



Avaya Solution & Interoperability Test Lab

Application Notes for TelStrat Engage 5.2 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using VoIP Recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelStrat Engage 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using VoIP recording. TelStrat Engage is a call recording solution.

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 stations on Avaya Aura® Communication Manager, and the port mirroring method to capture the media associated with the monitored agents for 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 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using VoIP recording. TelStrat Engage is a call recording solution.

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 stations on Avaya Aura® Communication Manager, and the port mirroring method to capture the media associated with the monitored agents with Avaya 9600 Series IP Deskphones for call recording.

The TSAPI interface is used by TelStrat Engage to monitor skill groups and agent stations on Avaya Aura® Communication Manager. When there is an active call at the monitored agent, TelStrat Engage is informed of the call via event reports from the TSAPI interface. TelStrat Engage starts the call recording by using the replicated media from the port mirroring method. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically requested monitoring on skill groups and agent stations and performed device queries using TSAPI.

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. Necessary user actions such as hold and resume 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 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.

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 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, resume, G.711 and G.729 codec, forwarding, service observing, long duration, multiple calls, multiple agents, conference, and transfer.

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:

- In the attended transfer and conference scenarios, the recording for the private conversation between the agent with the transfer-to or conference-to destination is captured in a separate recording entry for the agent by design.
- This release of Engage does not support recording of unparked calls.

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 RTP streams for agents with 9600 Series IP Deskphones were mirrored from the layer 2 switch, and replicated over to Engage.

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 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, Engage monitored the skill groups and agent station extensions shown in the table below.

| Device Type | Extension |
|---------------|--------------|
| VDN | 60001, 60002 |
| Skill Group | 61001, 61002 |
| Supervisor | 65000 |
| Agent ID | 65881, 65882 |
| Agent Station | 65001, 66002 |

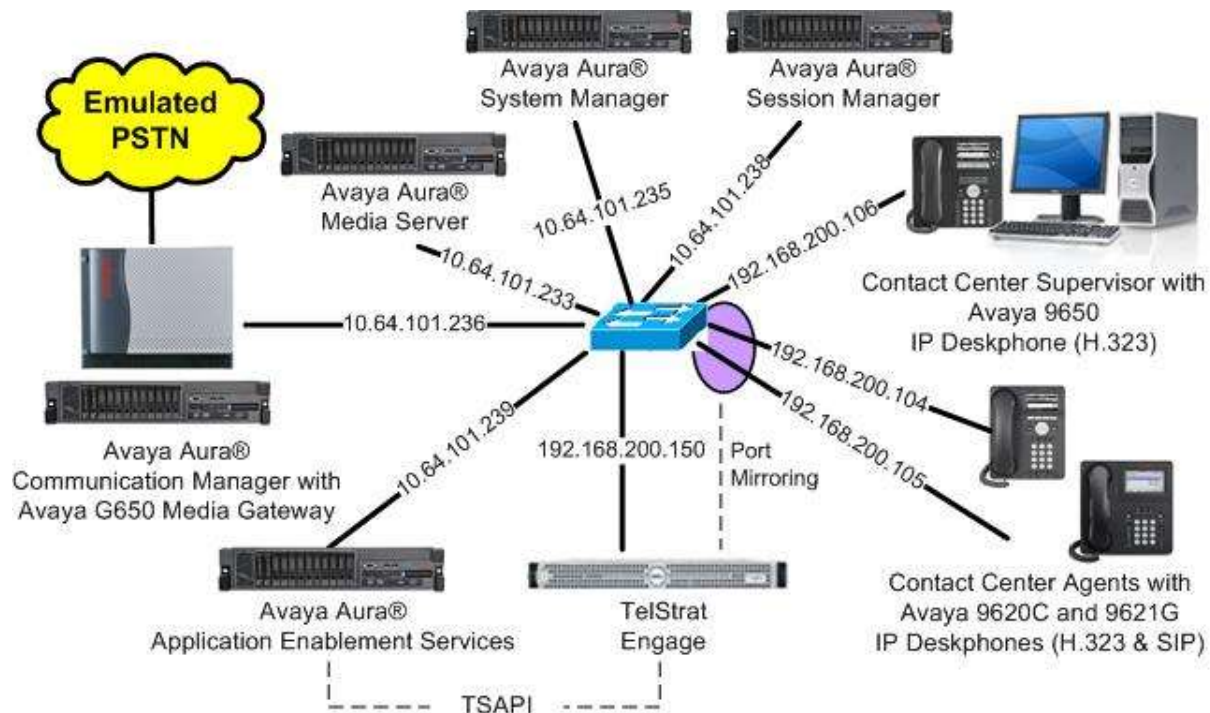


Figure 1: Compliance Testing Configuration

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 | 7.0 SP1 (7.0.0.1.0.441.22477) |
| Avaya G650 Media Gateway | NA |
| Avaya Aura® Media Server in Virtual Environment | 7.7.0.236 |
| Avaya Aura® Application Enablement Services in Virtual Environment | 7.0 Patch 1 (7.0.0.0.1.13) |
| Avaya Aura® Session Manager in Virtual Environment | 7.0 (7.0.0.0.0.700007) |
| Avaya Aura® System Manager in Virtual Environment | 7.0 (7.0.0.0.0.4036) |
| Avaya 9620C & 9650 IP Deskphones (H.323) | 3.250A |
| Avaya 9621G IP Deskphone (SIP) | 7.0.0.39 |
| TelStrat Engage on Windows Server 2008 <ul style="list-style-type: none">• VOIP Engine Module• Microsoft SQL Server 2012• Avaya TSAPI Windows Client (csta32.dll) | 5.2.0.14 R2 Standard 5.2.0.16 11.0.2100.60 7.0.0.131 |

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 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? n | DCS (Basic)? y | |
| ASAI Link Core Capabilities? n | DCS Call Coverage? y | |
| ASAI Link Plus Capabilities? n | DCS with Rerouting? y | |
| Async. Transfer Mode (ATM) PNC? n | | |
| Async. Transfer Mode (ATM) Trunking? n | Digital Loss Plan Modification? y | |
| ATM WAN Spare Processor? n | DS1 MSP? y | |
| 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: 60111 | | |
| Type: ADJ-IP | | |
| | | COR: 1 |
| Name: AES CTI 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
- Administer Engage user
- Disable security database
- Restart TSAPI service
- 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 separates the header from the main content area. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is at the top. Below it are two input fields: "Username" and "Password". At the bottom of the login box are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the very bottom of the page, centered, is the copyright notice: "Copyright © 2009-2015 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for "User" is displayed, including login details and system status. A red navigation bar at the top contains "Home", "Help", and "Logout" links. A left sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the OAM web interface, listing administrative domains and their functions. It also mentions that these domains can be managed by a single administrator or separate ones.

Welcome: User
Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Jan 19 09:24:20 EST 2016
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
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.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- 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 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" section selected in the left sidebar. The main content area is titled "Licensing" and provides instructions on how to set up and maintain the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. The top header and navigation bar are consistent with the previous screenshot.

Welcome: User
Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Jan 19 09:24:20 EST 2016
HA Status: Not Configured

Licensing | Home | Help | Logout

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

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

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

AVAYA
Aura® System Manager 7.0

Last Logged on at January 1, 2016
Log off

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
Application Enablement
View license capacity
View peak usage
COMMUNICATION_MANAGER
Communication Manager
Call Center
Configure Centralized Licensing
MSR
Media Server
SessionManager
SessionManager
Uninstall license
Server properties
Shortcuts
Help for Installed Product

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

You are here: Licensed Products > Application Enablement > View License Capacity

License installed on: October 12, 2015 2:21:49 PM +05:00

License File Host IDs: V1-19-37-80-8F-BF

Licensed Features

10 Items Show All

| Feature (License Keyword) | Expiration date | Licensed capacity |
|--|-----------------|---|
| CVLAN ASA1 VALUE_AES_CVLAN_ASA1 | permanent | 16 |
| Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP | permanent | 1000 |
| AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED | permanent | 3 |
| CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS | permanent | 16 |
| Product Notes VALUE_NOTES | permanent | SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;leptop;Cti5 MediumServerTypes: ibmx306;ibmx306m;del1950;xen;hs20;hs20_1 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; IXP_001, BasicUnrestricted DMCUnrestricted; IXM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CTE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES CCE_001, BasicUnrestricted, AdvancedUnrestrict CS1_T1_001, BasicUnrestricted, AdvancedUnrestrict CS1_T2_001, BasicUnrestricted, AdvancedUnrestrict AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestrict DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestrict AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC |
| AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED | permanent | 3 |
| TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS | permanent | 1000 |
| DLG VALUE_AES_DLG | permanent | 16 |
| Device Media and Call Control VALUE_AES_DMCC_DMC | permanent | 1000 |
| AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED | permanent | 3 |

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 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 includes 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 "cm7" 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 Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. 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. Each field has a dropdown menu. The "Link" field is set to "1", "Switch Connection" is set to "cm7", "Switch CTI Link Number" is set to "1", "ASAI Link Version" is set to "7", and "Security" is set to "Unencrypted". Below the fields are buttons for "Apply Changes" and "Cancel Changes".

6.4. 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: Tue Jan 19 09:23:33 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Jan 19 09:27:57 EST 2016
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

6.5. Disable Security Database

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

In the event that the security database is used by the customer with parameter already enabled, then follow reference [2] to configure access privileges for the Engage user from **Section 6.4**.

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: Tue Jan 19 09:23:33 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Tue Jan 19 09:24:20 EST 2016", 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 service 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.

6.6. Restart TSAPI Service

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Jan 19 09:24:20 EST 2016
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

| 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 |

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.7. Obtain Tlink Name

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

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

Welcome: User
Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Jan 19 09:24:20 EST 2016
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#CM7#CSTA#AES7
Delete Tlink

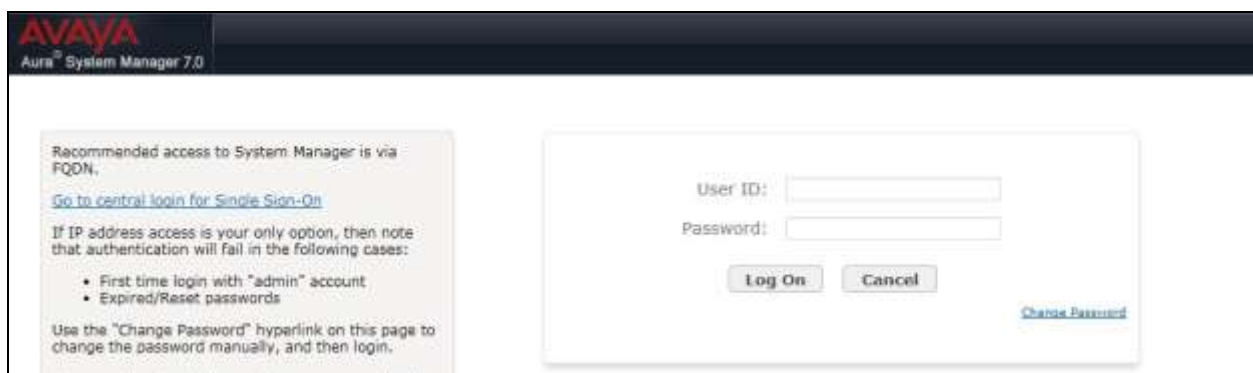
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

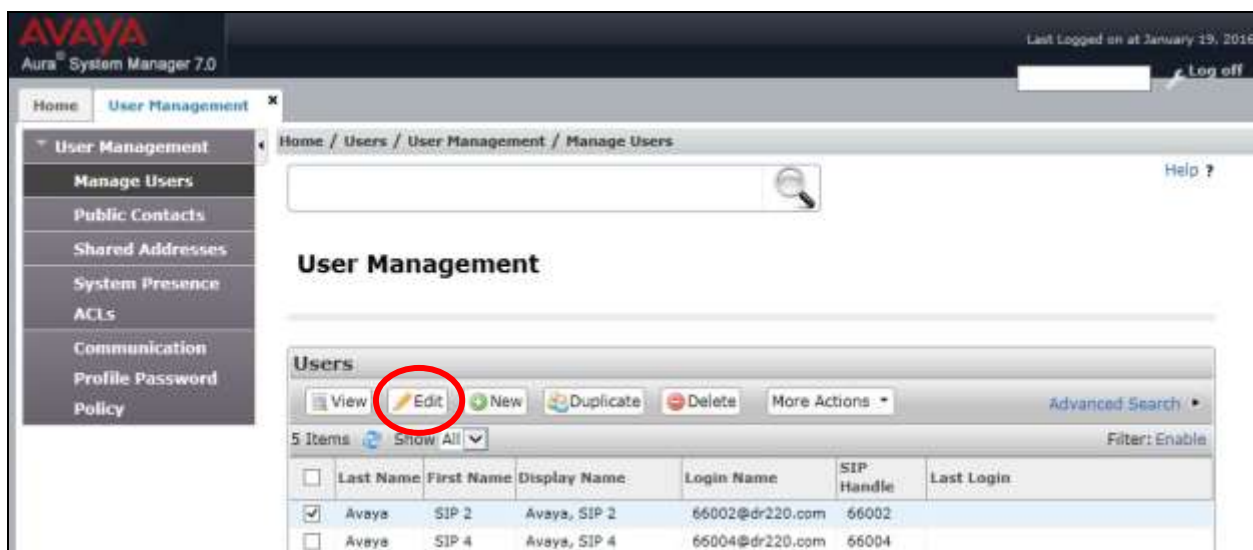
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login page. It features a dark header with the Avaya logo and 'Aura System Manager 7.0'. The main content area has a light background. On the left, there is a text box with instructions: '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.' On the right, there is a login form with fields for 'User ID:' and 'Password:', a 'Log On' button, a 'Cancel' button, and a 'Change Password' link.

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 **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



The screenshot shows the Avaya Aura System Manager 7.0 User Management screen. The header includes the Avaya logo, 'Aura System Manager 7.0', and a 'Log off' button. The left navigation pane has a 'User Management' section with a 'Manage Users' link. The main content area shows the 'User Management' title and a table of users. The 'Edit' button in the table's action bar is circled in red. The table has columns for 'Last Name', 'First Name', 'Display Name', 'Login Name', 'SIP Handle', and 'Last Login'. The first row is selected, showing 'Avaya', 'SIP 2', 'Avaya, SIP 2', '66002@dr220.com', and '66002'.

| | Last Name | First Name | Display Name | Login Name | SIP Handle | Last Login |
|-------------------------------------|-----------|------------|--------------|-----------------|------------|------------|
| <input checked="" type="checkbox"/> | Avaya | SIP 2 | Avaya, SIP 2 | 66002@dr220.com | 66002 | |
| <input type="checkbox"/> | Avaya | SIP 4 | Avaya, SIP 4 | 66004@dr220.com | 66004 | |

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes 'Home' and 'User Management'. The left sidebar lists various management options. The main content area is titled 'User Profile Edit: 66002@dr220.com'. The 'Communication Profile' tab is active, showing fields for 'Name' (Primary) and 'Communication Address' (Avaya SIP, 66002, dr220.com). The 'Session Manager Profile' and 'CM Endpoint Profile' sections are expanded. The 'CM Endpoint Profile' section shows 'System' as DR220-CMG-ES, 'Profile Type' as Endpoint, and 'Extension' as 66002. The 'Endpoint Editor' button is circled in red.

| Type | Handle | Domain |
|------------------------------------|--------|-----------|
| <input type="checkbox"/> Avaya SIP | 66002 | dr220.com |

CM Endpoint Profile

System: DR220-CMG-ES

Profile Type: Endpoint

Extension: 66002

Endpoint Editor

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.

AVAYA
Aura System Manager 7.0

Last Logged in at January 19, 2016 9:32 AM
Log off

Home / User Management / Manage Users

Edit Endpoint

Done Cancel

[Save As Template]

System: DR220-CM7-ES
Extension: 66002
Template: Select
Set Type: 96215PCC
Port: 500004
Security Code:
Name: Avaya, SIP 2

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

* Class of Restriction (COR): 1
* Emergency Location Ext: 66002
* Tenant Number: 1
* SIP Trunk: Q ear
Coverage Path 1: 1
Lock Message: ☐
Multibyte Language: first applicable

* Class Of Service (COS): 1
* Message Lamp Ext.: 66002
Type of 3PCC Enabled: Avaya
Coverage Path 2:
Localized Display Name: Avaya, SIP 2
Enable Reachability for Station Domain Control: system

* Required

Done Cancel

8. Configure Avaya 9600 Series IP Deskphones

This section provides the procedures for obtaining the MAC addresses from the 9600 Series IP Deskphones.

8.1. Obtain MAC Addresses

From the 96xx IP Deskphone, press the **MENU** or **HOME** → **Settings** buttons to display the **Main Menu** screen (not shown).

From the **Main Menu** 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 9600 Series IP Deskphones used by the agents in **Section 3**. In the compliance testing, the MAC addresses associated with the two agent telephones were “001B4F557C69” and “2CF4C5F669AD”.

9. Configure TelStrat Engage

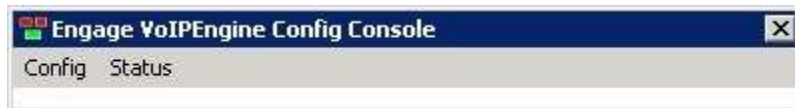
This section provides the procedures for configuring Engage. The procedures include the following areas:

- Launch VoIP engine
- Administer CTI
- Administer ACD groups
- Administer device port mappings

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 TSAPI client installation.

9.1. Launch VoIP Engine

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



9.2. 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.
- **TSAPI APP ID:** The Tlink name from **Section 6.7**.
- **User ID:** The Engage user credentials from **Section 6.4**.
- **Password:** The Engage user credentials from **Section 6.4**.

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

| Field | Value |
|--------------------|---------------|
| CTI Option | Avaya ACM |
| AES Server | 10.64.101.239 |
| DMCC Port | 0 |
| TSAPI APP ID | AVAYA#CM7#CST |
| Recording Board ID | 2300 |
| User ID | engage |
| Password | ***** |

Below the fields, there are two sections:

Calls To Record: Three radio buttons are present: 'All Trunk/Internal Calls' (selected), 'All Trunk Calls', and 'Calls Selected By DN'.

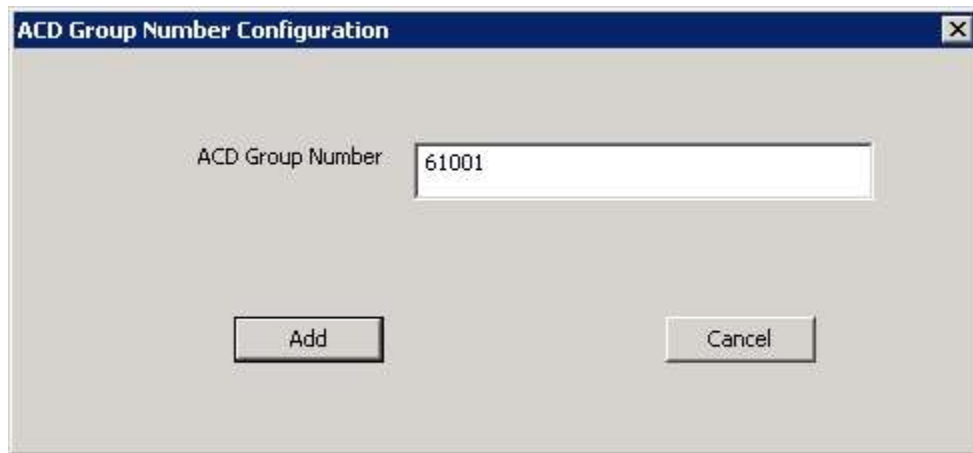
Port Mapping: A table with the following columns: Recording Channel, Device..., Mac Address, DN, Record With, and Trunk/Internal Calls. The table is currently empty.

On the right side of the 'Calls To Record' section, there are four buttons: 'SoftPhone', 'OnDemand', 'More', and 'ACD Groups'.

9.3. Administer ACD Groups

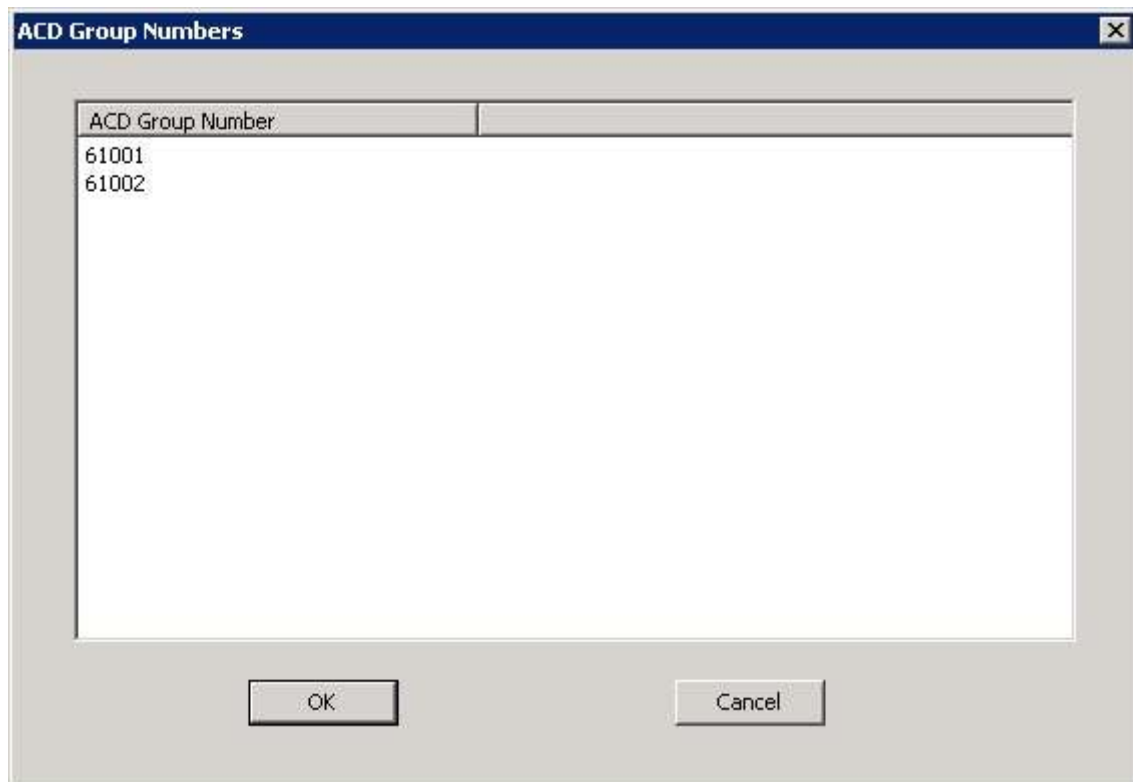
From the **VoIP Configuration** screen shown in **Section 9.2**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

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 "61001". 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 |
|------------------|
| 61001 |
| 61002 |

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

9.4. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 9.2**, 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**. Select the **Mirroring** radio button to enable the **MAC** field. For **MAC**, enter the MAC address of the first agent telephone from **Section 8.1**.

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 **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: 001B4F557C69

DN: 65001

Recording Channel: 0

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

Recording Stream:
☒ Mirroring ☐ STC Stream

Beep Tone: No

☐ HotDesk DN

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 “30353”, as shown below.

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

- CTI Option: Avaya ACM (dropdown)
- AES Server: 10.64.101.239
- DMCC Port: 0
- TSAPI APP ID: AVAYA#CM7#CST
- Recording Board ID: 2300
- User ID: engage
- Password: (masked with asterisks)

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

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

| | Recording Channel | Device... | Mac Address | DN | Record With | Trunk/Internal Calls |
|-----|-------------------|-----------|--------------|------------|-------------|----------------------|
| 000 | | 65001 | 001B4F557C69 | 65001 | Mirroring | Trunk/Internal |
| 000 | | 65001 | 001B4F557C69 | 3035365001 | Mirroring | Trunk/Internal |
| 001 | | 66002 | 2CF4C5F669AD | 66002 | Mirroring | Trunk/Internal |
| 001 | | 66002 | 2CF4C5F669AD | 3035366002 | Mirroring | Trunk/Internal |

At the bottom, there are fields for 'No. of Log Files' (set to 8), 'Config File Location', 'Other Parameters', and 'OK'/'Cancel' buttons.

10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, 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 | 7 | no | aes7 | established | 45 | 47 |

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 (not shown). The **TSAPI Link Details** screen is displayed.

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

**Application Enablement Services**
Management Console

Welcome: User
Last login: Thu Jan 21 10:16:46 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.1.13
Server Date and Time: Thu Jan 21 12:43:34 EST 2016
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

TSAPI Link Details

☐ Enable page refresh every 60 seconds

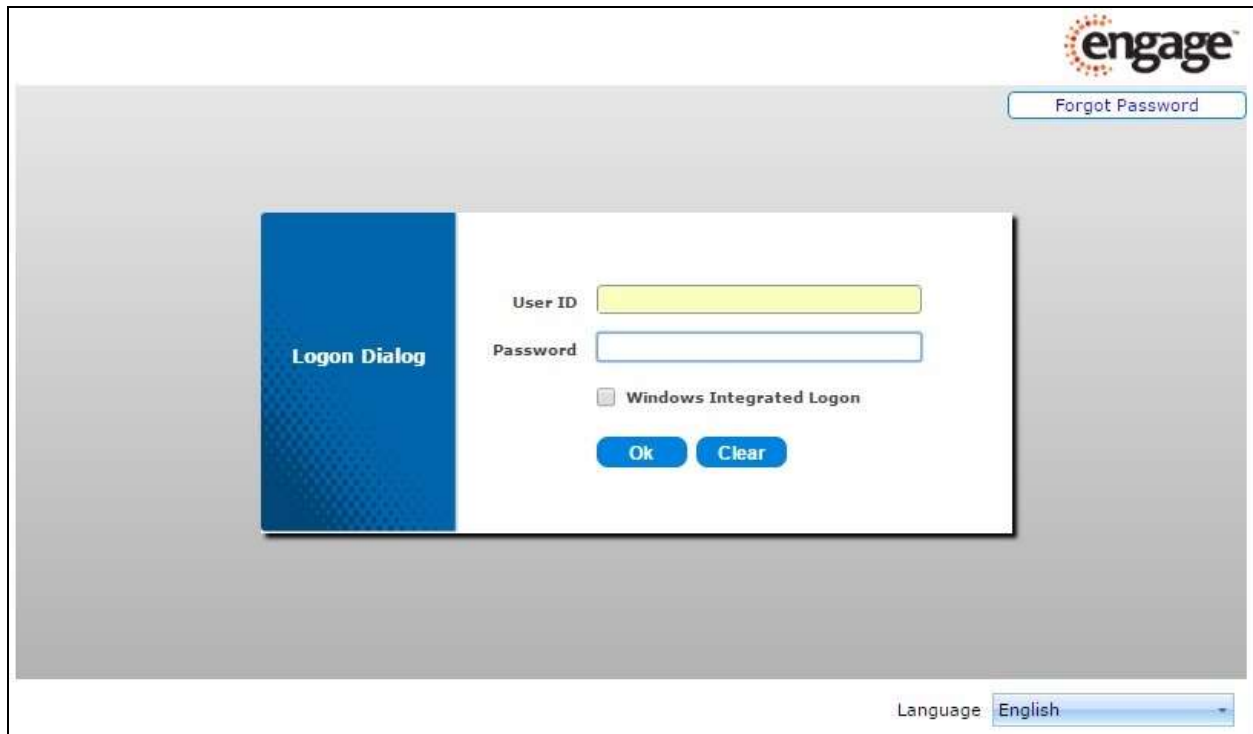
| | Link | Switch Name | Switch CTI Link ID | Status | Since | State | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|----------------------------------|------|-------------|--------------------|---------|--------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| <input checked="" type="radio"/> | 1 | cm7 | 1 | Talking | Fri Dec 18 17:38:27 2015 | Online | 17 | 4 | 47 | 45 | 30 |

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

10.3. Verify TelStrat Engage

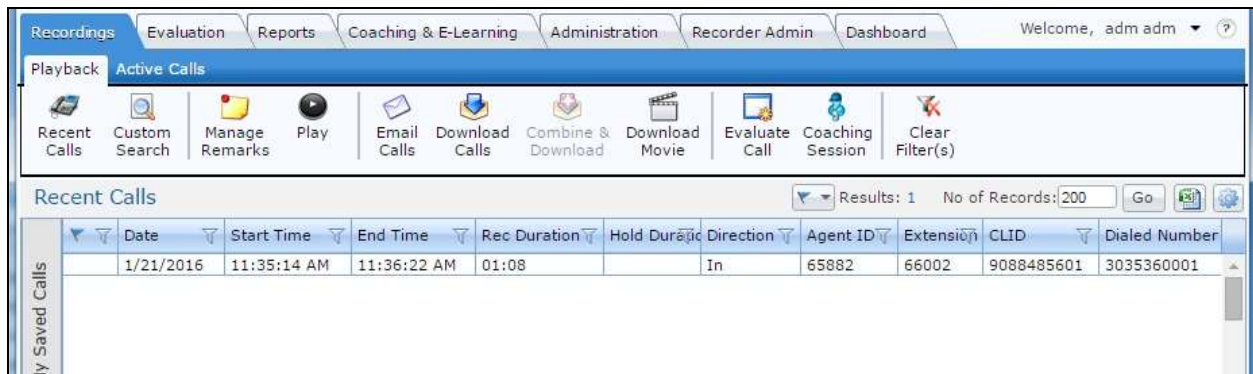
Log an agent into the skill group to handle and complete an ACD call. Access the Engage web-based interface by using the URL “http://ip-address/engage” in an Internet browser window, where “ip-address” is the IP address of the Engage server.

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

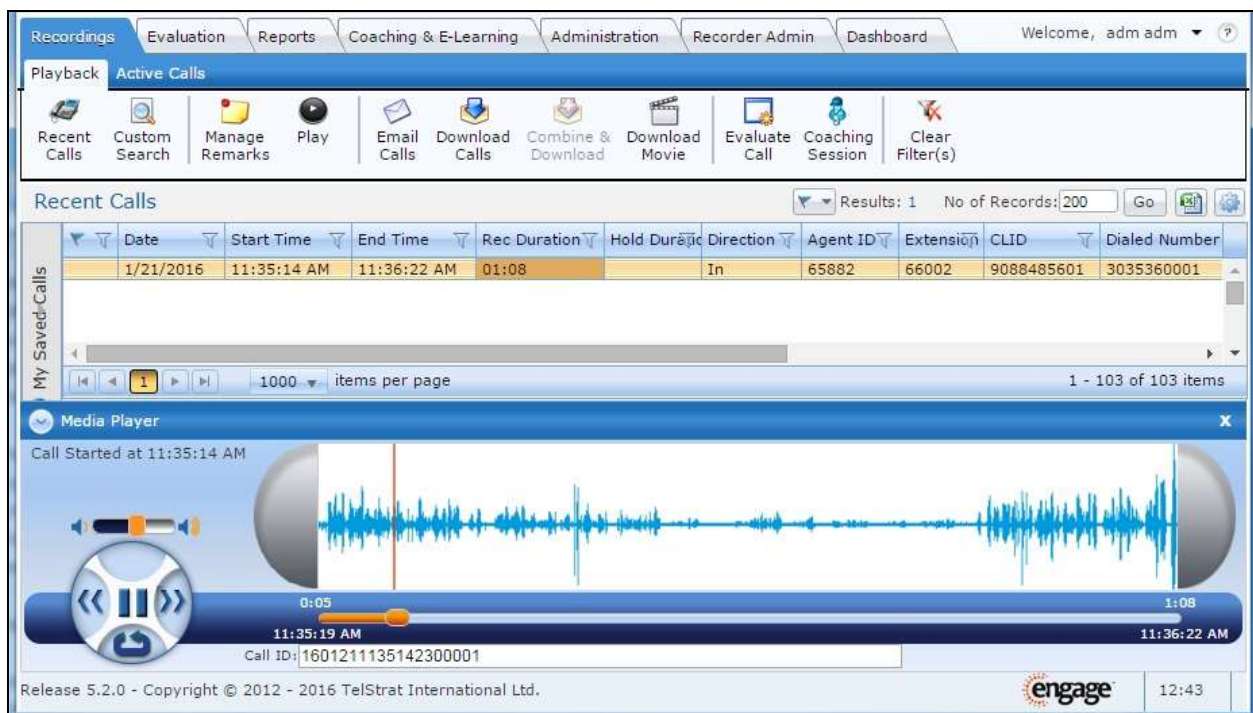


The screenshot shows the Engage web-based interface. In the top right corner, there is the Engage logo and a "Forgot Password" link. The main content area features a "Logon Dialog" window. This dialog has a blue header with the text "Logon Dialog". Below the header, there are two input fields: "User ID" and "Password". The "User ID" field is highlighted in yellow. Below these fields is a checkbox labeled "Windows Integrated Logon". At the bottom of the dialog are two buttons: "Ok" and "Clear". In the bottom right corner of the main interface, there is a "Language" dropdown menu currently set to "English".

The screen is updated with a list of 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.



11. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage 5.2 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using VoIP recording. All feature and serviceability test cases were completed with an observation 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 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
4. *Install – Setup Engage Server*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.
5. *Config Guide – Avaya CM*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.
6. *Recorder Administration Guide*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.

©2016 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.