



Application Notes for TelStrat Engage 5.7 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 and Avaya 9600 Series IP Deskphones for On-Demand Recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelStrat Engage 5.7 to interoperate with Avaya Aura® Communication Manager 7.1, Avaya Aura® Application Enablement Services 7.1, and Avaya 9600 Series IP Deskphones for on-demand recording. TelStrat Engage is a call recording solution.

In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface and Device, Media, and Call Control .NET interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents with Avaya 9600 Series IP Deskphones for on-demand call recording. TelStrat Engage also used the Web and Push interfaces from the Avaya 9600 Series IP Deskphones for agents to activate and deactivate on-demand call recording options.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the configuration steps required for TelStrat Engage 5.7 to interoperate with Avaya Aura® Communication Manager 7.1, Avaya Aura® Application Enablement Services 7.1, and Avaya 9600 Series IP Deskphones for on-demand recording. Engage is a call recording solution.

In the compliance testing, Engage used the Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) .NET interface from Application Enablement Services to monitor skill group and agent stations on Communication Manager, and to capture the media associated with the monitored agents with 9600 Series IP Deskphones for on-demand call recording. Engage also used the Web and Push interfaces from the 9600 Series IP Deskphones for agents to activate and deactivate on-demand call recording options.

The TSAPI interface is used by Engage to monitor skill groups and agent stations on Communication Manager, and for adding virtual IP softphones to active calls using the Single Step Conference method. The DMCC interface is used by TelStrat Engage to register virtual IP softphones, and to obtain the media for recording. The Web and Push interfaces are used by Engage to provide activation and deactivation of call recording options via the agents' 9600 Series IP Deskphones.

Upon notified of an active call at the monitored agent via TSAPI events, Engage adds a virtual IP softphone to the active call via the Single Step Conference method to obtain the media, and pushes recording options to the agent's 9600 Series IP Deskphone. The conversation associated with the entire call or with only specific portions of the call can be recorded depending on the option selected by the user.

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 requested monitoring on skill groups and agent stations, performed device queries using TSAPI, and registered virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings, and with manual actions to activate/deactivate recording options. Necessary user actions such as hold and resume were performed from the user 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 use of Engage logs for proper message exchanges and use of the Engage 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.

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and Engage did not include use of any specific encryption features as requested by TelStrat.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Engage:

- Use of DMCC registration services to register and un-register virtual IP softphones.
- Handling of TSAPI messages in areas of event notification and value queries.
- Use of TSAPI call control services and DMCC monitoring services to activate Single Step Conference for virtual IP softphones to obtain media for call recording.
- Proper recording, logging, and playback of calls for agent scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711 and G.729 codec, service observing, long duration, multiple calls, multiple agents, conference, and transfer.
- Proper display and operation of recording options on the agent phones with SIP and H.323 firmware.

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

2.2. Test Results

All test cases were executed, and the following were observations on Engage:

- By design, conversation cannot be saved while the call is on hold with an error displayed on phone when attempted.
- In the attended transfer and conference scenarios, there are at most two recording entries for the from-user, and the from-user needs to select Conversation Save during the private conversation with the to-user if that conversation is desired to be saved.
- For an active call that experienced an Ethernet disruption to Engage, as well as a call that had Conversation Save activated but later abandoned by caller while on hold, the phone display will continue to show the last set of recording options until arrival of the next call.
- With the phone refresh timer set to four seconds, it can take up to four seconds for the proper recording option screen to appear on the phone.
- In the long duration call scenario where the duration of a call was over an hour, the playback log showed 00:26 for Rec Duration instead of the expected 60:26. Upon playing the recording entry, the Media Player section did reflect end of recording being 60:26.

2.3. Support

Technical support on Engage can be obtained through the following:

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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Engage monitored the skill groups and agent stations show below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Agent ID	65881, 65882
Agent Station	65001 (H.323), 66002 (SIP)

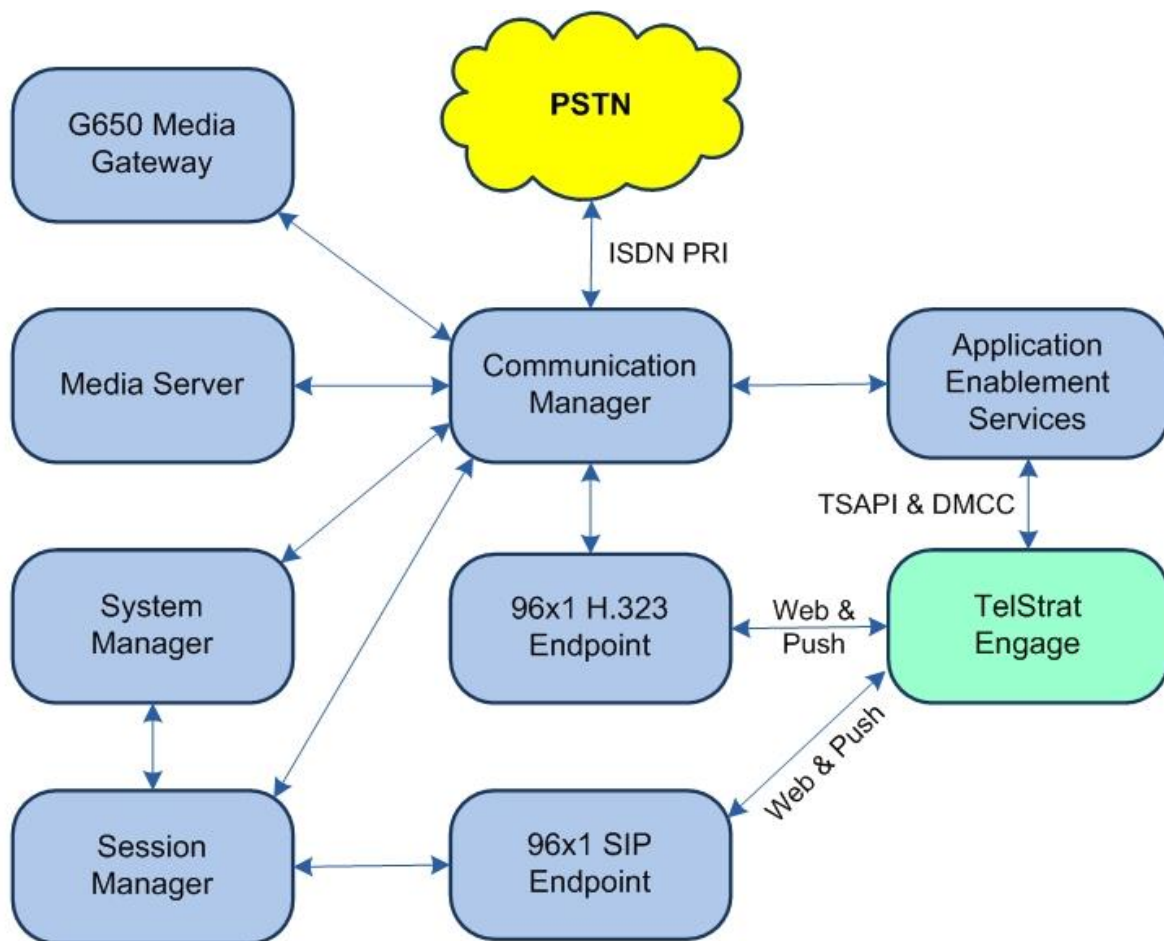


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	7.1 (7.1.3.3.0.532.25082)
Avaya G450 Media Gateway	39.5.0
Avaya Aura® Media Server in Virtual Environment	8.0.0.150
Avaya Aura® Application Enablement Services in Virtual Environment	7.1 (7.1.3.2.0.2-0)
Avaya Aura® Session Manager in Virtual Environment	7.1 (7.1.3.3.713307)
Avaya Aura® System Manager in Virtual Environment	7.1 (7.1.3.3.069127)
Avaya 9611G & 9641G IP Deskphones (H.323)	6.8202
Avaya 9611G IP Deskphone (SIP)	7.1.6.1.3
TelStrat Engage on Windows Server 2016 <ul style="list-style-type: none">• Recorder<ul style="list-style-type: none">- Avaya Phone Services• Web• Microsoft SQL Server 2016• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC .NET (ServiceProvider.dll)	5.7.2 Standard 5.7.2.5 5.7.2.6 5.7.2.4 13.0.5026.0 7.1.1.32 7.0.0.33

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 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 4**. 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 4 of 12
                                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? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      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
ATMS? y      DS1 Echo Cancellation? y
Attendant Vectoring? 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: 58001
Type: ADJ-IP
Name: AES 7.0.1
COR: 1
```

5.3. 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 “9620”.
- **Name:** A descriptive name.
- **Security Code:** Enter same value as **Extension**, as required by Engage.
- **IP SoftPhone:** “y”

```
add station 65991
```

Page 1 of 5

STATION	
Extension: 65991	Lock Messages? n
Type: 9620	Security Code: 65991
Port: IP	BCC: 0
Name: Engage Virtual 1	TN: 1
	COR: 1
	COS: 1
	Tests: y
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 65991
Display Language: english	Mute Button Enabled? y
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
	Customizable Labels? Y

Repeat this section to administer the desired number of virtual IP softphones, using sequential extension numbers. 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 65991 count 2
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
65991	S00081	Engage Virtual 1				1			
	9620		no			1			
65992	S00084	Engage Virtual 2				1			
	9620		no			1			

6. Configure Avaya Aura® Application Enablement Services

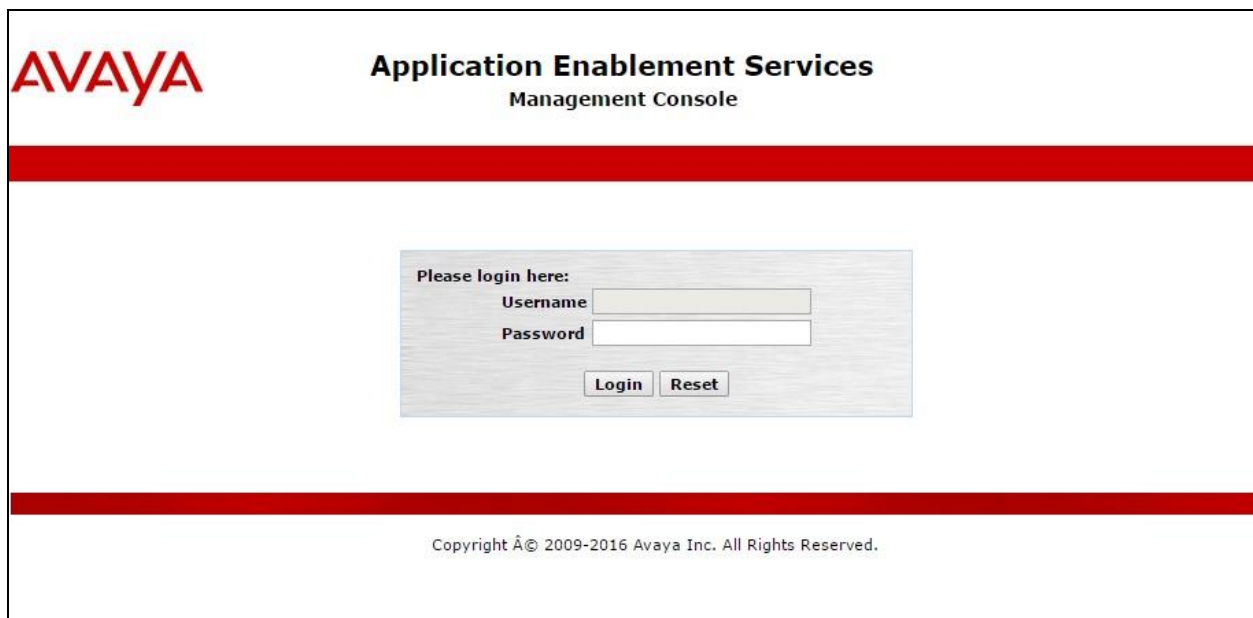
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

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 light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2016 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 displays user information: "Welcome: User", "Last login: Wed Sep 25 07:05:50 2019 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes15019/10.64.150.19", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.1.3.3.0.2-0", "Server Date and Time: Wed Sep 25 08:13:48 MDT 2019", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home", "Help", and "Logout" links. The left sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area displays the "Welcome to OAM" message, stating that the OAM Web provides tools for managing the AE Server and lists the administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these 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 applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The top header and "Welcome" message are the same as in the previous screenshot. The red navigation bar now shows "Licensing" as the active page. The left sidebar highlights "Licensing" and shows sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area displays the "Licensing" page, which provides instructions for setting up and maintaining the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

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 **Device Media and Call Control** and **TSAPI Simultaneous Users** as shown below. Note that the DMCC license is used for virtual IP softphones, and that the TSAPI license is used for device monitoring and call control.

AVAYA
Aura® System Manager 7.1

Last Logged on at September 2019 4:46
Go... Log off

Home User Management * Session Manager * Routing * Licenses *

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
ASBCE
►Session_Border_Controller_E_AE
CE
►COLLABORATION_ENVIRONMENT
COMMUNICATION_MANAGER
►Call_Center
►Communication_Manager
PRESENCE_SERVICES
►Presence_Services
SYSTEM_MANAGER
►System_Manager
SessionManager
►SessionManager
Utility_Services
►Utility_Services
Uninstall license
Server properties

Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard**

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: August 22, 2017 4:03:37 PM +00:00

License File Host IDs: VB-C3-E3-82-7B-BD-01

Licensed Features

13 Items Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	16
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	16
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. 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 sidebar contains a navigation tree with "AE Services" expanded, showing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", and "TSAPI Properties". The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "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 "cm15014" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left sidebar is the same as the previous screenshot. The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (dropdown menu with value "1"), "Switch Connection" (dropdown menu with value "cm15014"), "Switch CTI Link Number" (dropdown menu with value "1"), "ASAI Link Version" (dropdown menu with value "8"), and "Security" (dropdown menu with value "Unencrypted"). Below the form are buttons for "Apply Changes" and "Cancel Changes".

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 “cm15014”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, 'Application Enablement Services Management Console', and a welcome message for the user. The left navigation pane shows 'Communication Manager Interface' expanded, with 'Switch Connections' selected. The main content area displays the 'Switch Connections' table with one entry, 'cm15014', which is selected. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm15014	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.150.14” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm15014' screen. The left navigation pane is the same as the previous screenshot. The main content area has a title 'Edit H.323 Gatekeeper - cm15014' and a text input field containing '10.64.150.14'. Below the input field are buttons for 'Add Name or IP', 'Delete IP', and 'Back'.

6.5. 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Sep 25 07:05:50 2019 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.3.0.2-0
Server Date and Time: Wed Sep 25 08:13:48 MDT 2019
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 Idengage

* Common Nameengage

* Surnameengage

* 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

6.6. Administer 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. Make certain that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Engage user from **Section 6.5**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Wed Sep 25 07:05:50 2019 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes15019/10.64.150.19", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.1.3.3.0.2-0", "Server Date and Time: Wed Sep 25 08:13:48 MDT 2019", and "HA Status: Not Configured".

The main navigation bar is red and contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various management categories: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), 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 checkboxes is an "Apply Changes" button.

6.8. 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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Sep 25 07:05:50 2019 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.3.0.2-0
Server Date and Time: Wed Sep 25 08:13:48 MDT 2019
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

6.9. 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#CM15014#CSTA#AES15019”. Note the use of the switch connection “CM15014” 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 and the title "Application Enablement Services Management Console". A welcome message for the user is shown in the top right corner, including login details and system status. The main navigation bar at the top contains links for "Security", "Security Database", and "Tlinks", along with "Home", "Help", and "Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM15014#CSTA#AES15019" with a "Delete Tlink" button.

Welcome: User
Last login: Wed Sep 25 07:05:50 2019 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.3.0.2-0
Server Date and Time: Wed Sep 25 08:13:48 MDT 2019
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#CM15014#CSTA#AES15019
Delete Tlink

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

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

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is

User ID:

Password:

[Change Password](#)

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.

AVAYA
Aura® System Manager 7.1

Last Logged on at September 24, 2019 4:46 PM
Go... Log off

Home User Management Session Manager Routing Licenses

User Management
Manage Users
Public Contacts
Shared Addresses
System Presence ACLs
Communication Profile
Password Policy

Home / Users / User Management / Manage Users

Search

User Management

Users

More Actions [Advanced Search](#)

16 Items Show 15 Filter: Enable

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input type="checkbox"/>	53101	Station	53101, Station	53101@avaya.com	53101	
<input checked="" type="checkbox"/>	CM7	SIP2	CM7, SIP2	66002@avaya.com	66002	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab, followed by expanding **CM Endpoint Profile** as shown below.

Click on the **Endpoint Editor** icon.

The screenshot shows the 'User Profile Edit' interface for the user '66002@avaya.com'. The left sidebar contains a 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', 'Communication Profile', and 'Password Policy'. The main content area has a breadcrumb trail 'Home / Users / User Management / Manage Users' and a 'Help ?' link. The 'Communication Profile' tab is selected, showing a 'Communication Profile Password' field and an 'Edit' link. Below this is a 'Name' section with a 'Primary' radio button and a 'Select : None' dropdown. The 'Communication Address' section contains a table with one entry: 'Avaya SIP' with handle '66002' and domain 'avaya.com'. The 'Session Manager Profile' is checked, 'Avaya Breeze Profile' is unchecked, and 'CM Endpoint Profile' is checked. Under 'CM Endpoint Profile', the 'System' is 'cm15014', 'Profile Type' is 'Endpoint', and 'Use Existing Endpoints' is unchecked. The 'Extension' is '66002', and the 'Endpoint Editor' button is highlighted with a red box.

User Profile Edit: 66002@avaya.com [Commit & Continue](#) [Commit](#) [Cancel](#)

Identity * **Communication Profile** **Membership** **Contacts**

Communication Profile ▾

Communication Profile Password: [Edit](#)

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name

☒ Primary

Select : None

* Name:

Default : ☒

Communication Address ▾

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	avaya.com

Select : All, None

☒ **Session Manager Profile** ▾

☐ **Avaya Breeze Profile** ▾

☒ **CM Endpoint Profile** ▾

* System:

* Profile Type:

Use Existing Endpoints: ☐

Display Extension Ranges

* Extension: [Endpoint Editor](#)

In the updated screen, locate the **Type of 3PCC Enabled** parameter and select “Avaya” from the drop-down list as shown below. Retain the existing values in the remaining fields.

Repeat this section to configure all SIP agents from **Section 3**.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'User Management', 'Session Manager', 'Routing', and 'Licenses'. The left sidebar lists 'User Management' options: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', 'Communication Profile', and 'Password Policy'. The main content area is titled 'Edit Endpoint' and contains the following fields:

System	cm15014	Extension	66002
Template	9611SIPCC_DEFAULT_CM_7_1	Set Type	9611SIPCC
Port	S00061	Security Code	
Name	CM7, SIP2		

Below these fields are several tabs: 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The 'General Options (G)' tab is active and contains the following settings:

Enhanced Call Fwd (E)	Button Assignment (B)	Profile Settings (P)	Group Membership (M)
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	CM7, SIP2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

A red box highlights the 'Type of 3PCC Enabled' dropdown menu, which is currently set to 'Avaya'. At the bottom left, there is a legend: '* Required'. At the bottom right, there are 'Done' and 'Cancel' buttons.

8. Configure Avaya 9600 Series IP Deskphones

This section provides the procedures for configuring 9600 Series IP Deskphones. The procedures include the following areas:


- Administer phone parameters
- Reboot telephones

8.1. Administer Phone Parameters

From the file server serving the 9600 Series IP Deskphones, locate and open the **46xxsettings.txt** file. Navigate to the relevant phone parameters sub-section, in this case **SETTINGS9611** (not shown).

Under the **WMLIDLEURI** sub-section, set **PUSHCAP**, **TPSLIST**, **SUBSCRIBELIST**, and **WMLHOME** parameters as shown below, where “10.64.101.206” is the IP address of the Engage server running the Web server component.

Repeat this section for all relevant 9600 Series IP Deskphone types. In the compliance testing, the **SETTINGS9611** and **SETTINGS9641** sub-sections were configured, to correspond to the 9611G and 9641G IP Deskphones used by agents for activation/deactivation of recording options.



```
##
## 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 PUSHCAP 2222
SET TPSLIST 10.64.101.206
SET SUBSCRIBELIST http://10.64.101.206/EngageOnDemandAvayaPhoneServices/TelStratSubscribe.aspx
SET WMLHOME http://10.64.101.206/EngageOnDemandAvayaPhoneServices/TelStrat.aspx

##### End of 9611 model-specific settings #####
GOTO GROUP_SETTINGS
```

8.2. Reboot Telephones

After the Engage server has been configured in **Section 9**, manually reboot the 9600 Series IP Deskphones to pick up the new phone settings.

9. Configure TelStrat Engage

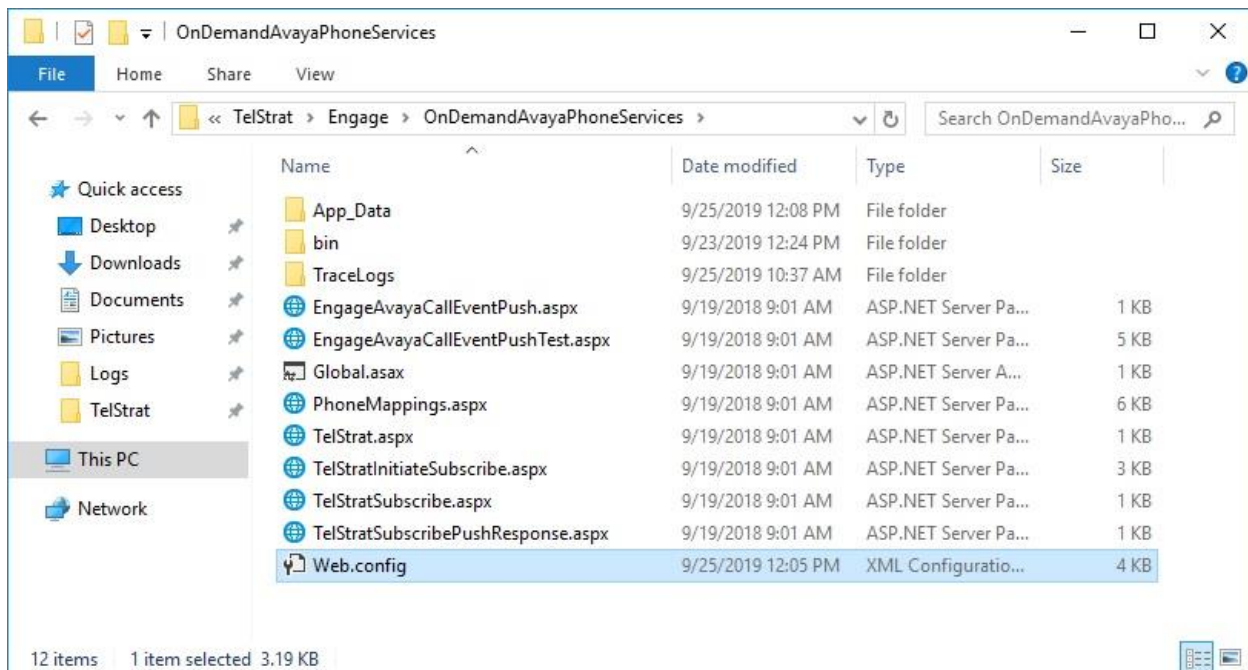
This section provides the procedures for configuring Engage. The procedures include the following areas:

- Administer Web.config
- Launch VoIP engine
- Administer CTI
- Administer OnDemand
- Administer ACD groups
- Administer softphones
- Administer device port mappings
- Restart service

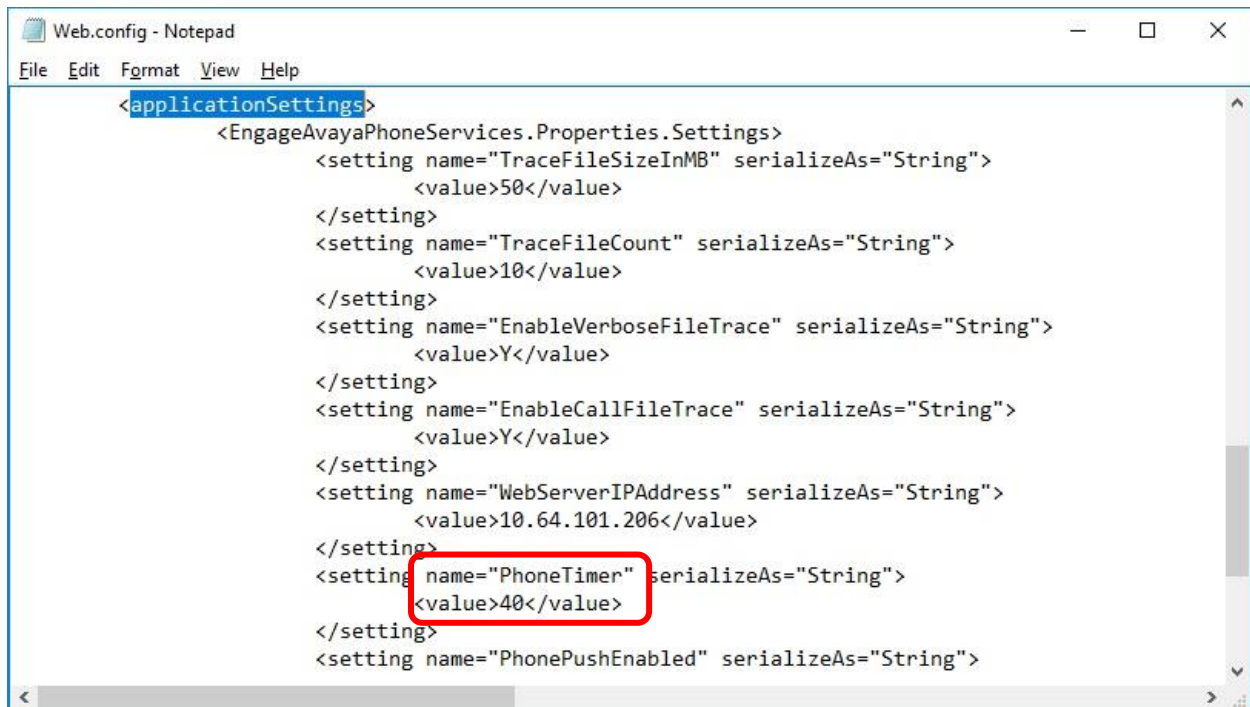
This section assumes the TSAPI client is already installed on the Engage server along with the IP address of the Application Enablement Services server configured as part of the installation, and that the on-demand recording schedule has already been configured.

9.1. Administer Web.config

From the Engage server, navigate to the **C:\Program Files (x86)\TelStrat\Engage\OnDemandAvayaPhoneServices** directory to locate the **Web.config** file shown below.



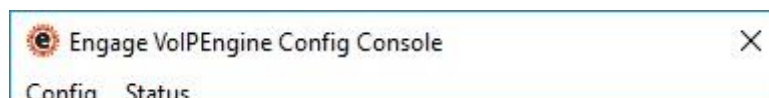
Open the **Web.config** file with the desired application. Scroll down to the **applicationSettings** sub-section. For **PhoneTimer**, enter the desired value. In the compliance testing, the default **30** was changed to **40**, which corresponded to a refresh rate of 4 seconds for the phone display.



```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <applicationSettings>
    <EngageAvayaPhoneServices.Properties.Settings>
      <setting name="TraceFileSizeInMB" serializeAs="String">
        <value>50</value>
      </setting>
      <setting name="TraceFileCount" serializeAs="String">
        <value>10</value>
      </setting>
      <setting name="EnableVerboseFileTrace" serializeAs="String">
        <value>Y</value>
      </setting>
      <setting name="EnableCallFileTrace" serializeAs="String">
        <value>Y</value>
      </setting>
      <setting name="WebServerIPAddress" serializeAs="String">
        <value>10.64.101.206</value>
      </setting>
      <setting name="PhoneTimer" serializeAs="String">
        <value>40</value>
      </setting>
      <setting name="PhonePushEnabled" serializeAs="String">
        <value>Y</value>
      </setting>
    </EngageAvayaPhoneServices.Properties.Settings>
  </applicationSettings>
</configuration>
```

9.2. Launch VoIP Engine

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



9.3. Administer CTI

The **VoIP Configuration** screen is displayed, along with the **Avaya ACM** tab, as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **CTI Option:** “Avaya ACM”
- **AES Server:** The IP address of the Application Enablement Services server.
- **DMCC Port:** The unencrypted DMCC server port from **Section 6.7**.
- **TSAPI APP ID:** The Tlink name from **Section 6.9**.
- **User ID:** The Engage user credentials from **Section 6.5**.
- **Password:** The Engage user credentials from **Section 6.5**.

The screenshot shows the 'VoIP Configuration' window with the 'Avaya ACM' tab selected. The fields are populated as follows:

- CTI Option:** Avaya ACM (dropdown)
- AES Server:** 10.64.150.19
- DMCC Port:** 4721
- TSAPI APP ID:** AVAYA#CM15014#
- Recording Board ID:** 2300
- User ID:** engage
- Password:** (masked with asterisks)

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

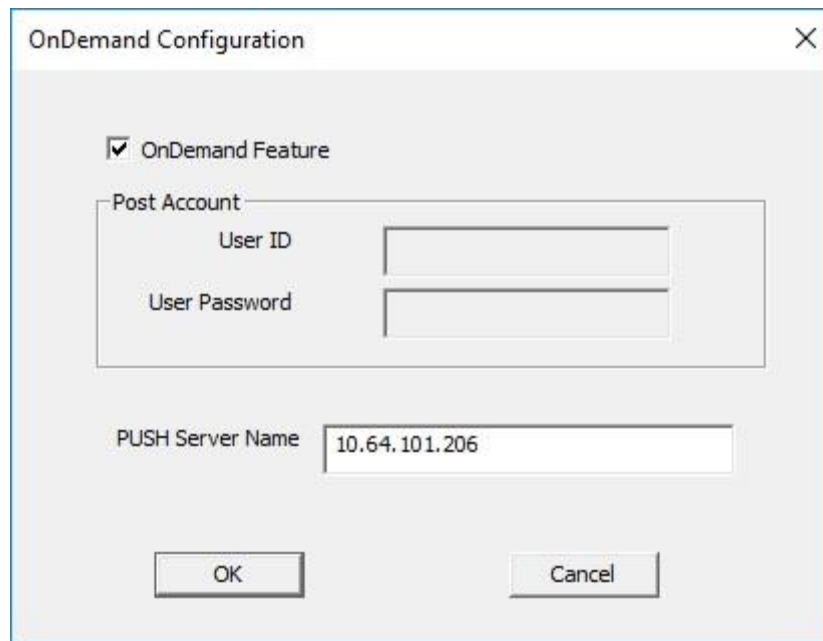
The 'Port Mapping' section contains a table with the following headers:

Recording Channel	Device ID	Mac Address	DN	Record With
-------------------	-----------	-------------	----	-------------

9.4. Administer OnDemand

From the **VoIP Configuration** screen shown in **Section 9.3**, click on **OnDemand** to display the **OnDemand Configuration** screen below.

Check **OnDemand Feature**. For **PUSH Server Name**, enter the IP address of the Engage server, as shown below.

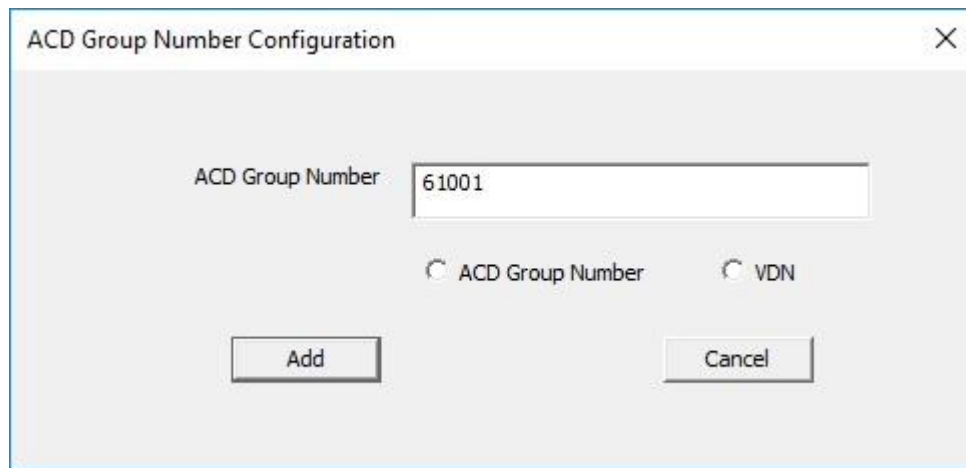


The image shows a dialog box titled "OnDemand Configuration" with a close button (X) in the top right corner. Inside the dialog, there is a checkbox labeled "OnDemand Feature" which is checked. Below this, there is a section titled "Post Account" containing two input fields: "User ID" and "User Password". Below the "Post Account" section, there is a label "PUSH Server Name" followed by an input field containing the IP address "10.64.101.206". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

9.5. Administer ACD Groups

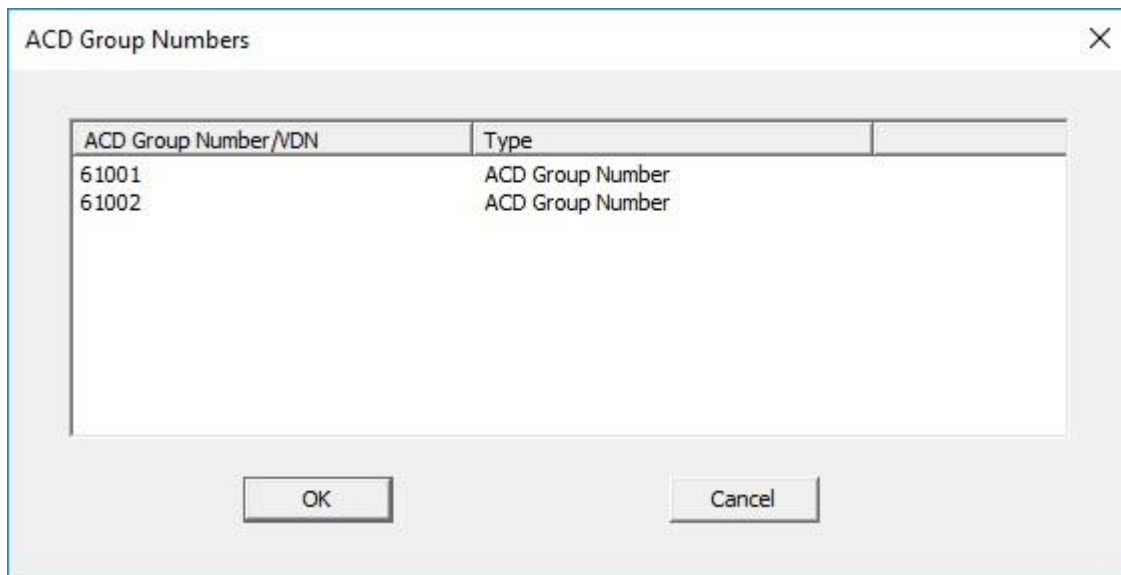
From the **VoIP Configuration** screen shown in **Section 9.3**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

The **ACD Group Number Configuration** screen is displayed next. Enter the first skill group extension from **Section 3**, in this case “61001”.



The dialog box titled "ACD Group Number Configuration" contains a text input field labeled "ACD Group Number" with the value "61001". Below the input field are two radio buttons: "ACD Group Number" (which is selected) and "VDN". At the bottom of the dialog 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 dialog box titled "ACD Group Numbers" displays a table with two columns: "ACD Group Number/VDN" and "Type". The table contains two rows of data. Below the table are two buttons: "OK" and "Cancel".

ACD Group Number/VDN	Type
61001	ACD Group Number
61002	ACD Group Number

9.6. Administer Softphones

From the **VoIP Configuration** screen shown in **Section 9.3**, click on **SoftPhone** to display the **Softphone Station Configuration** screen below.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **CMServer:** The IP address of the H.323 gatekeeper from **Section 6.4**.
- **From:** The extension of the first virtual IP softphone from **Section 5.3**.
- **To:** The extension of the last virtual IP softphone from **Section 5.3**.



The image shows a 'SoftPhone Station Configuration' dialog box with a close button (X) in the top right corner. It contains several input fields and two buttons at the bottom.

Field Label	Value
Certificate Name	
Service Observe Access Code	
CM Server	10.64.101.14
From	65991
To	65992
SoftPhone Station IP	10.64.101.206

Buttons: OK, Cancel

9.7. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 9.3**, right-click in the empty bottom 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**.

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 received dialed number can contain 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 **Recording Channel**, enter an available port, which begins with “0”. Retain the default values in the remaining fields.

Device And CommSrv Port Mapping

Device ID: 65001

MAC:

DN: 65001

Recording Channel: 0

Calls To Record

☐ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream

☐ Mirroring

☒ STC Stream Warning Tone: Inherited

☐ HotDesk DN

Add Cancel

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

In the compliance testing, one entry was created for each agent as shown below.

VoIP Configuration

Avaya ACM

CTI Option: Avaya ACM

AES Server: 10.64.150.19

DMCC Port: 4721

TSAPI APP ID: AVAYA#CM15014#

Recording Board ID: 2300

User ID: engage

Password: XXXXXXXXX

Calls To Record:

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

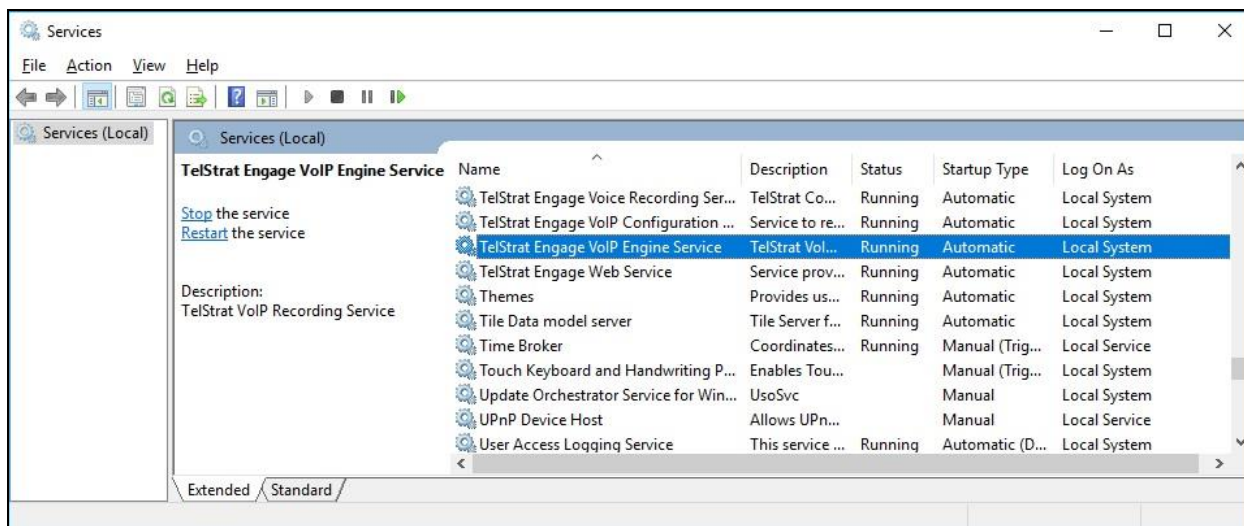
Buttons: SoftPhone, OnDemand, More, ACD Groups

Port Mapping

Recording Channel	Device ID	Mac Address	DN	Record With
000	65001		65001	STC Stream
001	66002		66002	STC Stream

9.8. Restart Service

Select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Restart the **TelStrat Engage VoIP Engine Service** shown below.



10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, 9600 Series IP Deskphones, and Engage.

10.1. 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	8	no	aes15019	established	43	46

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 5.3** 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		
65000	1616	IP_Phone	y	192.168.200.142		
	1	1.3120		10.64.150.14		
65001	9641	IP_Phone	y	192.168.200.143		
	1	6.8202		10.64.150.14		
65991	9620	IP_API_A	y	10.64.150.19		
	1	3.2040		10.64.150.14		
65992	9620	IP_API_A	y	10.64.150.19		
	1	3.2040		10.64.150.14		

10.2. 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**.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Thu Sep 26 06:53:21 2019 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes15019/10.64.150.19
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.3.3.0.2-0
Server Date and Time: Thu Sep 26 07:01:33 MDT 2019
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ 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 checked="" type="radio"/>	1	cm15014	1	Talking	Thu Sep 19 15:35:28 2019	Online	17	4	17	29	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 Engage user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the total number of softphone extensions from **Section 9.6**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Thu Sep 26 06:53:21 2019 from 192.168.200.20
 Number of prior failed login attempts: 0
 HostName/IP: aes15019/10.64.150.19
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.1.3.3.0.2-0
 Server Date and Time: Thu Sep 26 07:00:42 MDT 2019
 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
 - ▶ Logs
 - ▶ Log Manager
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - **DMCC Service Summary**
 - Switch Conn Summary
 - TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every seconds

Session Summary [Device Summary](#)
 Generated on Thu Sep 26 06:59:57 MDT 2019

Service Uptime: 6 days, 15 hours 23 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 50709

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	E44B0B23C86494656 FC630DA7A0E1E90-11	engage	Engage	10.64.101.206	XML Unencrypted	2

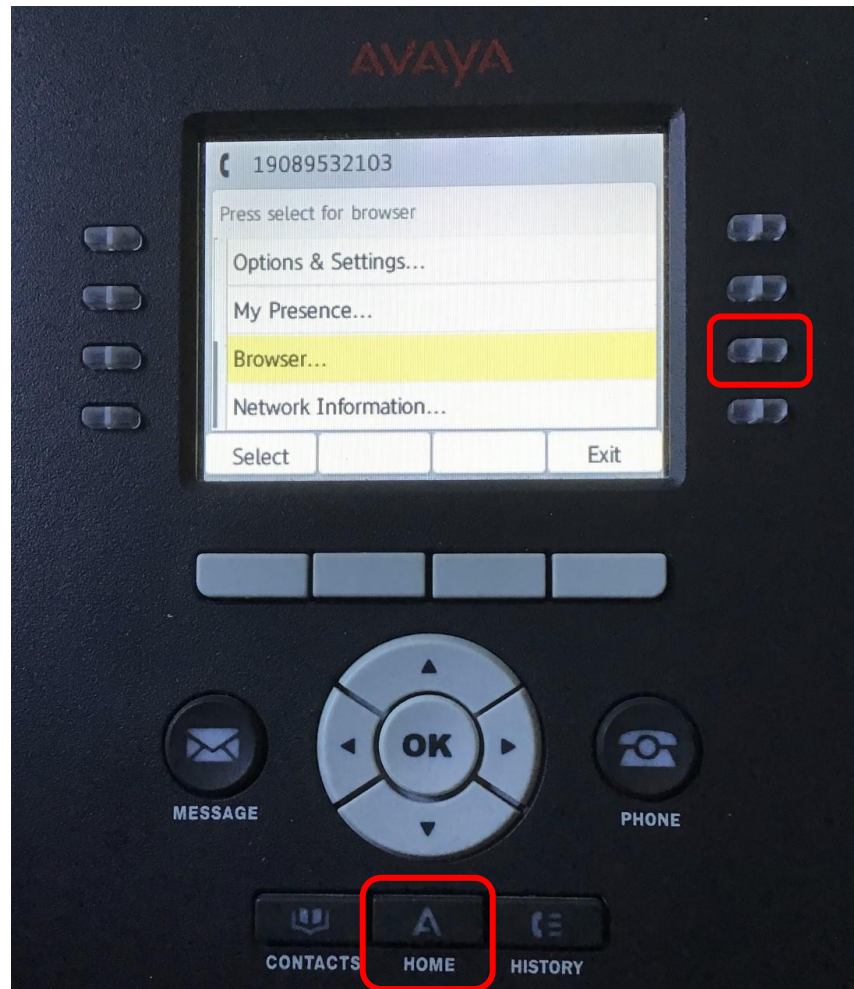
Item 1-1 of 1
 Go

10.3. Verify Avaya 9600 Series IP Deskphones

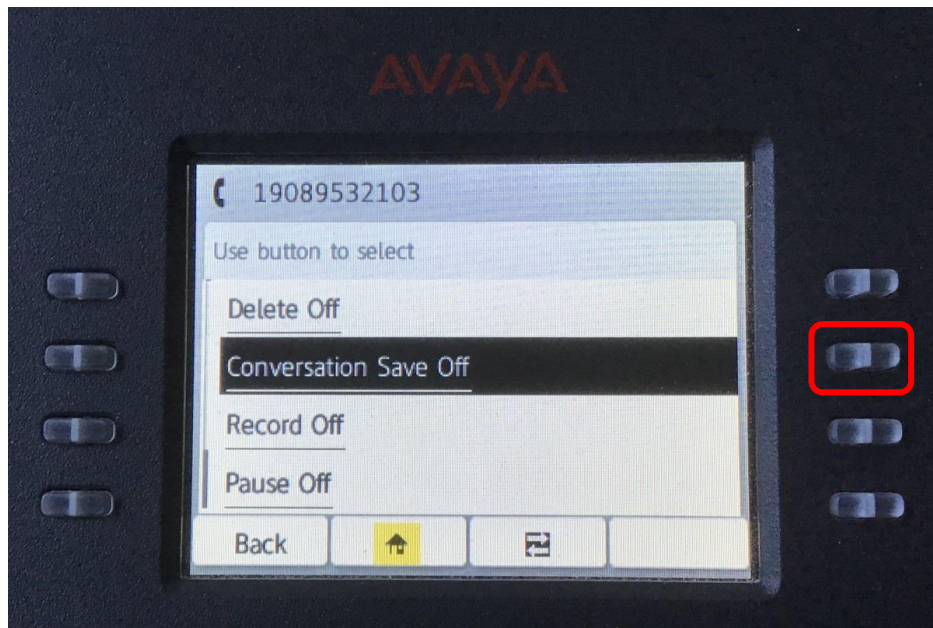
Log an agent into the skill group to answer an ACD call.

From the agent's 9600 Series IP Deskphone, press the **HOME** key to display the screen below. Verify that the **Browser** option is included in the listing, as shown below on a 9611G IP Deskphone running the SIP firmware.

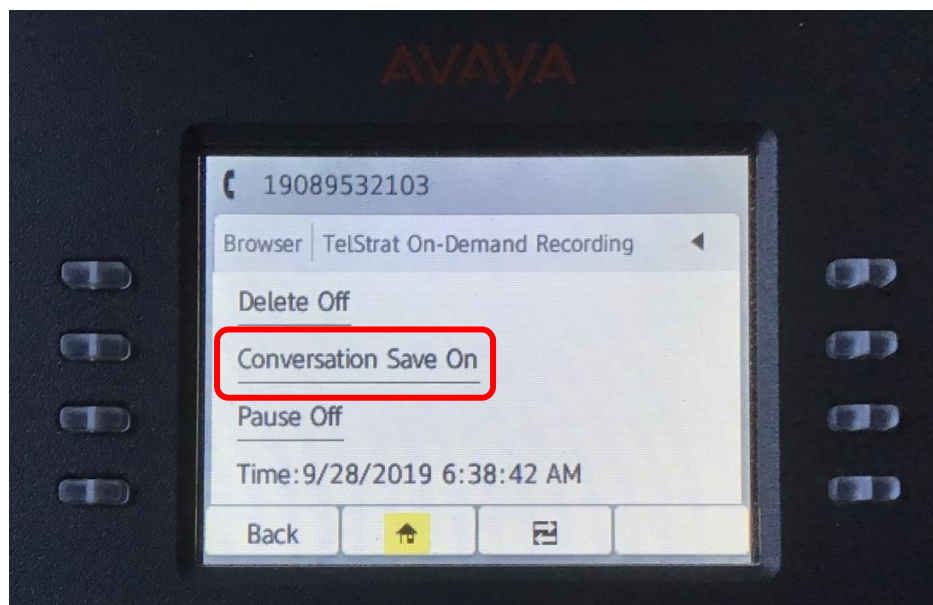
Use the navigational keys or the key to the right of the **Browser** option to select the option.



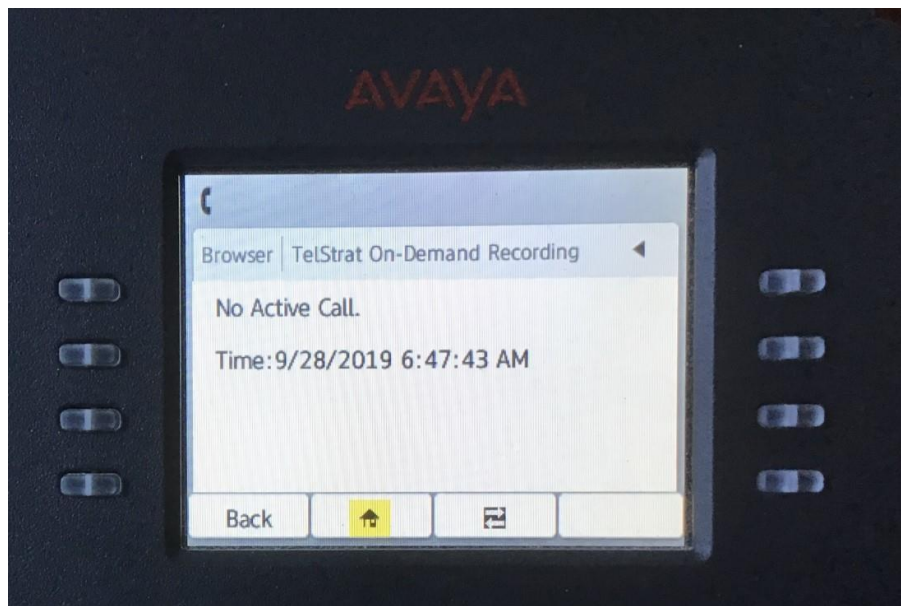
Verify that a list of recording options is displayed as shown below. Use the navigational keys or the key to the right of the **Conversation Save Off** option to select the option.



Verify that the display is updated to show **Conversation Save On**, which is indication that the current conversation will be saved.



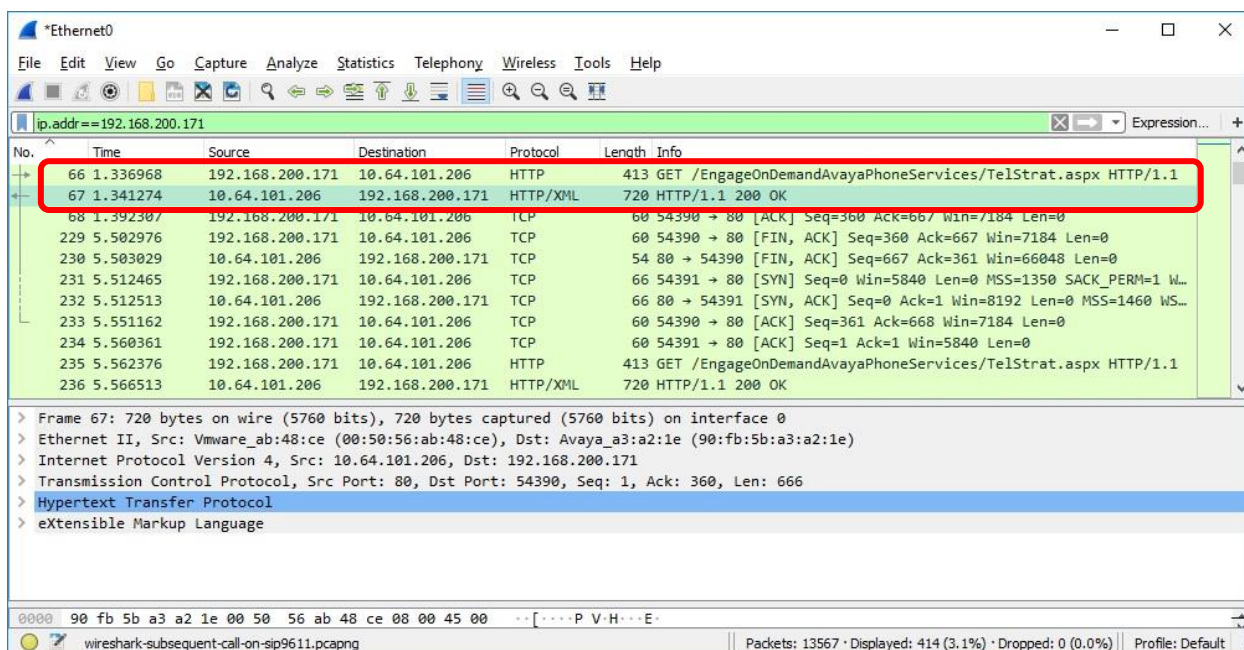
Complete the ACD call. Verify that the display is updated to **No Active Call** as shown below.



10.4. Verify TelStrat Engage

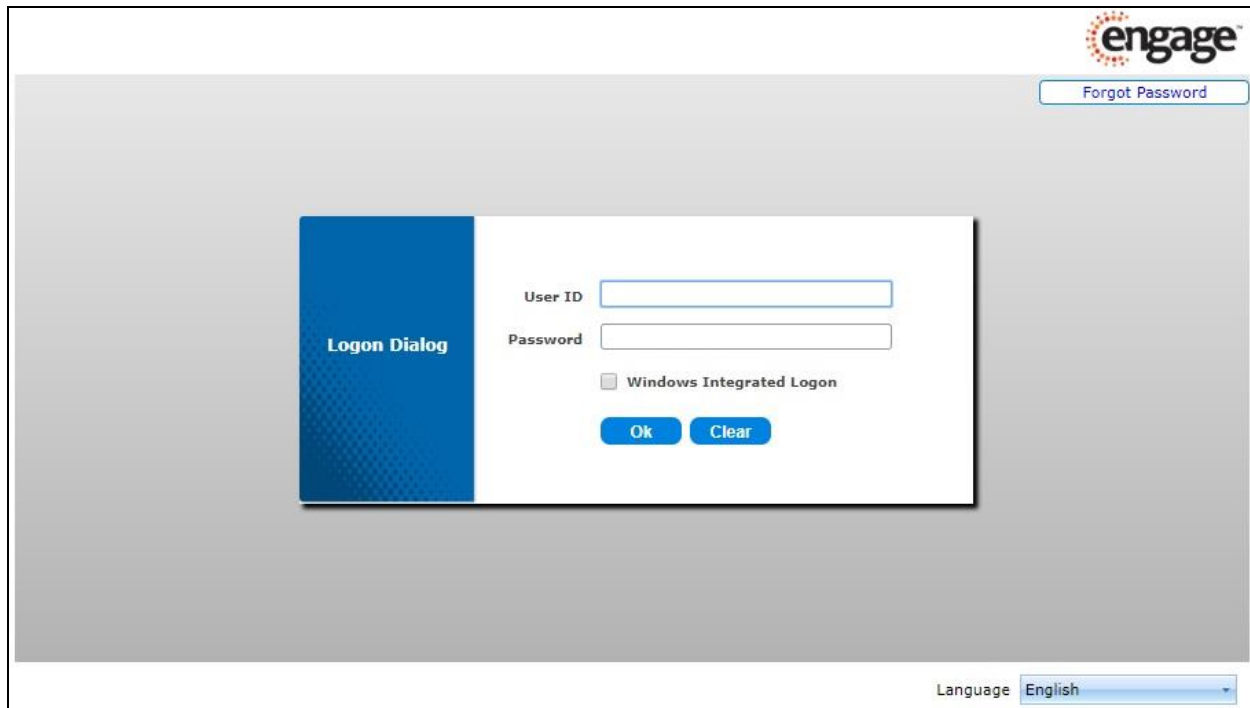
While there is an active call at the agent, use the Wireshark application to capture exchanges between Engage and the agent phone. Note that web page with aspx extension is not explicitly supported by Avaya and can be supported only if returns strictly WML/XML as content.

Verify that the Engage response associated with the aspx web page HTTP GET request from the phone contained XML content, as shown below in the **Protocol** column with “HTTP/XML”.



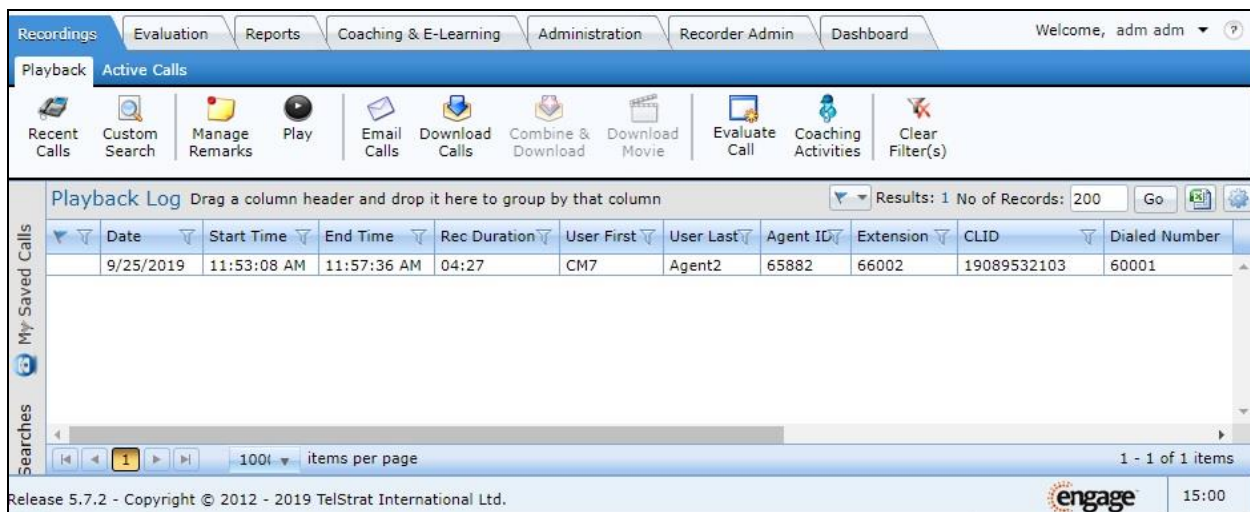
Complete the active ACD call. Access the Engage web-based interface by using the URL “http://ip-address/engage” in an Internet browser window, where “ip-address” is the IP address of the Engage server.

The **Logon Dialog** screen below is displayed. Log in using the appropriate credentials.



The screenshot shows the Engage web-based interface's logon dialog. The Engage logo is in the top right corner. Below it is a "Forgot Password" link. The main area features a "Logon Dialog" window with a blue header. Inside the dialog, there are input fields for "User ID" and "Password". Below these fields is a checkbox labeled "Windows Integrated Logon". At the bottom of the dialog are "Ok" and "Clear" buttons. In the bottom right corner of the main interface, there is a "Language" dropdown menu set to "English".

The screen is updated with a list of call recordings. Verify that there is an entry reflecting the ACD call with the agent, with proper values in the relevant fields.



The screenshot shows the Engage Playback Log screen. The top navigation bar includes tabs for Recordings, Evaluation, Reports, Coaching & E-Learning, Administration, Recorder Admin, and Dashboard. The user is logged in as "adm adm". Below the navigation bar is a toolbar with icons for Recent Calls, Custom Search, Manage Remarks, Play, Email Calls, Download Calls, Combine & Download, Download Movie, Evaluate Call, Coaching Activities, and Clear Filter(s). The main area displays a "Playback Log" table with columns: Date, Start Time, End Time, Rec Duration, User First, User Last, Agent ID, Extension, CLID, and Dialed Number. The table shows one record for a call on 9/25/2019. The bottom of the screen shows a footer with "Release 5.7.2 - Copyright © 2012 - 2019 TelStrat International Ltd.", the Engage logo, and the time "15:00".

Date	Start Time	End Time	Rec Duration	User First	User Last	Agent ID	Extension	CLID	Dialed Number
9/25/2019	11:53:08 AM	11:57:36 AM	04:27	CM7	Agent2	65882	66002	19089532103	60001

Double click on the entry and verify that the call recording can be played back.

The screenshot displays the Engage Recorder Admin web application. The top navigation bar includes tabs for Recordings, Evaluation, Reports, Coaching & E-Learning, Administration, Recorder Admin, and Dashboard. The user is logged in as 'adm adm'. The 'Playback' section is active, showing a 'Playback Log' table with columns: Date, Start Time, End Time, Rec Duration, User First, User Last, Agent ID, Extension, CLID, and Dialed Number. A single record is shown for 9/25/2019, 11:53:08 AM to 11:57:36 AM, with a duration of 04:27. Below the table is a media player for the selected call. The call started at 9/25/2019, 11:53:08 AM. The media player shows a waveform and a progress bar. The call ID is 1909251153086DU2300001. The bottom of the page shows the Engage logo and the text 'Release 5.7.2 - Copyright © 2012 - 2019 TelStrat International Ltd.' and '15:01'.

Date	Start Time	End Time	Rec Duration	User First	User Last	Agent ID	Extension	CLID	Dialed Number
9/25/2019	11:53:08 AM	11:57:36 AM	04:27	CM7	Agent2	65882	66002	19089532103	60001

Call Start at 9/25/2019, 11:53:08 AM

Call ID: 1909251153086DU2300001

Release 5.7.2 - Copyright © 2012 - 2019 TelStrat International Ltd. engage 15:01

11. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage 5.7 to successfully interoperate with Avaya Aura® Communication Manager 7.1, Avaya Aura® Application Enablement Services 7.1, and Avaya 9600 Series IP Deskphones for on-demand recording. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 8, August 2019, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.3, Issue 6, August 2019, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 5, July 2018, available at <http://support.avaya.com>.
4. *Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.0.1, January 2017, available at <http://support.avaya.com>.
5. *Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, Release 6.8.2, June 2019, available at <http://support.avaya.com>.
6. *Config Guide – Avaya ACM On Demand Recording*, Release 5.7, Issue 1.0, available at <http://esupport.telstrat.com>.
7. *Engage Recorder Administration Guide*, Release 5.7, Issue 1.0, available at <http://esupport.telstrat.com>.

©2019 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.