Changes" and "Cancel Changes" buttons.

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “S8300D”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' selected, with 'Switch Connections' highlighted. The main area displays a table of switch connections. The table has columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. Two connections are listed: S8300D (selected with a radio button) and S8800. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. A top banner shows 'Communication Manager Interface | Switch Connections' and 'Home | Help | Logout'. A top right box contains user information and system status.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	1
<input type="radio"/> S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as the H.323 gatekeeper, in this case “10.32.39.83” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8300D' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field containing '10.32.39.83' and an 'Add Name or IP' button. Below the input field is the label 'Name or IP Address' and two buttons: 'Delete IP' and 'Back'. The top banner and top right box are identical to the previous screenshot.

6.5. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

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 for the user. The left navigation pane shows a tree structure with "Security" expanded, and "Security Database" and "Control" selected. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Nov 19 07:58:28 MST 2013
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit
 - ▶ Certificate Management
 - Enterprise Directory
 - ▶ Host AA
 - ▶ PAM
 - ▼ Security Database
 - Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services


☐ Enable SDB for DMCC Service

☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

6.6. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Nov 19 07:58:28 MST 2013
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

6.7. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Discover.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES_125_72”. Note the use of the switch connection “S8300D” from **Section 6.3** as part of the Tlink name.

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 for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", lists three Tlink names: "AVAYA#S8300D#CSTA#AES_125_72" (selected), "AVAYA#S8800#CSTA#AES_125_72", and "AVAYA#S8800#CSTA-S#AES_125_72". A "Delete Tlink" button is visible below the list.

Welcome: User
Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Nov 19 07:58:28 MST 2013
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name

- ☒ AVAYA#S8300D#CSTA#AES_125_72
- ☐ AVAYA#S8800#CSTA#AES_125_72
- ☐ AVAYA#S8800#CSTA-S#AES_125_72

Delete Tlink

6.8. Administer Discover User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Nov 19 07:59:20 MST 2013
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Iddiscover

* Common Namediscover

* Surnamediscover

* User Password●●●●●●●●

* Confirm Password●●●●●●●●

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.9. Enable Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 19 07:58:13 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Nov 19 07:58:28 MST 2013
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

Enabled Disabled

TR/87 Port4723

Enabled Disabled

7. Configure Uptivity Discover

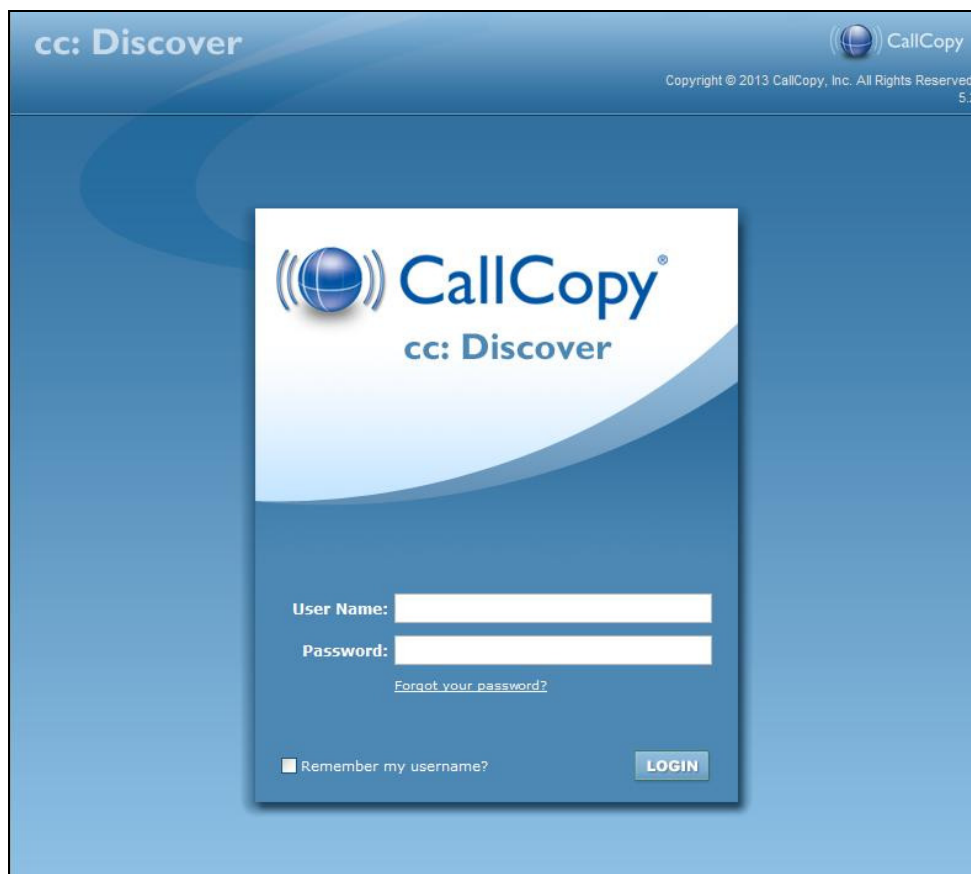
This section provides the procedures for configuring Discover. The procedures include the following areas:

- Launch web interface
- Administer CTI cores
- Administer voice boards

The configuration of Discover is performed by the Uptivity installation team. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Web Interface

Access the Discover web-based interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Discover server. Log in using the appropriate credentials.



The screenshot shows the CallCopy cc: Discover web interface. At the top, there is a header bar with the text "cc: Discover" on the left and the CallCopy logo and "Copyright © 2013 CallCopy, Inc. All Rights Reserved. 5.2" on the right. The main content area has a blue background with a white login box in the center. Inside the login box, there is the CallCopy logo and the text "cc: Discover". Below this, there are two input fields: "User Name:" and "Password:". A link labeled "Forgot your password?" is positioned below the password field. At the bottom of the login box, there is a checkbox labeled "Remember my username?" and a "LOGIN" button.

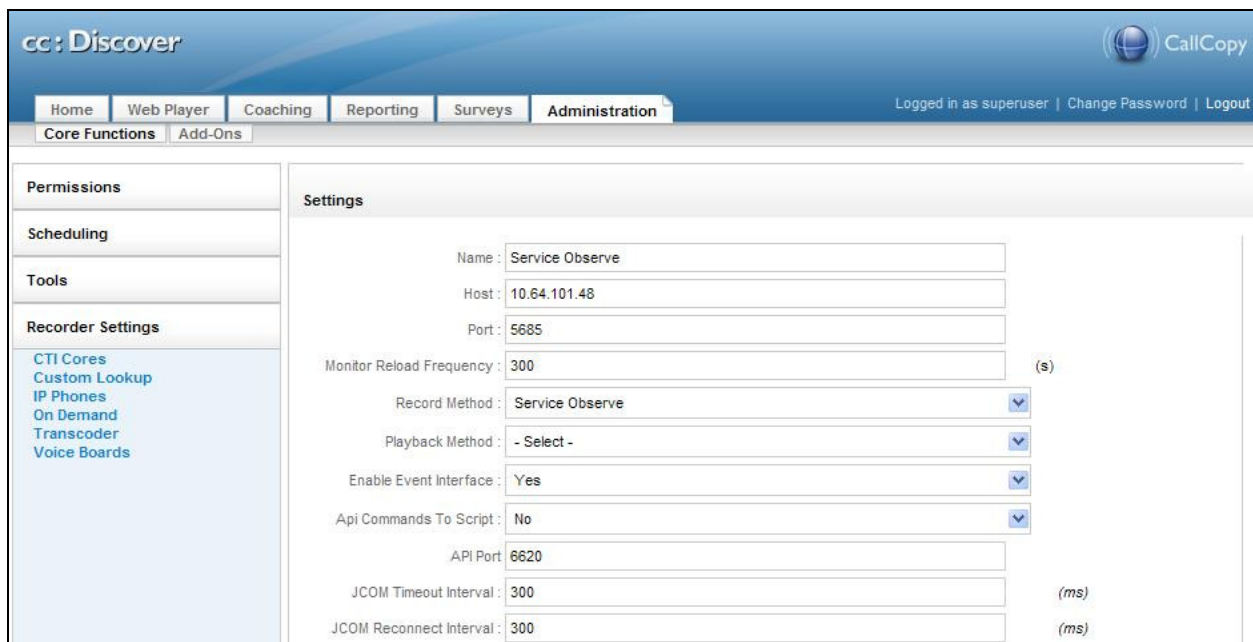
7.2. Administer CTI Cores

The screen below is displayed. Select the **Administration** tab from the top menu, followed by **Recorder Settings** → **CTI Cores** from the left pane, to display the **CTI Cores List** in the right pane.

Click on the pencil icon associated with the relevant CTI core entry, in this case “Service Observe”. Note that the name may vary.



The **Settings** screen is displayed next. Scroll all the way down to the bottom of the screen, and click on the pencil icon associated with the **cc_AvayaTSAPIFx** entry (not shown).



The **Avaya TSAPI Settings** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Server Name:** The Tlink name from **Section 6.7**.
- **Server Username:** The Discover user credentials from **Section 6.8**.
- **Server Password:** The Discover user credentials from **Section 6.8**.

In the **Monitors** section, create an entry for each agent station and skill group from **Section 3**, with “Device” and “Group” as **Monitor Type** respectively, as shown below.

cc: Discover CallCopy

Home Web Player Coaching Reporting **Administration** Logged in as superuser | Change Password | Logout

Core Functions

Permissions

- Users
- Groups
- Roles

Scheduling

Tools

Recorder Settings

System Settings

Web Portal Settings

Avaya TSAPI :: Settings Back Save

Server Name: AVAYA#S8300D#CSTA#AES_125_72

Server Username: discover

Server Password:

Register Monitor Delay: 1000

Number of AES Connection Attempts: 0

Private Data Type: ECS#2-7

TS Version: TS1-2

Query Info On Establish: No

Register DMCC by Agent Login: No

Monitor Devices by Group: No

Monitors:

Monitor Type: Device

Monitor Values:

Prefix:

Postfix:

Filter Monitors: All Monitors

ID	Monitor Type
45001	device
45002	device
48101	group
48102	group

Return to the **Settings** screen. Scroll all the way down to the bottom of the screen, and click on the pencil icon associated with the **cc_AvayaDMCC** entry (not shown).

The **Avaya DMCC Settings** screen is displayed. For **Service Observe Code**, enter the Service Observing listen only feature access code from **Section 5.4**. Retain the default values for the remaining fields.

The screenshot shows the 'cc: Discover' web interface. The top navigation bar includes 'Home', 'Web Player', 'Coaching', 'Reporting', 'Surveys', and 'Administration'. The 'Administration' tab is active, showing 'Core Functions' and 'Add-Ons' sub-tabs. On the left, a 'Permissions' sidebar lists 'Users', 'Groups', and 'Roles'. The main content area is titled 'Avaya DMCC :: Settings' and contains the following fields:

- Service Observe Code : *19
- Dial Digit Delay : 100 (ms)
- Dial Service Observe by Alias : No
- Register DMCC Monitors : No
- Generate Phone Events : No

At the top right of the settings area are 'Back' and 'Save' buttons.

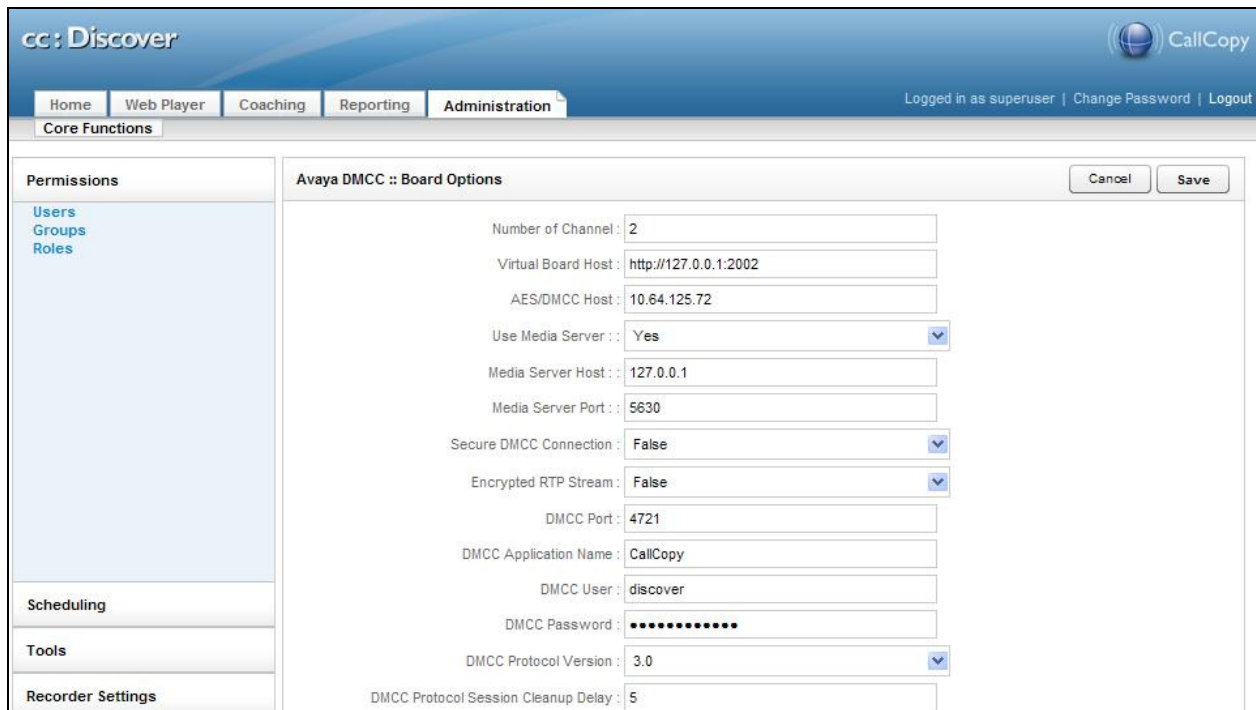
7.3. Administer Voice Boards

Select **Recorder Settings** → **Voice Boards** from the left pane, to display the **Voice Boards List** in the right pane.

Click on the pencil icon associated with the relevant voice board entry, in this case “AVAYADMCC”. Note that the name may vary.



The **Avaya DMCC Board Options** screen is displayed. For **AES/DMCC Host**, enter the IP address of Application Enablement Services. For **DMCC User** and **DMCC Password**, enter the Discover user credentials from **Section 6.8**. Retain the default values in the remaining fields.



Scroll down the screen. For **Avaya Call Manager Host**, enter the IP address of the H.323 gatekeeper from **Section 6.4**.

In the **Channel Configuration** section, update the channel entries with the virtual IP softphone extension and security code from **Section 5.7**, as shown below. Note that the number of channel entries is controlled by the Discover license.

Recorder Settings	DMCC Protocol Session Cleanup Delay : 5		
System Settings	DMCC Protocol Session Duration : 180		
Web Portal Settings	Avaya Call Manager Host : 10.32.39.83		
	Logging Server Port : 2003		
	API Server Host : 127.0.0.1		
	API Port : 5620		
	API Connection Timeout : 1000		
	API Socket Timeout : 10000		
	API Reconnect Tries : 5000		
	DMCC Station Endpoint Host : 10.64.101.48		
	DMCC Codec : G.711 - Mu-Law		
	RTP Listening Interface (NIC) : C6D12F1A-4B6E-4FFA-A908-B75AFD0F77F0		
	DMCC Station Endpoint Initial Port : 7000		
	Temp Recording Location : c:\default_rec		
	UNC Paths : <input type="button" value="Add"/>		
	<input type="button" value="Local"/> <input type="button" value="Remote"/>		
	Board1 of 4 :: Channel Configuration		
	Channels Per Page :: 25		
#Assign	Station	Password	Name
1 Anything	45991	45991	
2 Anything	45992	123456	

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Discover.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	6	no	aes_125_72	established	60	62

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.7** are displayed along with the IP address of the Application Enablement Services server, as shown below.


```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address
45000	9650	IP_Phone	y	10.32.39.104	
	1	3.210A		10.32.39.83	
45001	1608	IP_Phone	y	10.32.39.105	
	1	1.340B		10.32.39.83	
45002	9611	IP_Phone	y	10.32.39.106	
	1	6.3037		10.32.39.83	
45991	4624	IP_API_A	y	10.64.125.72	
	1	3.2040		10.32.39.83	
45992	4624	IP_API_A	y	10.64.125.72	
	1	3.2040		10.32.39.83	

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**.



Application Enablement Services

Management Console

Welcome: User
Last login: Thu Nov 21 14:29:23 2013 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Thu Nov 21 15:03:29 MST 2013
HA Status: Not Configured

[Status](#) | [Status and Control](#) | [TSAPI Service Summary](#)

[Home](#) | [Help](#) | [Logout](#)

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary



■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details


☐ Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	S8800	2	Talking	Fri Nov 8 06:50:48 2013	Online	16	0	15	15	30
	2	S8300D	1	Talking	Thu Nov 21 06:48:51 2013	Online	16	4	62	60	30

For service-wide information, choose one of the following:

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Discover user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the total number of configured channels from **Section 7.3**.



Application Enablement Services

Management Console

Welcome: User

Last login: Thu Nov 21 14:29:23 2013 from 10.32.39.20

Number of prior failed login attempts: 0

HostName/IP: aes_125_72/10.64.125.72

Server Offer Type: VIRTUAL_APPLIANCE_ON_SP

SW Version: 6.3.1.0.19-0

Server Date and Time: Thu Nov 21 15:03:39 MST 2013

HA Status: Not Configured

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
 - Alarm Viewer
 - Log Manager
 - ▶ Logs
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - **DMCC Service Summary**
 - Switch Conn Summary

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Nov 21 15:03:39 MST 2013

Service Uptime: 7 days, 23 hours 17 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 79

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 66

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	CEB51AB99E70AC569 82D783B2CA4C001-1018	discover	CallCopy	10.64.101.48	XML Unencrypted	2

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1

1 Go

8.3. Verify Uptivity Discover

Log an agent into the skill group to handle and complete an ACD call. Follow the procedures in **Section 7.1** to log in to the Discover web-based interface.

Select the **Web Player** tab from the top menu, to display a list of recording entries for the current day. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.

cc:Discover

CallCopy

Home Web Player Coaching Reporting Surveys Administration

Logged in as superuser | Change Password | Logout

Call List Live Monitor

Calendar

November, 2013

Su Mo Tu We Th Fr Sa

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

24 25 26 27 28 29 30

Filter Current Filter: Time Recorded X Settings

Record ID	Voice Port	Time Recorded	Duration	Agent Number	Number Called DNIS	CallerID ANI	Call Direction
87	45001	11/21/2013 4:39:58 PM	00:00:44	45881	9088448001	7328883754	I

Double click on the entry to listen to the playback. Verify that the screen is updated and that the call recording is played back.

cc:Discover

CallCopy

Home Web Player Coaching Reporting Surveys Administration

Logged in as superuser | Change Password | Logout

Call List Live Monitor

Calendar

November, 2013

Su Mo Tu We Th Fr Sa

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

24 25 26 27 28 29 30

Filter Current Filter: Time Recorded X Settings

Record ID	Voice Port	Time Recorded	Duration	Agent Number	Number Called DNIS	CallerID ANI	Call Direction
87	45001	11/21/2013 4:39:58 PM	00:00:44	45881	9088448001	7328883754	I

Pages: 1 25 Items Per Page Go To Page: 1 of 1 GO

Web Player

Layer Details

ID	Start	Stop	Type	Info
1	0:24	0:28	Silence	

Playback Details

0:11 / 0:44

9. Conclusion

These Application Notes describe the configuration steps required for Uptivity Discover to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013, available at <http://support.avaya.com>.
3. *Avaya DMCC Service Observe Integration Guide*, v5.2, May 2013, available upon request to Uptivity Support.

©2014 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.