



Avaya Solution & Interoperability Test Lab

Application Notes for Engelbart esuits² Special Purpose Console Framework 1.2.1 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1– Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Engelbart esuits² Special Purpose Console Framework 1.2.1 to interoperate with Avaya Aura® Communication Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4. Engelbart esuits² Special Purpose Console Framework used the Java Telephony Application Programming Interface and System Management Service Web Service from Avaya Aura® Application Enablement Services.

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 Engelbart esuits² Special Purpose Console (SPC) Framework 1.2.1 to interoperate with Avaya Aura® Communication Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4.

Engelbart esuits² SPC Framework used the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services for basic call control via a web-based agent interface.

Engelbart esuits² SPC Framework used Application Enablement Service System Management Service (SMS) to access Communication Manager configuration data to monitor agent states, calls in VDN, and allow agents to select skills at login and supervisor can change agent status or move them to a different skill.

2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming ACD calls were placed with available agents running the web based Engelbart esuits² SPC Framework on the desktops. Manual call controls were exercised from Engelbart esuits² SPC Framework to verify proper call actions such as answer and transfer.

For the SMS testing, manually change the skills of agent on Communication Manager and on Engelbart esuits² SPC Framework. Verify agent status and skills list update in Engelbart esuits² SPC Framework.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connections to the Engelbart esuits² SPC Framework server and to the agent desktop.

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 Avaya systems and Engelbart esuits² SPC Framework did not include use of any specific encryption features as requested by Engelbart.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Engelbart esuits² SPC Framework:

- Handling of JTAPI/TSAPI messages in the areas of event notifications, value queries, and set agent states.
- Use of JTAPI/TSAPI call control services to support call control actions such as answer and transfer from the agent desktops.
- Proper handling of call scenarios involving inbound, outbound, ACD, non-ACD, transfer, conference, multiple agents, multiple calls, and long duration.
- Verify agent can select skills at login. SPC can show all agent's status in each skill.
- Verify supervisor can change agent status or move them to a different skill.

The serviceability testing focused on verifying the ability of Engelbart esuits² SPC Framework to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the Engelbart esuits² SPC Framework server and to the agent desktop.

2.2. Test Results

All test cases were executed and verified successfully.

2.3. Support

Technical support on Engelbart esuits² SPC Framework can be obtained through the following:

Engelbart Software GmbH

Alpenstrasse 12

6300 Zug

Switzerland

Tel: +41 41 511 35 02

E-Mail: info@engelbart-software.com

Parkstrasse 40

88212 Ravensburg

Germany

Tel: +49 751 7642 4300

E-Mail: info@engelbart-software.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described. In the compliance testing, Engelbart esuits² SPC Framework monitored the agent station extensions shown in the table below.

Device Type	Extension
Routing VDN	88000, 88001
Skill Group	87000, 87001
Agent Station	70017, 70018
Supervisor Station	80010
Agent ID	80000, 80001

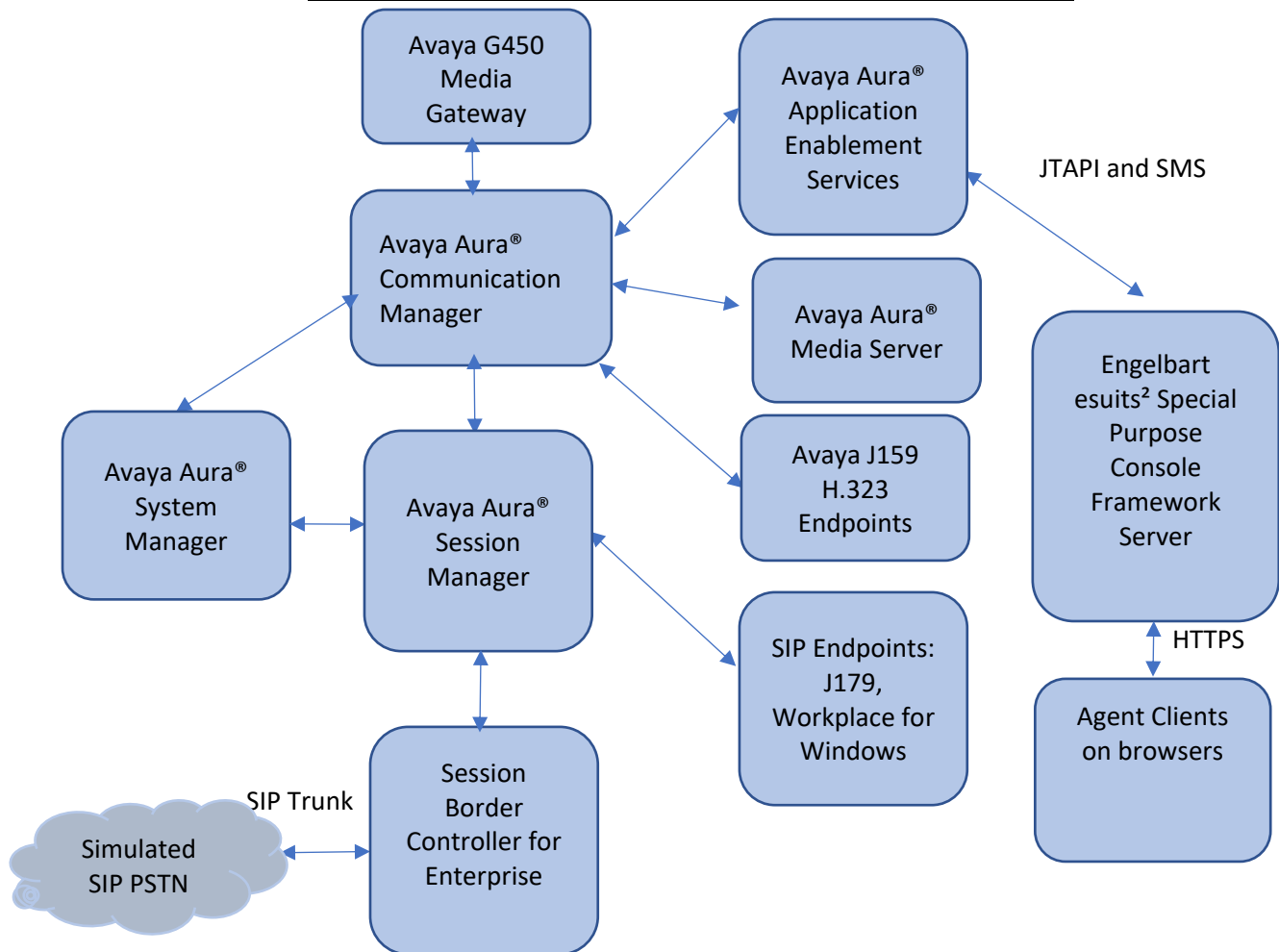


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.3.4.1014185
Avaya Aura® Session Manager in Virtual Environment	8.1.3.4.813401
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.4 - 01.0.890.0-27348
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.4.0.2-0
Avaya Session Border Controller for Enterprise	8.1.3
Avaya Workplace Client for Windows	3.22.0
Avaya J179 IP Phone (SIP)	4.0.9
Avaya J159 IP Deskphone (H.323)	6.8.5
Engelbart esuits ² Special Purpose Console (SPC) Framework - Avaya JTAPI Client	1.2.1 8.1.3

5. Configure Avaya Aura® Communication Manager

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

- Administer CTI link
- Administer Reason Codes
- Administer hunt group and agent
- Add new user on Communication Manager for SMS service

5.1. 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: 79999		
Type: ADJ-IP		
COR: 1		
Name: aes95		

5.2. Administer Reason Codes

For contact centers that use reason codes, enter the **change reason-code-names** command. Configure the **Aux Work** and **Logout** reason codes as desired. The compliance testing used the default values used by Engelbart esuits² Special Purpose Console (SPC) Framework, which are shown below.

change reason-code-names		Page 1 of 1
REASON CODE NAMES		
Aux Work/ Interruptible?		Logout
Reason Code 1:	In a Meeting	/n Break
Reason Code 2:	Out of Office	/n Lunch
Reason Code 3:	Lunch	/n
Reason Code 4:		/n
Reason Code 5:		/n
Reason Code 6:		/n
Reason Code 7:		/n Other
Reason Code 8:		/n
Reason Code 9:		/n
Default Reason Code:		

5.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. The following sections give step by step instructions on how to add the following

- Hunt Group
- Agent

5.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **1** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: VoiceService	Queue? y	
Group Extension: 87000	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

On **Page 2** ensure that **Skill** is set to **y** as shown below.

add hunt-group 1		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

5.3.2. Repeat this section to create hunt-group 2 with Group Extension 87001Add Agent

In the compliance testing, the agents 80000 and 80001 were created.

To add a new agent, type **add agent-loginID x**, where x is an available login id for the new agent.

add agent-loginID 80000	Page	1 of 3
AGENT LOGINID		
Login ID: 80000	AAS? n	
Name: Voice Agent	AUDIX? n	
TN: 1	Check skill TNS to match agent TN? n	
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code:	LWC Log External Calls? n	
	AUDIX Name for Messaging:	
	LoginID for ISDN/SIP Display? n	
	Password:****	
	Password (enter again):****	
MWI Served User Type: sip-adjunct	Auto Answer: station	
AUX Agent Remains in LOA Queue: system	MIA Across Skills: system	
AUX Agent Considered Idle (MIA): system	ACW Agent Considered Idle: system	
Work Mode on Login: system	Aux Work Reason Code Type: system	
	Logout Reason Code Type: system	
Maximum time agent in ACW before logout (sec): system		
	Forced Agent Logout Time:	
WARNING: Agent must log in again before changes take effect		

On **Page 2**, add the required skills. Note that the skill **1** and skill **2** are added to this agent so when a call for **Voice Service** is initiated, the call can be routed to this agent.

add agent-loginID 80000	Page	2 of 3
AGENT LOGINID		
Direct Agent Skill:	Service	Objective? n
Call Handling Preference: skill-level	Local Call Preference? n	
SN RL SL	SN RL SL	SN RL SL
1: 1 1	16: 16: 16:	46: 46: 46:
2: 2 1	17: 17: 17:	47: 47: 47:
3: 3 1	18: 18: 18:	48: 48: 48:
4: 4 1	19: 19: 19:	49: 49: 49:
5: 5 1	20: 20: 20:	50: 50: 50:
6: 6 1	21: 21: 21:	51: 51: 51:
7: 7 1	22: 22: 22:	52: 52: 52:
8: 8 1	23: 23: 23:	53: 53: 53:
9: 9 1	24: 24: 24:	54: 54: 54:
10: 10 1	25: 25: 25:	55: 55: 55:

Repeat this section to add another agent **80001**.

5.4. Add new user on Communication Manager for SMS service

A new user for SMS service needs to be created on Communication Manager. Open a browser session to Communication Manager and log in as shown below. Enter the proper credentials and click on Logon

AVAYA

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

Help Log Off

This Server: cm93

Logon

Logon ID:

Password:

Logon

Once logged in click on **Administration** at the top of the page and select **Server (Maintenance)** from the drop-down menu.

AVAYA

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

Help Log Off

Administration
Licensing
Server (Maintenance)

This Server: cm93

The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

System Management Interface

© 2001-2022 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

In the left window select **Security → Administrator Accounts**. In the main window Select **Add**

Login, for the compliance testing **Privileged Administrator** was chosen to read and write to the fields in Communication Manager. Select **Submit** when done.

AVAYA

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: cm93

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

Data Backup/Restore

Backup Now

Backup History

Schedule Backup

Backup Logs

View/Restore Data

Restore History

Security

Administrator Accounts

Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

☒ Add Login

☒ Privileged Administrator

☐ Unprivileged Administrator

☐ SAT Access Only

☐ Web Access Only

☐ CDR Access Only

☐ Business Partner Login (dadmin)

☐ Business Partner Craft Login

☐ Custom Login

☐ Change Login

☐ Remove Login

☐ Lock/Unlock Login

☐ Add Group

☐ Remove Group

Enter the **Login name** and a suitable **password**. Click on **Submit** when done.

AVAYA

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

Help Log Off Administration

Administration / Server (Maintenance) This Server: cm93

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

Data Backup/Restore

Backup Now

Backup History

Schedule Backup

Backup Logs

View/Restore Data

Restore History

Security

Administrator Accounts

Login Account Policy

Change Password

Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	<input type="text" value="smsadmin"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/>
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/smsadmin"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="....."/>
Re-enter password	<input type="password" value="....."/>
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes

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 Engelbart user
- Administer security database
- Restart services
- Obtain Tlink name
- Configure SMS

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.



Application Enablement Services Management Console

[Help](#)

Please login here:

Username

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Jul 20 15:13:05 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Fri Jul 29 18:49:40 ICT 2022
HA Status: Not Configured

HomeHome | 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).

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Jul 20 15:13:05 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Fri Jul 29 18:50:20 ICT 2022
HA Status: Not Configured

LicensingHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

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

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

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

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍

Home | **Licenses**

Licenses

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View license capacity
 - View peak usage
- ASBCE
- ▶ Session_Border_Controller_E_AE
- AVAYAAURAWEBGATEWAY
- ▶ AVAYAAURAWEBGATEWAY
- AVP
- ▶ AVP
- CCTR
- ▶ ContactCenter
- CE
- ▶ COLLABORATION_ENVIRONMENT
- COMMUNICATION_MANAGER
- ▶ Call_Center
- ▶ Communication_Manager
- ▶ Dialog_Designer
- IPO
- ▶ IP_Office
- MESSAGING
- ▶ Messaging
- MSR

Application Enablement (CTI) - Release: 8 - SID: 10503000 **Standard Li**

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

License installed on: September 6, 2019 4:38:44 PM +07:00

License File Host IDs: V7-67-C3-CF-17-1A-01

Licensed Features

13 Items 🔍 Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100

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 left navigation pane is expanded to 'TSAPI' and 'TSAPI Links'. The main content area displays the 'TSAPI Links' screen with a table header: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the header are buttons for 'Add Link', 'Edit Link', and 'Delete Link'. The top right corner shows a welcome message for 'User cust' and system information.

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 **CM93** 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 expanded to 'TSAPI' and 'TSAPI Links'. The main content area displays the 'Add TSAPI Links' form with the following fields: 'Link' (text input), 'Switch Connection' (dropdown menu with 'CM93' selected), 'Switch CTI Link Number' (dropdown menu with '1' selected), 'ASAI Link Version' (dropdown menu with '12' selected), and 'Security' (dropdown menu with 'Both' selected). Below the fields are buttons for 'Apply Changes' and 'Cancel Changes'. The top right corner shows a welcome message for 'User cust' and system information.

6.4. Administer Engelbart 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.



Application Enablement Services Management Console

Welcome: User cust
Last login: Fri Jun 24 11:40:32 2022 from 172.16.8.167
Number of prior failed login attempts: 1
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Mon Jun 27 16:38:34 ICT 2022
HA Status: Not Configured

User Management | User Admin | Add User

[Home](#) | [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 Id

engelbart

* Common Name

engelbart

* Surname

engelbart

* User Password

* Confirm Password

Admin Note

Avaya Role

None ▼

Business Category

Car License

CM Home

Css Home

CT User

Yes ▼

Department Number

Display Name


Employee Number

Employee Type

6.5. 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. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the Engelbart user from **Section 6.4**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Jul 20 15:13:05 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Fri Jul 29 18:57:18 ICT 2022
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

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

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

6.6. Restart Services

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**.



Application Enablement Services Management Console

Maintenance | Service Controller

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▼ Maintenance
 - Date Time/NTP Server
 - ▶ Security Database
 - Service Controller**
 - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

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](#)

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 Engelbart esuits² SPC Framework.

In this case, the associated Tlink name is **AVAYA#CM93#CSTA#AES95**. Note the use of the switch connection **CM93** from **Section 6.3** as part of the Tlink name.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Jul 20 15:13:05 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Fri Jul 29 18:58:58 ICT 2022
HA Status: Not Configured


Security | Security Database | TlinksHome | 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#CM93#CSTA#AES95
☐ AVAYA#CM93#CSTA-S#AES95
Delete Tlink

6.8. Configure SMS

Select **AE Services** → **SMS** → **SMS Properties**. Configure all fields as in screenshot with **Default CM Host Address** using Communication Manager IP address, and **Default CM Admin Port** with 5022

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Mon Aug 15 13:26:39 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Wed Aug 31 18:59:48 ICT 2022
HA Status: Not Configured

AE Services | SMS | SMS PropertiesHome | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▼ SMS

▪ SMS Properties

▶ TSAPI

▶ TWS

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

SMS Properties

Default CM Host Address10.30.5.93

Default CM Admin Port5022

CM Connection ProtocolSSH ▼

SMS LoggingNORMAL ▼

SMS Log Destinationapache ▼

CM Proxy Trace LoggingNONE ▼

Max Sessions per CM5

Proxy Shutdown Timer1800 seconds

SAT Login Keepalive180 seconds

CM Terminal TypeOSSIZ ▼

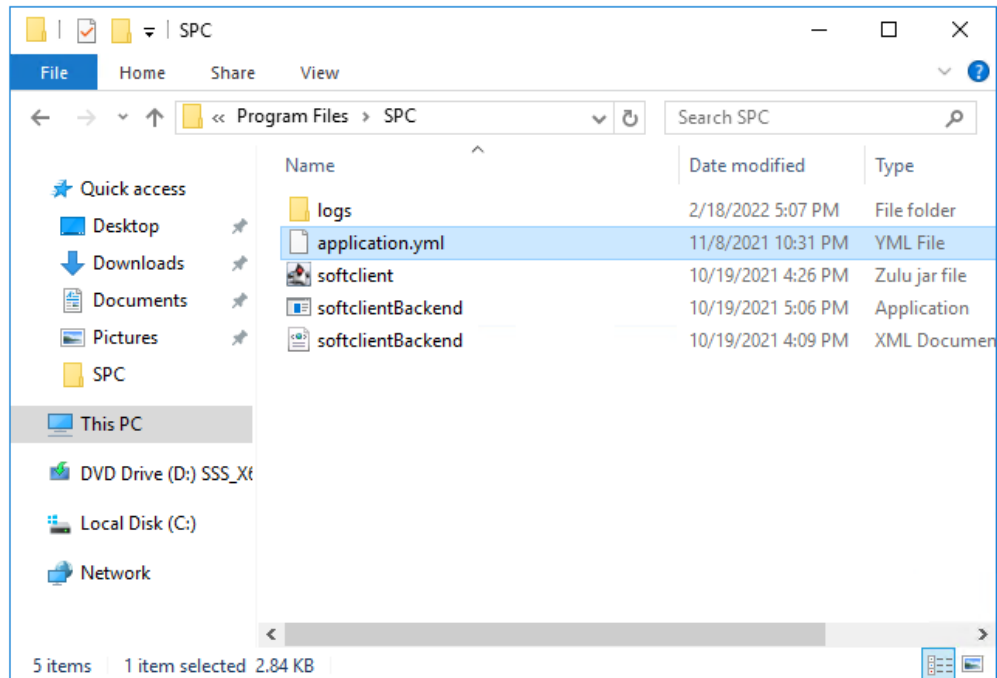
Proxy Log Destination/var/log/avaya/aes/ossicm.log

Apply ChangesRestore DefaultsCancel

7. Configure Engelbart esuits² Special Purpose Console Framework

This section shows the steps required configuration for working with Application Enablement Services. All installation and basic configuration related to Engelbart esuits² SPC Framework is performed by to Engelbart engineers and, thus, is not documented.

From Engelbart esuits² SPC Framework Server, go to the SPC installation folder, i.e C:\Program Files\SPC.



Select **application.yml** file and edit. Scroll down and provide information for avaya jtapi and sms

- jtapi:**
- **service-name** : Tlink name in **Session 6.7**
 - **user**: The Engelbart user credentials from **Section 6.4**.
 - **password**: The engelbart user credentials from **Section 6.4**.
 - **address**: IP address of Application Enablement Services.

- sms:**
- **default-uri**: SMS URL with AES IP address.
 - **username**: The smsadmin user credentials from **Section 5.5**.
 - **password**: The smsadmin user credentials from **Section 5.5**.

```
avaya:
  jtapi:
    service-name: AVAYA#CM93#CSTA#AES95
    user: engelbart
    password: [REDACTED]
    servers:
      - address: 10.30.5.95
        port: 450
  sms:
    default-uri: https://10.30.5.95/smsxml/SystemManagementService.php
    username: smsadmin
    password: [REDACTED]
```

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Engelbart esuits² SPC Framework.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify 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	12	no	aes95	established	14	14

Enter the command **list agent-loginID** verify that agent **80000** and **80001** shown in **Section 5.3** is logged-in to extension **70017** and **70018**.


```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension		Dir	Agt	AAS/AUD		COR Ag Pr SO	
		Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80000	Voice Agent	70017						1	lvl
	1/01	/	/	/	/	/	/	/	
80001	Voice Agent1	70018						1	lvl
	1/01	/	/	/	/	/	/	/	

8.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3.** and that the **Associations** column reflects the number of agents that are logged in.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Aug 31 18:59:35 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Wed Aug 31 19:17:18 ICT 2022
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
	1	CM93	1	Talking	Fri Aug 26 17:02:58 2022	Online	18	2	15	15	30

Online Offline

For service-wide information, choose one of the following:
TSAPI Service Status TLink Status User Status

Verify the CTI user status by selecting **Status → Status and Control → TSAPI Service Summary → User Status**. The **Open Streams** section of this page displays open stream created by the **engelbart** user with the **Tlink**.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Wed Aug 31 18:59:35 2022 from 172.16.8.167
 Number of prior failed login attempts: 0
 HostName/IP: aes95/10.30.5.95
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.3.4.0.2-0
 Server Date and Time: Wed Aug 31 19:19:09 ICT 2022
 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
 - ▶ Logs
 - ▶ Log Manager
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - **TSAPI Service Summary**
- ▶ User Management
- ▶ Utilities
- ▶ Help

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 2
Closed Streams 15

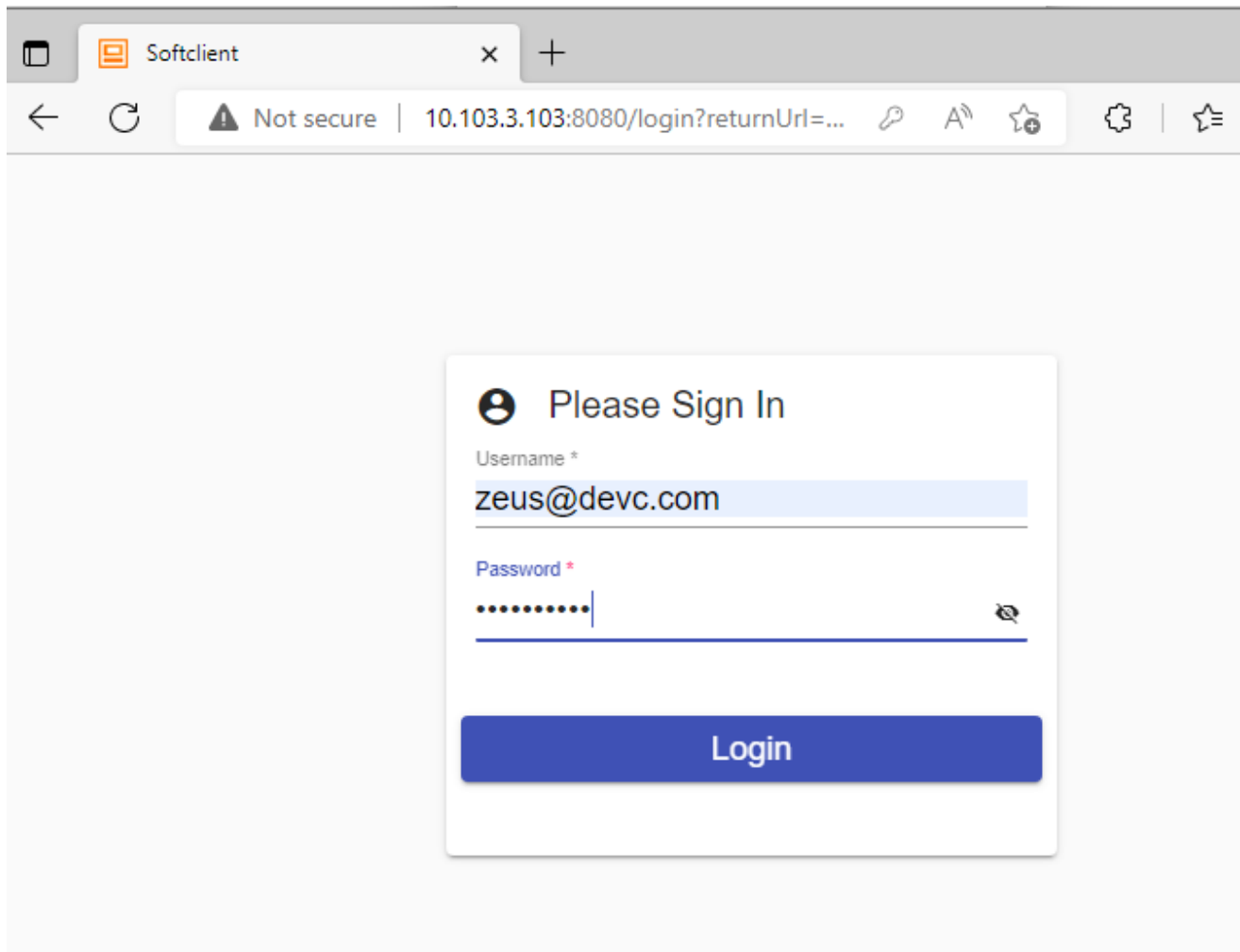
Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCUserDoNotModify	Sat 30 Jul 2022 05:44:54 PM +07		AVAYA#CM93#CSTA#AES95
engelbart	Tue 30 Aug 2022 04:29:31 PM +07		AVAYA#CM93#CSTA#AES95

Show Closed Streams
Close All Opened Streams
Back

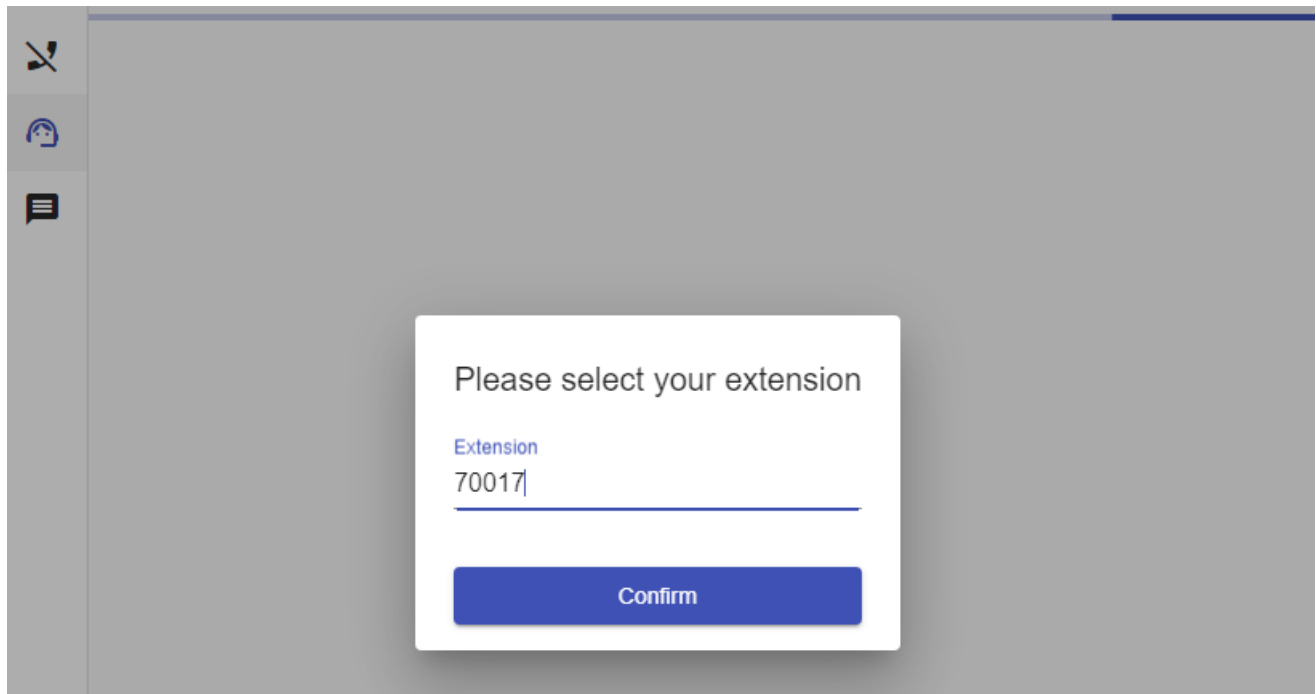
8.3. Verify Engelbart esuits² Special Purpose Console (SPC) Framework

From the agent PC, launch the web-based interface and login with user provided by Engelbart.



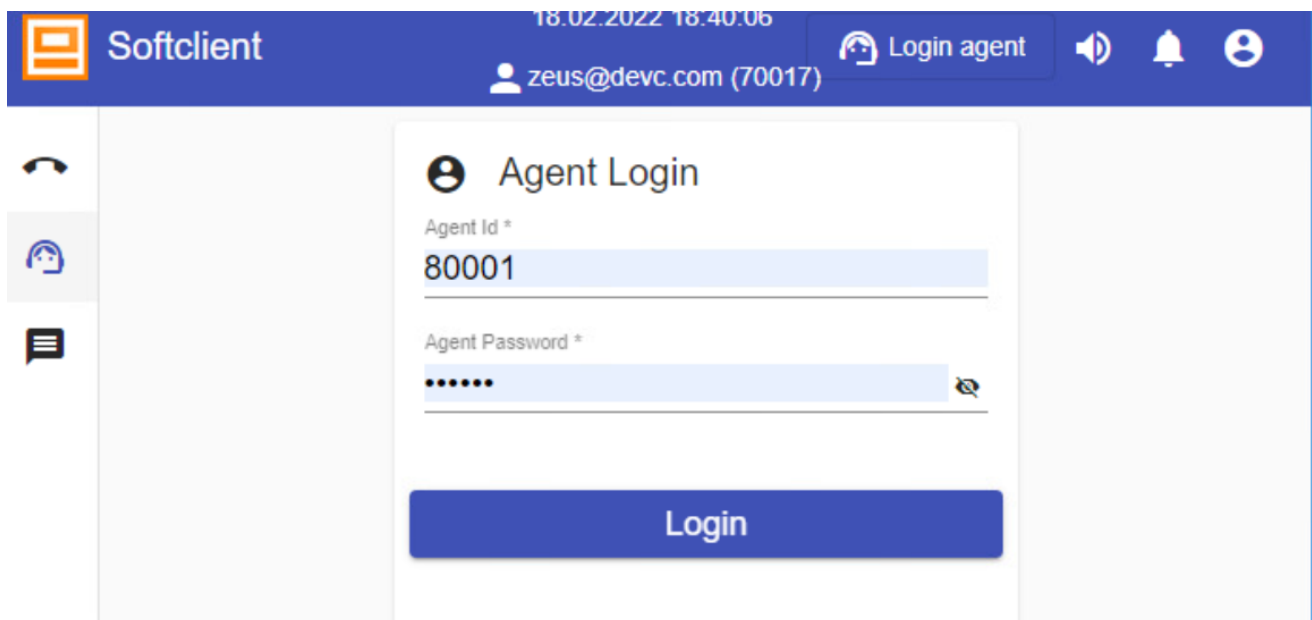
The screenshot shows a web browser window with a single tab titled 'Softclient'. The address bar displays '10.103.3.103:8080/login?returnUrl=...' with a 'Not secure' warning. The main content area features a 'Please Sign In' dialog box. This dialog has a title bar with a user icon and the text 'Please Sign In'. Below the title, there are two input fields: 'Username *' containing 'zeus@devc.com' and 'Password *' which is masked with dots. A blue 'Login' button is positioned at the bottom of the dialog. The background of the browser window is a light gray.

After logged in, enter relevant station extension from **Section 3**.



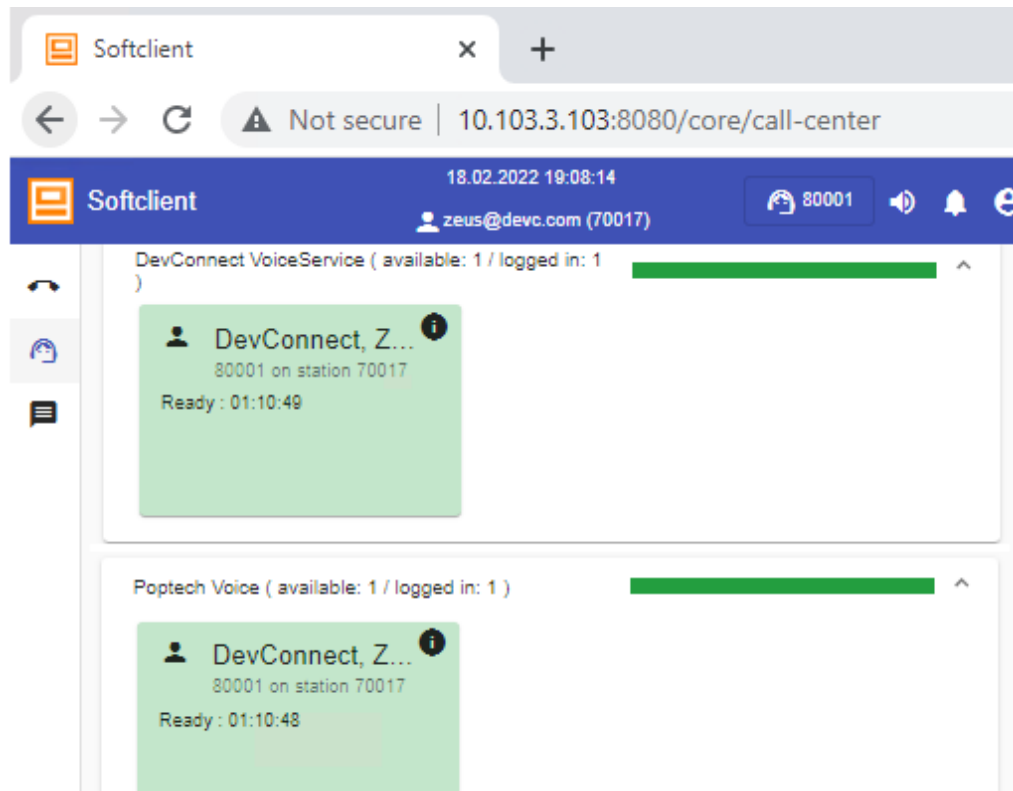
The screenshot shows a modal dialog box titled "Please select your extension". Inside the dialog, there is a label "Extension" followed by a text input field containing the value "70017". Below the input field is a blue button labeled "Confirm". The dialog is centered on a grey background. On the left side of the background, there is a vertical sidebar with three icons: a crossed-out phone, a headset, and a speech bubble.

Press **Login agent** in top right and enter relevant agent ID and password from **Section 3**.

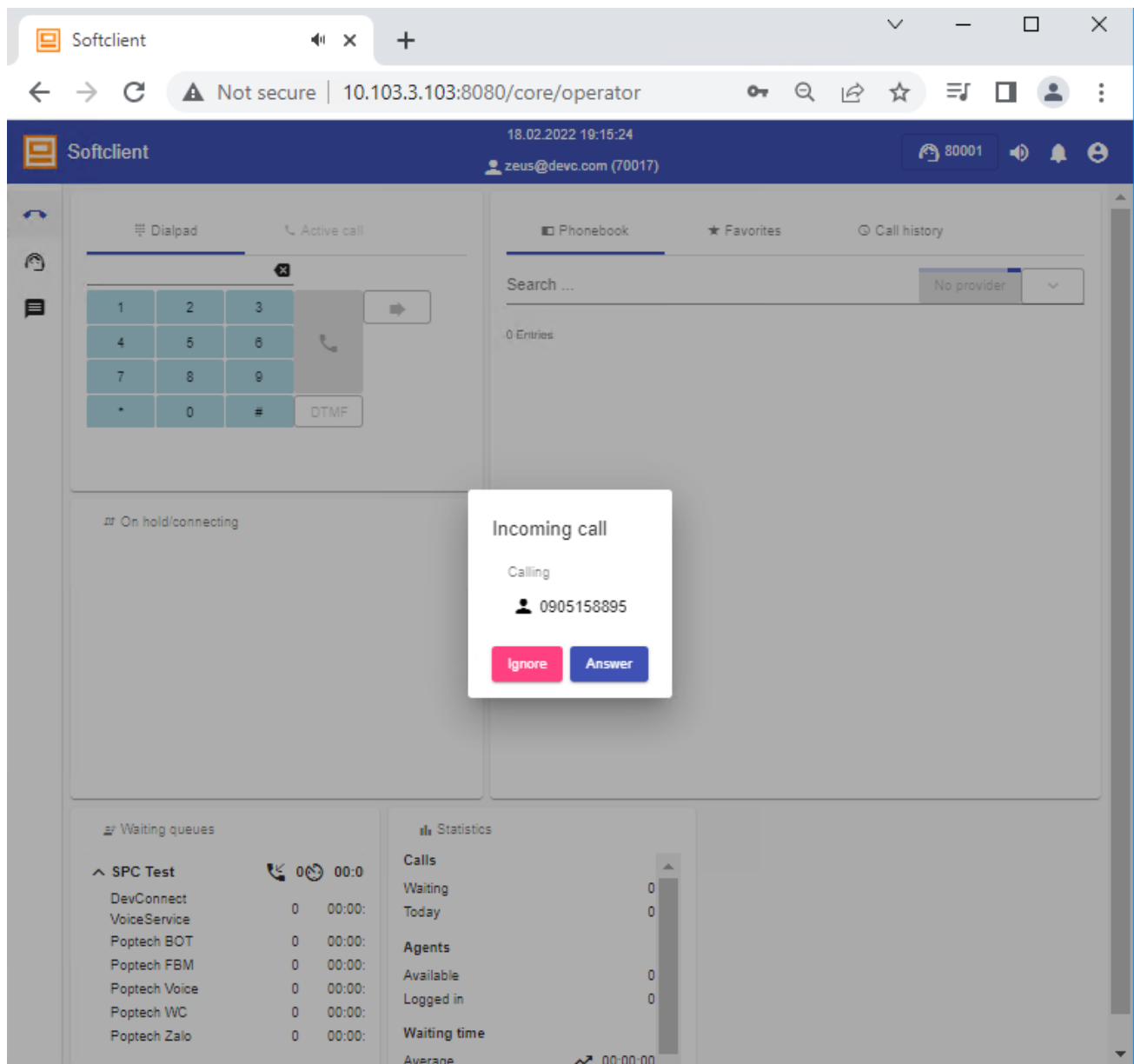


The screenshot shows the "Agent Login" screen within the Softclient application. The top blue header bar contains the Softclient logo, the date and time "18.02.2022 18:40:06", the user email "zeus@devc.com (70017)", and a "Login agent" button. The main content area has a light grey background with a vertical sidebar on the left containing three icons: a phone, a headset, and a speech bubble. The central area displays the "Agent Login" form with two input fields: "Agent Id *" containing "80001" and "Agent Password *" with masked characters. A blue "Login" button is at the bottom of the form.

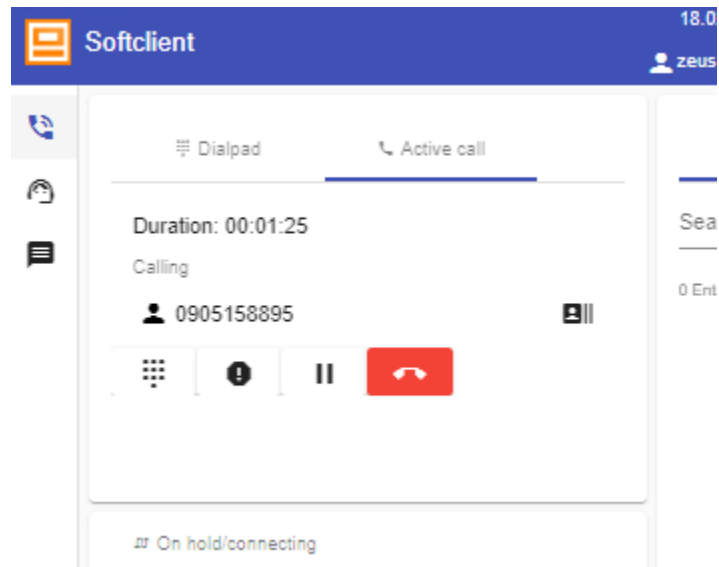
After login successfully Engelbart esuits² SPC Framework will show all skills assigned to agent in **Section 5.3.2**.



Make an incoming ACD call from the PSTN. Verify that the call is ringing at the available agent's telephone. Also verify that a pop-up box is displayed on the agent desktop with proper call information, as shown below.



Press **Answer** to accept the call. Verify that the agent is connected to the PSTN with two-way talk path, and that the agent screen is updated with line as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for the Engelbart esuits² Special Purpose Console Framework 1.2.1 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4. All feature and serviceability test cases were completed without any observations.

10. Additional References

This section references the Avaya and Engelbart esuits² SPC Framework product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, Sept 2021
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 17, Nov 2021
4. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 12, Oct 2021

Product Documentation for Engelbart products may be found at <https://www.engelbart-software.com/>

©2022 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.