



Avaya Solution & Interoperability Test Lab

Application Notes for TelStrat Engage with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services and Avaya IP Deskphones for On-Demand Recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelStrat Engage to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 and Avaya IP Deskphones for on-demand call recording.

In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent station extensions on Avaya Aura® Communication Manager. The port mirroring method was used to capture the media associated with the monitored agents with Avaya 96xx IP Deskphones, and the Web Browser Interface to the Avaya 96xx IP Deskphones was used to activate/deactivate the on-demand call recording.

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 TelStrat Engage to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 and Avaya IP Deskphones for on-demand call recording.

In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent station extensions on Avaya Aura® Communication Manager. The port mirroring method was used to capture the media associated with the monitored agents with Avaya 96xx IP Deskphones, and the Web Browser Interface to the Avaya 96xx IP Deskphones was used to activate/deactivate the on-demand call recording.

The TSAPI interface is used by TelStrat Engage to monitor the skill groups and agent station extensions. When there is an active call on the monitored agent, TelStrat Engage is informed of the call via event reports from the TSAPI interface. TelStrat Engage captures the audio by using the replicated media from the port mirroring method. TSAPI event reports are also used to determine when to stop the call recordings.

The Web Browser interface is used by Telstrat Engage to provide activation/deactivation of call recording options via the agents' Avaya 96xx IP Deskphones.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically uses TSAPI to query on the skill group and agent station extensions and request monitoring.

For the manual part of the testing, each call was handled manually with activation/deactivation of call recording initiated from the agent telephone and 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 Engage.

The verification of tests included using the Engage logs for proper message exchanges, and using the Engage Client application for proper logging and playback of the 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 Engage:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.
- Proper display of browser pages and begin/end/cancel of call recordings from the agent telephones.

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

2.2. Test Results

All test cases were executed and passed. The following were observations on Engage from the compliance testing:

- In the blind conference scenario, there is at most one recording entry for the conference-from agent, and the agent needs to initiate the Conversation Save during the initial conversation with the customer, as the option is not provided after the conference action completes.
- In the attended transfer and conference scenarios, there are at most two recording entries for the from-agent, and the from-agent needs to select Conversation Save during the private conversation with the to-agent if that conversation is desired to be saved.
- The initial access to the Web Browser page after a link interruption will display the “Browser page cannot be rendered” message. The workaround is to press the HOME or MENU button.

2.3. Support

Technical support on Engage can be obtained through the following:

- **Phone:** (972) 633-4548
- **Email:** support@telstrat.com

3. Reference Configuration

Engage has an Engage Client application that can be used to review and playback the call recordings. In the compliance testing, the Engage Client application was installed on the supervisor PC. The RTP streams for agents with Avaya 96xx IP Deskphones were mirrored from the layer 2 switch, and replicated over to Engage.

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 addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described.

In the compliance testing, the contact center devices consisted of two VDNs, two skill groups, one supervisor, and two agents shown in the table below. Engage requested monitoring on the skill group and agent station extensions.

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

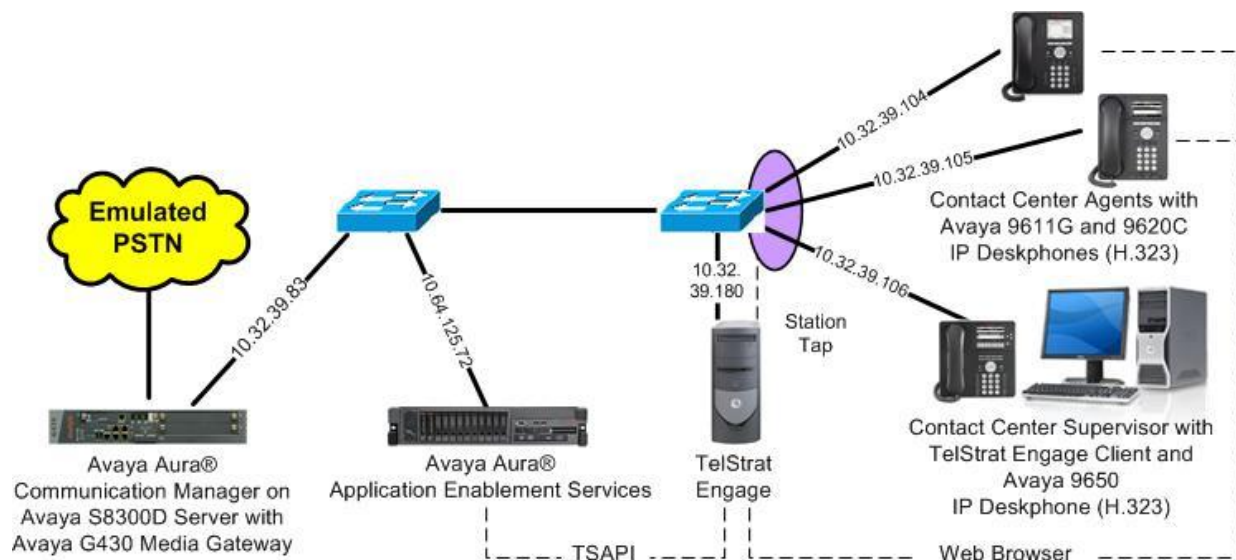


Figure 1: Compliance Testing Configuration

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	6.2 SP3 (R016x.02.0.823.0-20001)
Avaya Aura® Application Enablement Services	6.2 (r6-2-0-18-0)
Avaya 9611G IP Deskphone (H.323)	6.2209
Avaya 9620C IP Deskphone (H.323)	3.105S
Avaya 9650 IP Deskphone (H.323)	3.105S
TelStrat Engage on Windows 2008 Server Standard <ul style="list-style-type: none">• Microsoft SQL Server 2008• Avaya TSAPI Windows Client (csta32.dll)	3.6.1.11 SP 2 R2 6.2.0.257
TelStrat Engage Client on Windows XP Professional	3.6.1.11 2002 SP3

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

5.1. Verify License

Log in to the System Access Terminal (SAT) 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)?	y	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?	y	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n			

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:	TSAPI Link			

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
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Engage user

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" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar, centered, is a login box with a light gray background. Inside the box, the text "Please login here:" is followed by two input fields: "Username" and "Password". Below these fields is a blue "Login" button. At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

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 and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and server information. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining the purpose of the OAM Web and listing the administrative domains it manages: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Feb 19 07:24:07 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

Home | Help | Logout

Home

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.
- 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.
- Help - Use Help to obtain a few tips for using the OAM Help system

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 in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, including the need to use the WebLM Server Address and WebLM Server Access. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the Reserved Licenses option.

Welcome: User
Last login: Tue Feb 19 07:24:07 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking
Security

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:


- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



Web License Manager (WebLM v6.2)

Help | About | Change Password | Log off

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 6:07:47 PM -05:00

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

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;del11950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx309;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0

6.3. Administer TSAPI Link

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

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 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" screen, which contains a table with one link and three buttons: "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	4	Both

Buttons: Add Link, Edit Link, Delete Link

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 5.2**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Add TSAPI Links" screen displayed. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security, along with "Apply Changes" and "Cancel Changes" buttons.

Form fields:

- Link: 2
- Switch Connection: S8300D
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Unencrypted

Buttons: Apply Changes, Cancel Changes

6.4. 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, and click **Apply Changes**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. Below these is an 'Apply Changes' button. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Feb 19 07:24:07 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', 'SW Version: r6-2-0-18-0', and 'Server Date and Time: Tue Feb 19 07:27:34 MST 2013'. The top navigation bar shows 'Security | Security Database | Control' and 'Home | Help | Logout'.

6.5. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked. Below the table is a link 'For status on actual services, please use [Status and Control](#)'. At the bottom are buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays user information: 'Welcome: User', 'Last login: Tue Feb 19 07:24:07 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', 'SW Version: r6-2-0-18-0', and 'Server Date and Time: Tue Feb 19 07:27:34 MST 2013'. The top navigation bar shows 'Maintenance | Service Controller' and 'Home | Help | Logout'.

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input 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

6.6. 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 Engage.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES2-S8800”. 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 with categories like "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", and "Security". Under "Security", the "Security Database" is expanded, showing sub-items: "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks". The main content area, titled "Tlinks", lists three Tlink names with radio buttons for selection: "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 located below the list.

Welcome: User
Last login: Tue Feb 19 07:24:07 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
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

6.7. Administer Engage 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. Click **Apply** at the bottom of the screen (not shown 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 'User Management' expanded, leading to 'User Admin' and then 'Add User'. The main content area is titled 'Add User' and contains a form with various fields. Fields marked with an asterisk (*) are required. The 'CT User' field is a dropdown menu set to 'Yes'. The 'Avaya Role' field is a dropdown menu set to 'None'. The 'User Password' and 'Confirm Password' fields are masked with dots. The 'Admin Note' field is a text area. The 'Business Category', 'Car License', 'CM Home', 'Css Home', 'Department Number', 'Display Name', 'Employee Number', and 'Employee Type' fields are text boxes.

Welcome: User
Last login: Tue Feb 19 07:24:07 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
SW Version: r6-2-0-18-0
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

User Management | User Admin | Add User Home | Help | Logout

Add User

Fields marked with * can not be empty.

* User Id: engage
* Common Name: engage
* Surname: engage
* User Password:
* Confirm Password:
Admin Note:
Avaya Role: None
Business Category:
Car License:
CM Home:
Css Home:
CT User: Yes
Department Number:
Display Name:
Employee Number:
Employee Type:

7. Configure Avaya 96xx IP Deskphones

This section provides the procedures for configuring Avaya 96xx IP Deskphones. The procedures include the following areas:

- Administer phone parameters
- Obtain MAC addresses
- Reboot telephones

7.1. Administer Phone Parameters

From the HTTP server serving the 96xx IP Deskphones, locate the **46xxsettings.txt** file. Navigate to the relevant phone parameters section, in this case **SETTINGS9611**.

Under the **WMLIDLEURI** subsection, set **TPSLIST**, **SUBSCRIBELIST**, and **WMLHOME** parameter as shown below, where “10.32.39.180” is the IP address of the Engage server running the Web Server component.

Repeat this section for all relevant 96xx IP Deskphone types. In the compliance testing, the 9611G and 9620C IP Deskphones were used for testing activation/deactivation of on-demand call recording.

```
#####  
##  
# SETTINGS9611  
##  
##### Add settings for 9611 telephones below #####  
.  
.  
##  
## WMLHOME specifies the URL of a WML page to be displayed by default in the WML  
browser,  
## and whenever the Home softkey is selected in the browser.  
## The value can contain zero or one URL of up to 255 characters; the default value  
is null ("").  
## If the value is null, the WML browser will be disabled.  
## SET WMLHOME http://www.myco.com/ipphoneapps/home.wml  
##  
## WMLIDLEURI specifies zero or one URL for a WML page to be displayed when the  
telephone  
## has been idle for the number of minutes specified by the value of WMLIDLETIME.  
## The value can contain up to 255 characters; the default value is null ("").  
## SET WMLIDLEURI http://www.myco.com/ipphoneapps/idlepage.wml  
##  
  
SET TPSLIST 10.32.39.180  
SET SUBSCRIBELIST  
http://10.32.39.180/EngageOnDemandAvayaPhoneServices/TelStratSubscribe.aspx  
SET WMLHOME http://10.32.39.180/EngageOnDemandAvayaPhoneServices/TelStrat.aspx  
  
##### End of 9611 model-specific settings #####  
GOTO GROUP_SETTINGS
```

7.2. Obtain MAC Addresses

From the Avaya IP Deskphone, press the **MENU** or **HOME** button to display the **MENU** or **HOME** screen (not shown).

From the **MENU** or **HOME** screen, navigate to **Network Information** → **Miscellaneous** to display the **Miscellaneous** screen (not shown).

From the **Miscellaneous** screen, page down as necessary to display the **MAC** parameter (not shown). Make a note of the **MAC** address, which will be used later to configure Engage.

Repeat this section for all Avaya IP Deskphones used by the agents in **Section 3**. In the compliance testing, the MAC addresses associated with the two agent telephones were “001B4F558683 and “7038EEC9D518”.

7.3. Reboot Telephones

After the Engage server has been configured in **Section 8**, manually reboot the 96xx IP Deskphones to pick up the new phone settings.

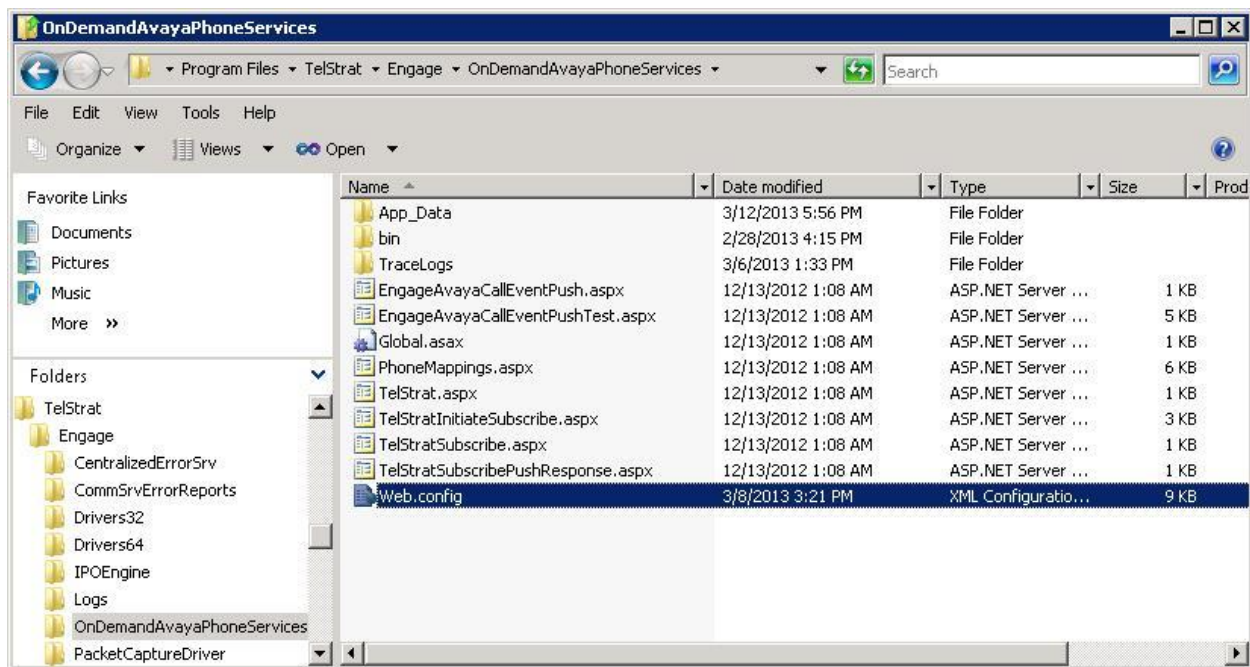
8. Configure TelStrat Engage

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

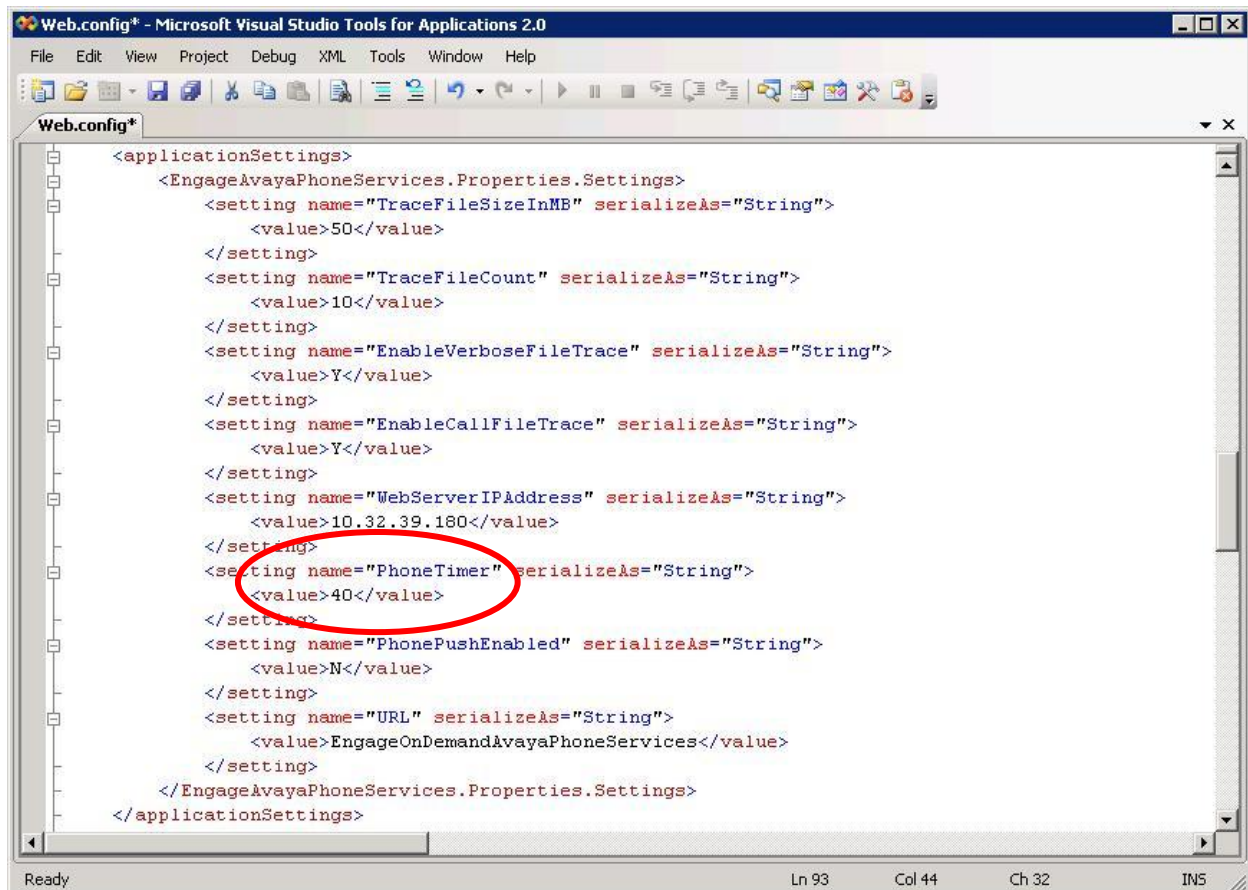
- Administer Web.config
- Administer OnDemand
- Administer TSAPI
- Administer ACD groups
- Administer device port mappings

8.1. Administer Web.config

From the Engage server, navigate to the **C:\Program Files\TelStrat\Engage\OnDemandAvayaPhoneServices** directory to locate the **Web.config** file shown below.



Open the **Web.config** file with the desired application. Scroll down to the **applicationSettings** subsection. For **PhoneTimer**, enter the desired value. In the compliance testing, the default **30** was changed to **40**, for better interoperability with the Avaya 9611 G IP Deskphone.

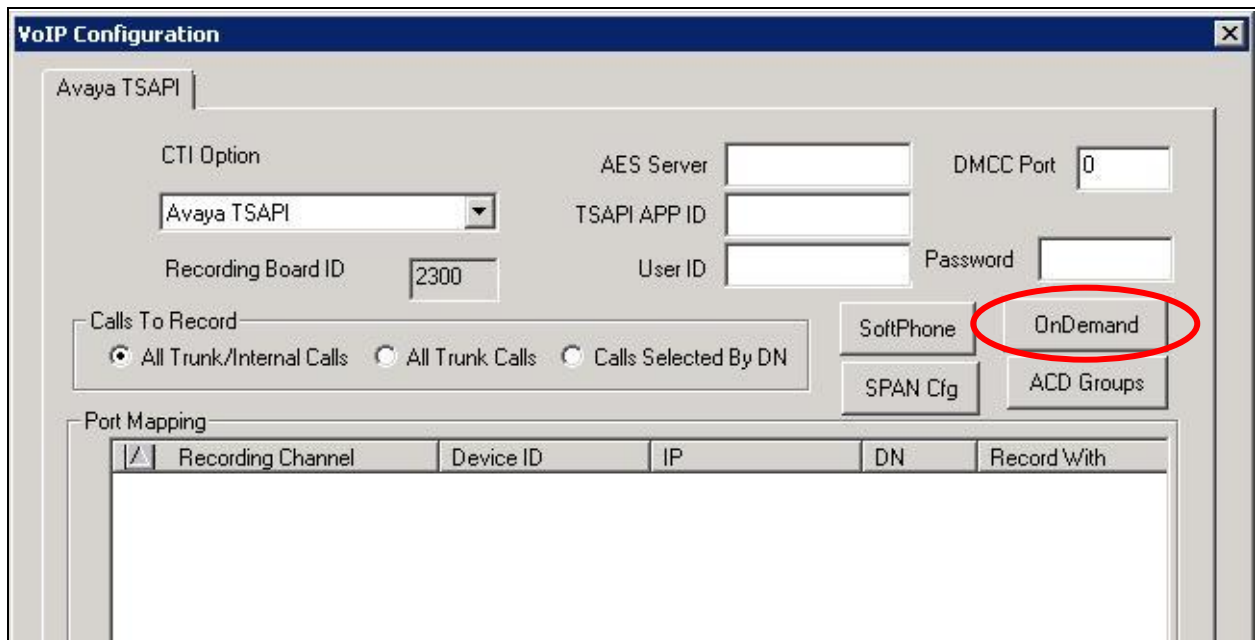


8.2. Administer OnDemand

From the Engage server, select **Start** → **All Programs** → **TelStrat Engage** → **VOIP Engine Configuration**, to display the **Engage VoIP Engine Config Console** screen below. Select **Config**.



The **VoIP Configuration** screen is displayed. Click **OnDemand**.



The **VoIP Configuration** window is shown. It has a tab labeled **Avaya TSAPI**. The window contains several input fields and buttons. The **OnDemand** button is circled in red.

CTI Option: **Avaya TSAPI** (dropdown menu)

AES Server: []

DMCC Port: **0** (text box)

TSAPI APP ID: []

Recording Board ID: **2300** (text box)

User ID: []

Password: []

Calls To Record:

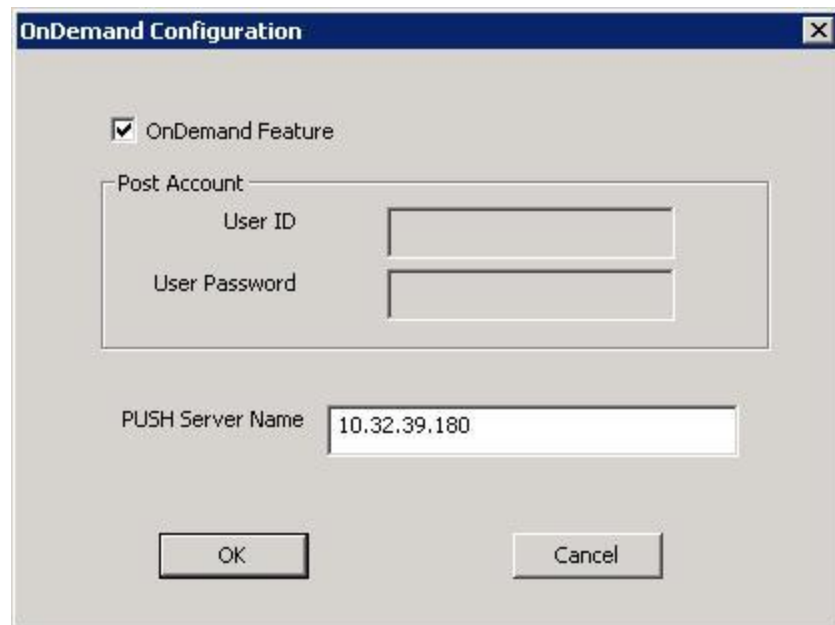
- ☒ All Trunk/Internal Calls
- ☐ All Trunk Calls
- ☐ Calls Selected By DN

Buttons: **SoftPhone**, **OnDemand** (circled), **SPAN Cfg**, **ACD Groups**

Port Mapping:

Recording Channel	Device ID	IP	DN	Record With

The **OnDemand Configuration** screen is displayed next. Check **OnDemand Feature**. For **PUSH Server Name**, enter the IP address of the Engage server running the Web Server component.



The **OnDemand Configuration** window is shown. It contains a checkbox for **OnDemand Feature** which is checked. Below it is a **Post Account** section with **User ID** and **User Password** fields. At the bottom is the **PUSH Server Name** field with the value **10.32.39.180**.

☒ **OnDemand Feature**

Post Account

User ID: []

User Password: []

PUSH Server Name: **10.32.39.180**

Buttons: **OK**, **Cancel**

8.3. Administer OnDemand

The **VoIP Configuration** screen is displayed again. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **CTI Option:** “Avaya TSAPI”
- **AES Server:** The IP address of the Application Enablement Services server.
- **TSAPI APP ID:** The Tlink name from **Section 6.6**.
- **User ID:** The Engage user credentials from **Section 6.7**.
- **Password:** The Engage user credentials from **Section 6.7**.

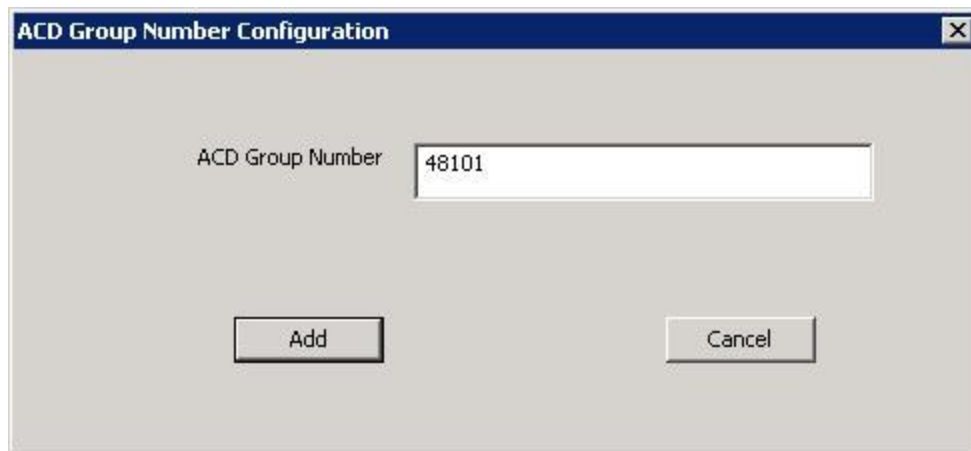
The image shows a screenshot of the "VoIP Configuration" window. The window has a title bar with the text "VoIP Configuration" and a close button. Below the title bar, there is a tab labeled "Avaya TSAPI". The main area of the window contains several fields and buttons. The "CTI Option" field is a dropdown menu with "Avaya TSAPI" selected. The "AES Server" field is a text box containing "10.64.125.72". The "DMCC Port" field is a text box containing "0". The "TSAPI APP ID" field is a text box containing "AVAYA#S8300D#C". The "Recording Board ID" field is a text box containing "2300". The "User ID" field is a text box containing "engage". The "Password" field is a text box containing "XXXXXXXXXX". Below these fields, there is a section labeled "Calls To Record" with three radio buttons: "All Trunk/Internal Calls" (selected), "All Trunk Calls", and "Calls Selected By DN". To the right of the "Calls To Record" section are four buttons: "SoftPhone", "OnDemand", "SPAN Cfg", and "ACD Groups". Below the "Calls To Record" section is a section labeled "Port Mapping" which contains a table with the following columns: "Recording Channel", "Device ID", "Mac Address", "DN", "Record With", and "Trunk/Internal Calls". The table is currently empty.

Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal Calls
-------------------	-----------	-------------	----	-------------	----------------------

8.4. Administer ACD Groups

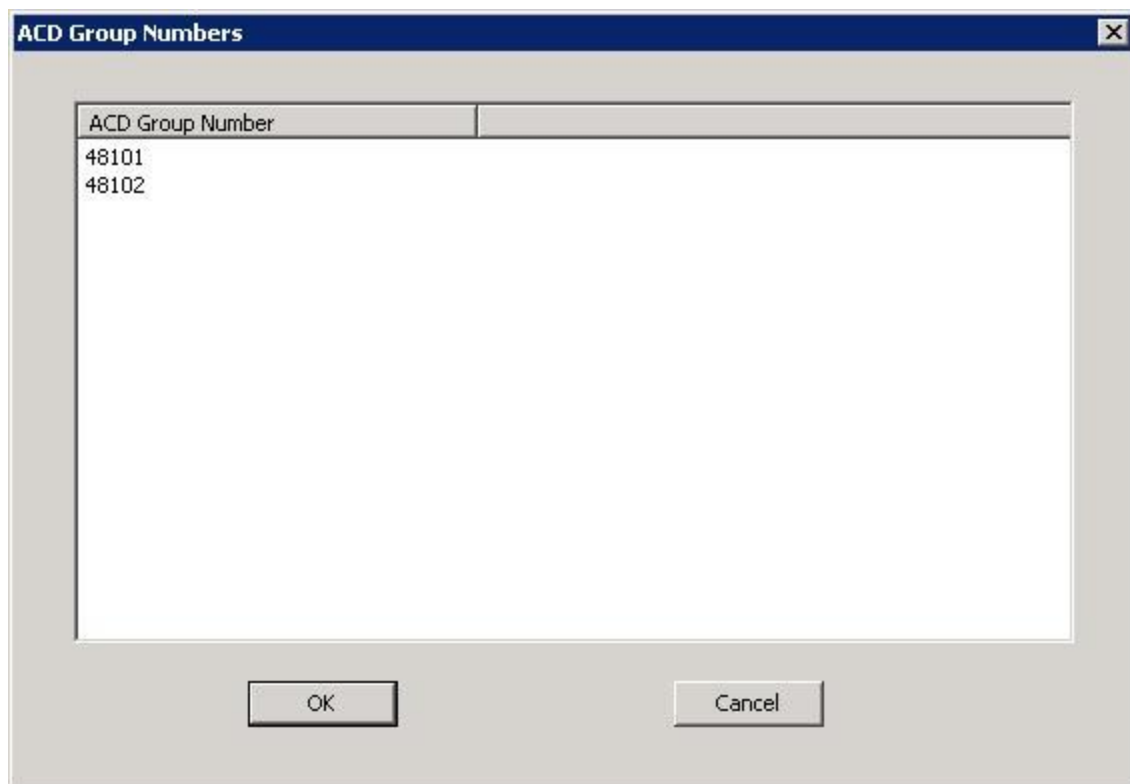
From the **VoIP Configuration** screen shown in **Section 8.2**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

The **ACD Group Number Configuration** screen is displayed next. Enter the first skill group extension from **Section 3**.



The image shows a dialog box titled "ACD Group Number Configuration". It has a text input field labeled "ACD Group Number" containing the value "48101". Below the input field are two buttons: "Add" and "Cancel".

Repeat this section to add all remaining skill groups. In the compliance testing, two skill groups were configured as shown below.



The image shows a dialog box titled "ACD Group Numbers". It contains a list box with the following items:

ACD Group Number
48101
48102

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

8.5. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 8.2**, right-click in the empty pane and select **ADD**. The **Device And CommSrv Port Mapping** screen is displayed.

For **Device ID**, enter the first agent station extension from **Section 3**. Select the **Mirroring** radio button to enable the **MAC** field. For **MAC**, enter the MAC address of the first agent telephone from **Section 7.2**.

For **DN**, enter the dialed number to reach the agent directly for personal calls (non-ACD). For calls originated within Communication Manager, this is usually the agent station extension, depending on the switch configuration. For calls originated outside of Communication Manager, the dialed number usually contains the dial plan prefix. Note that a device port mapping needs to be created for every possible number that can be dialed to reach the agent directly.

For **CommSrv Port Number**, enter an available port, which begins with “0”.

Retain the default in the remaining fields.

Device And CommSrv Port Mapping

Device ID: 45001

MAC: 001B4F558683

DN: 45001

CommSrv Port Number: 0

Calls To Record:
☒ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream:
☒ Mirroring ☐ Service Observe
☐ STC Stream

Beep Tone: No

Add Cancel

Repeat this section to create device port mappings for all agents in **Section 3**.

In the compliance testing, two entries were created for each agent. The incoming non-ACD trunk calls to reach the agent directly will have a prefix of “90884”, as shown below.

The image shows a 'VoIP Configuration' dialog box with the 'Avaya TSAPI' tab selected. The settings include:

- CTI Option: Avaya TSAPI (dropdown)
- AES Server: 10.64.125.72
- DMCC Port: 0
- TSAPI APP ID: AVAYA#S8300D#C
- Recording Board ID: 2300
- User ID: engage
- Password: (masked with asterisks)

Under 'Calls To Record', the radio button 'All Trunk/Internal Calls' is selected. To the right are buttons for 'SoftPhone', 'OnDemand', 'SPAN Cfg', and 'ACD Groups'.

The 'Port Mapping' section contains a table with the following data:

	Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal Calls
000		45001	001B4F558683	45001	Mirroring	Trunk/Internal
000		45001	001B4F558683	9088445001	Mirroring	Trunk/Internal
001		45002	7038EEC9D518	45002	Mirroring	Trunk/Internal
001		45002	7038EEC9D518	9088445002	Mirroring	Trunk/Internal

At the bottom, there is a 'No. of Log Files' field set to 8, a 'Config File Location' button, and 'OK' and 'Cancel' buttons.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, Avaya 96xx IP Deskphones, and Engage.

9.1. 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	4	no	aes_125_72	established	27	27

9.2. 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 number of skill groups and agent station extensions from **Section 3**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Mar 6 07:45:11 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
SW Version: r6-2-0-18-0
Server Date and Time: Wed Mar 6 07:46:18 MST 2013

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ 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 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input type="radio"/>	1	S8800	2	Talking	Wed Feb 13 11:51:18 2013	Online	16	0	15	15	30
<input checked="" type="radio"/>	2	S8300D	1	Talking	Wed Mar 6 07:07:49 2013	Online	16	4	27	27	30

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

9.3. Verify Avaya 96xx IP Deskphones

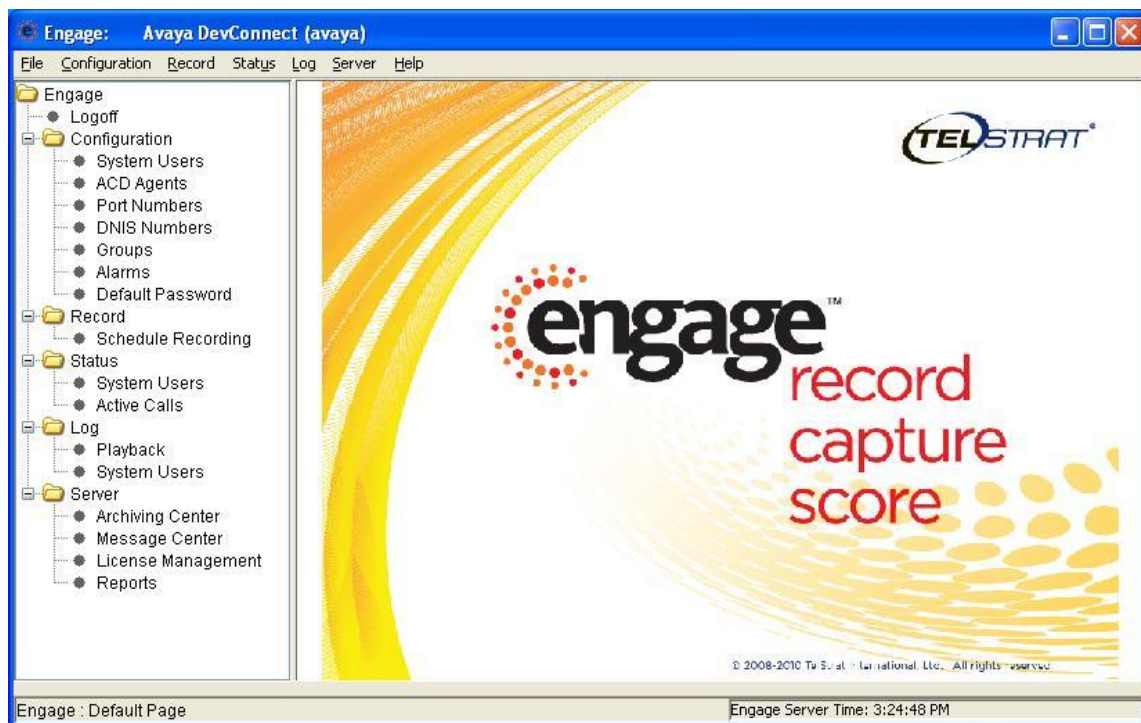
Log an agent into the skill group to answer an ACD call. From the agent's 96xx IP Deskphone, press the **MENU** or **HOME** button to display the **MENU** or **HOME** screen (not shown). Verify that the **Browser** option is included in the listing.

Select the **Browser** option, and verify that a list of recording options is displayed (not shown). Press the **Conversation Save Off** option, and verify that the display is updated to show **Conversation Save On** (not shown), which indicates the current conversation will be saved.

Complete the ACD call.

9.4. Verify TelStrat Engage

From the PC running the Engage Client application, select **Start** → **All Programs** → **TelStrat Engage** → **Engage Client** to launch the application, and log in using the appropriate credentials. The **Engage** screen below is displayed. Select **Engage** → **Log** → **Playback** from the left pane.



The **Engage** screen is updated with a list of the call recordings. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Double click on the entry and verify that the call recording can be played back.



10. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 and Avaya 96xx IP Deskphones for on-demand call recording. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 1, July 2012, available at <http://support.avaya.com>.
3. *Engage Server Installation and Administration Guide*, Product Release 3.6, Standard 1.2, June 2012, available on the installation CD.
4. *Engage Contact Center Suite System Administration Guide*, Product Release 3.6, Standard 3.4, June 2012, available on the installation CD.
5. *Engage Contact Center Suite Configuring Engage with Avaya Aura Communication Manager*, Product Release 3.6.1, Standard 1.3, October 2012, available on the installation CD.

©2013 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.