



Avaya Solution & Interoperability Test Lab

Application Notes for Algotech AlgoCC 4.7.4 with Avaya Aura® Communication Manager 8.1.3 using Avaya Aura® Application Enablement Services 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Algotech AlgoCC 4.7.4 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3.

The compliance testing focused on the voice integration of Algotech AlgoCC with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Service Application Programming Interface.

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 Algottech AlgoCC 4.7.4 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3

The compliance testing focused on the voice integration of Algottech AlgoCC 4.7.4 with Communication Manager via the Application Enablement Services Telephony Service Application Programming Interface (TSAPI).

Algottech AlgoCC provides complete function set for customer interaction, multimedia communication channels (voice, e-mail, SMS, webchat, Callback, IMChat), application interface for agents, reporting and quality monitoring. AlgoCC uses the TSAPI interface to monitor agent and supervisor station extensions, provide screen pops and call control from agent desktops in an Avaya call center environment.

AlgoCC uses a client/server architecture. Main server components are the AlgoCC application server, Web Server, and the Database server. AlgoCC supports both on-premise and cloud deployments, and the compliance testing used the cloud deployments method with the AlgoCC Server in the Algottech Cloud and it connected to Avaya Application Enablement Services via TSAPI in the DevConnect Lab through VPN Tunneling.

2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound ACD calls using AlgoCC clients. This was performed by calling inbound to a VDN and/or outbound using AlgoCC clients. Where applicable, agent call controls were performed using the AlgoCC client.

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 this Application Note, the interface between Avaya systems and Algotech AlgoCC did not include use of any specific encryption features as requested by Algotech.

2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Change Agent state** – Login, Ready, Not Ready, After Call Work using AlgoCC client.
- **Inbound Calls** – Answer calls using AlgoCC client.
- **Outbound Calls** – Make calls using Avaya Phones and control using AlgoCC client.
- **Hold/Transfer**– Place callers on hold and transfer using AlgoCC client.
- **Failover Testing** - Verify the ability of AlgoCC server/client to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All test cases were executed. The following were observations on AlgoCC client from the compliance testing.

- AlgoCC client does not support initiate Conference.

2.3. Support

Technical support can be obtained for the AlgoCC solution as follows:

E-mail: helpdesk@algotech.cz

Internet: <https://helpdesk.algotech.cz>

Tel: +420 225 006 444

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.

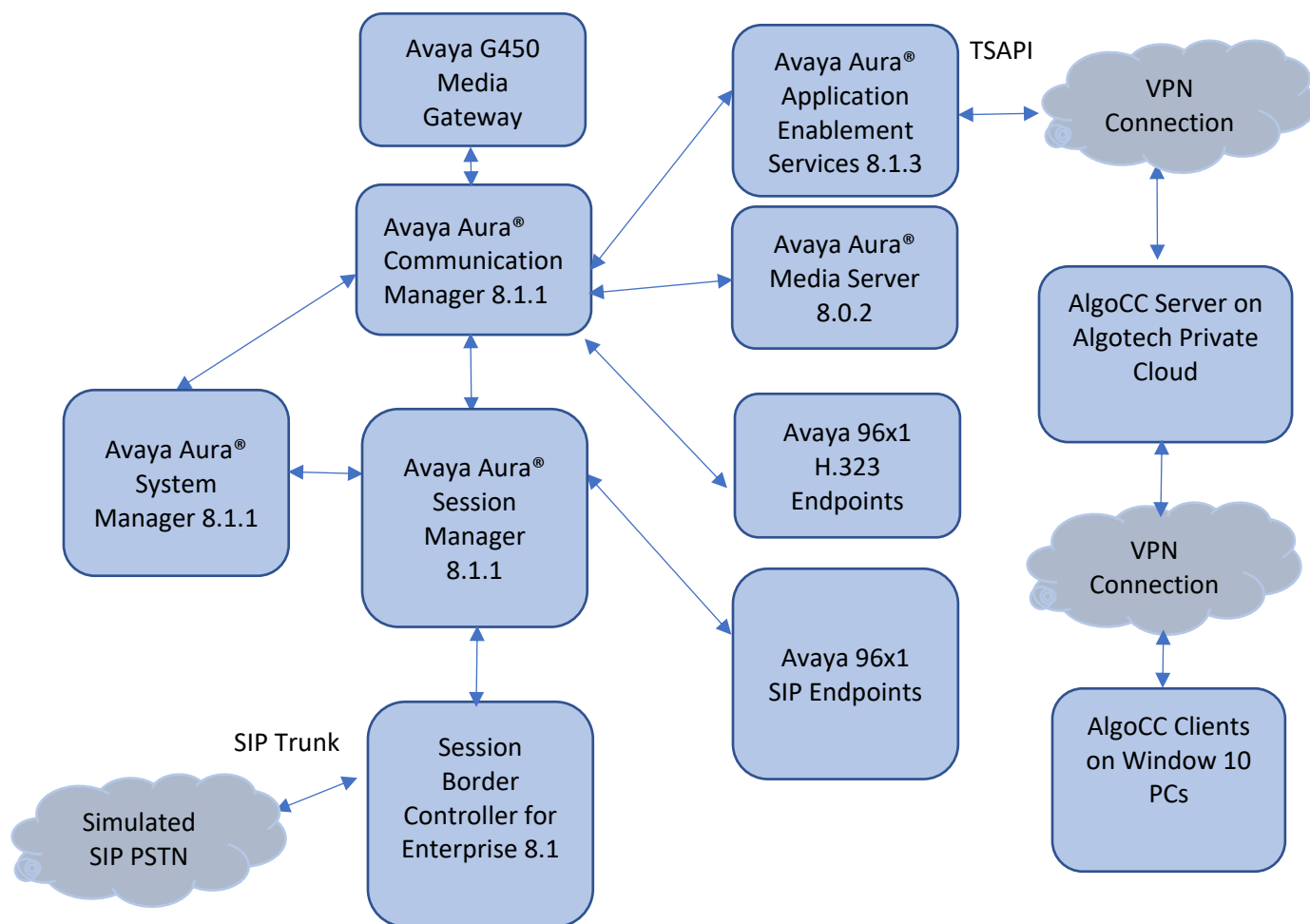


Figure 1: Compliance Testing Configuration

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
Avaya Aura® Session Manager in Virtual Environment	8.1.3
Avaya Aura® Communication Manager in Virtual Environment	8.1.3
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
Avaya Session Border Controller for Enterprise	8.1.1
Avaya 9621G & 9641G IP Desk phone (SIP)	7.1.8
Avaya 9608G & 9641G IP Desk phone (H.323)	6.8.3
AlgoCC AlgoCC Server AlgoCC Client	4.7.4 4.7.4

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 hunt group and agent

5.1. Verify License

Log into 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		
(NOTE: You must logoff & login to effect the permission changes.)		

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

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: Voice Service	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. Add 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 the 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):	
	Auto Answer: station	
	MIA Across Skills: system	
	ACW Agent Considered Idle: 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** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly 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	SN	RL SL
1: 1	1	16:		31:		46:	
2:		17:		32:		47:	
3:		18:		33:		48:	
4:		19:		34:		49:	
5:		20:		35:		50:	
6:		21:		36:		51:	
7:		22:		37:		52:	
8:		23:		38:		53:	
9:		24:		39:		54:	
10:		25:		40:		55:	

Repeat this section to add another agent 80001.

5.4.Administer Vectors and VDNs

Add a vector using the **change vector n** command, where **n** is a vector number. Note that the vector steps may vary, and below is a sample vector used in the compliance testing.

```
change vector 1                                     Page 1 of 6

                                CALL VECTOR

    Number: 1                                Name: VoiceService
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
    Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
    Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
    Variables? y      3.0 Enhanced? y
01 wait-time      2      secs hearing silence
02 queue-to      skill 1      pri t
03 wait-time      2      secs hearing silence
04 stop
05
06
07
08
09
10
11
12

                                Press 'Esc f 6' for Vector Editing
```

Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive Name and the vector number from above for Destination. Retain the default values for all remaining fields.

```
change vdn 88000                                     Page 1 of 3

                                VECTOR DIRECTORY NUMBER

                                Extension: 88000                                Unicode Name? n
                                Name*: Voice VDN
                                Destination: Vector Number      1
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none      Report Adjunct Calls as ACD*? n

                                VDN of Origin Annc. Extension*:
                                1st Skill*:
                                2nd Skill*:
                                3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

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 Avaya user
- Administer security database
- 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.



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: Thu Feb 18 14:36:40 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 17:38:46 ICT 2021
HA Status: Not Configured

Home

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.

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

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: Thu Feb 18 14:36:40 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 17:39:12 ICT 2021
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

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

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. The TSAPI license is used for device monitoring.

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
- AVAYAARAWEBCONTROL
- AVAYAARAWEBCONTROL
- 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 License

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 top right corner displays user information: Welcome: User cust, Last login: Thu Feb 18 14:36:40 2021 from 10.128.224.59, Number of prior failed login attempts: 0, HostName/IP: aes95/10.30.5.95, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 8.1.3.0.0.25-0, Server Date and Time: Mon Feb 22 17:44:37 ICT 2021, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. 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 **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 the same as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains form fields for: Link (text input with value 1), Switch Connection (dropdown menu with value CM93), Switch CTI Link Number (dropdown menu with value 1), ASAI Link Version (dropdown menu with value 9), and Security (dropdown menu with value Both). At the bottom are buttons for 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

6.4. Administer algocc 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: Mon Feb 22 17:38:25 2021 from 10.128.224.163
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 18:20:23 ICT 2021
HA Status: Not Configured

User Management | User Admin | List All UsersHome | 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

* User Id

* Common Name

* Surname

User Password

Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

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 and click **Apply Changes**.

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 Avaya user from **Section 6.4**.

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 user "cust" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

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 AlgoCC.

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows a welcome message for user 'cust' and system information: 'Last login: Thu Feb 18 14:36:40 2021 from 10.128.224.59', 'Number of prior failed login attempts: 0', 'HostName/IP: aes95/10.30.5.95', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.3.0.0.25-0', 'Server Date and Time: Mon Feb 22 17:50:34 ICT 2021', and 'HA Status: Not Configured'. The main header reads 'AVAYA Application Enablement Services Management Console'. A red navigation bar contains 'Security | Security Database | Tlinks' and links for 'Home | Help | Logout'. The left sidebar lists various services, with 'Security' expanded to show 'Security Database' and its sub-items: 'Control', 'CTI Users', 'Devices', 'Device Groups', and 'Tlinks'. The main content area, titled 'Tlinks', shows a single entry with the 'Tlink Name' 'AVAYA#CM93#CSTA#AES95' and a 'Delete Tlink' button.

7. Configure Algotech AlgoCC Server and Client

7.1. Configure Algotech AlgoCC Server

All configuration related to Algotech AloCC Server is performed by Algotech engineers and, thus, is not documented.

7.2. Configure Algotech AlgoCC Client

Download AlgoCC Launcher at URL provided by Algotech:

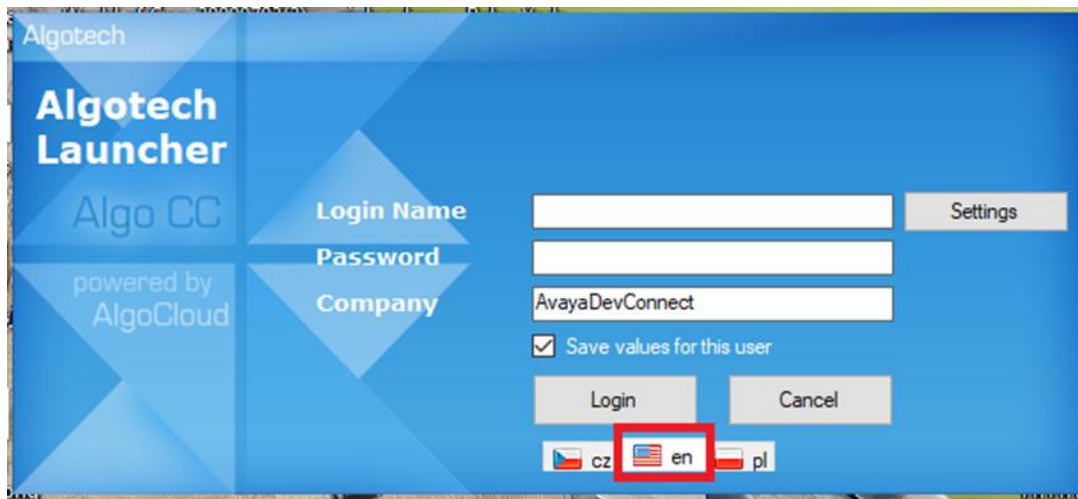
<http://<IPAddress>/AlgoCCLauncher180/>



Run AlgoCC Launcher with its desktop icon:

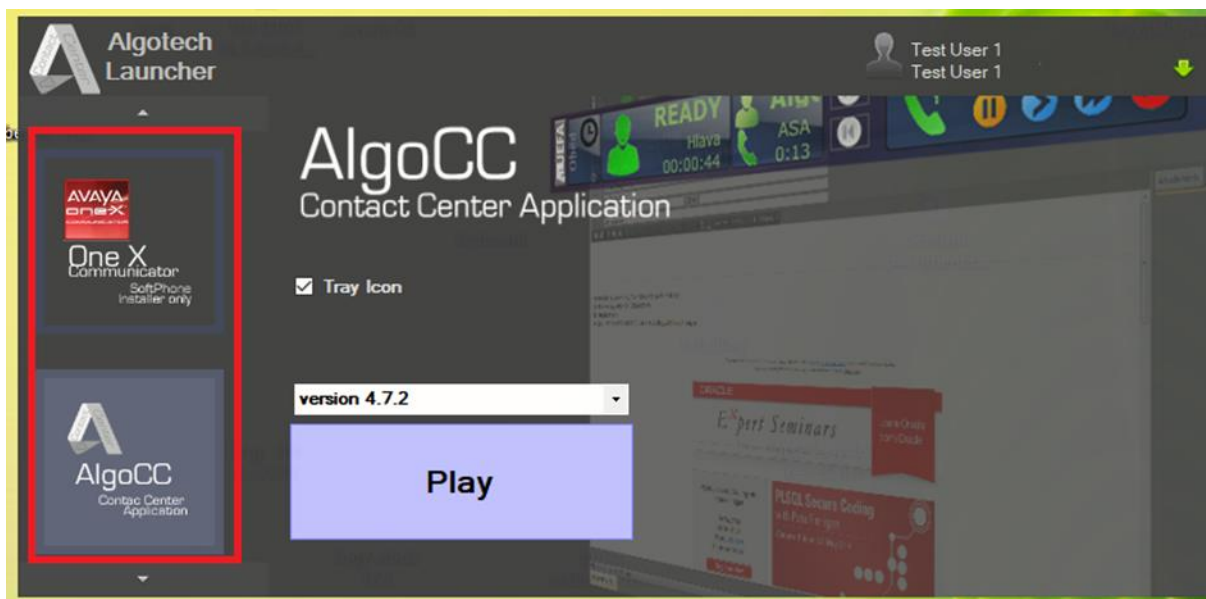


Enter login details provided by Algotech and choose “en” language option for English:



After opening AlgoCC Launcher, choose AlgoCC application at left menu options (Avaya one-X Communicator also available here for download).

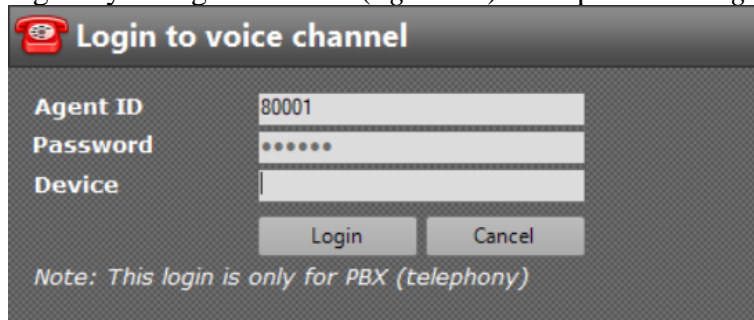
Download version 4.7.4 or newer by button **Download**, or eventually update the version by button **Update**. Then click on **Play**.



Login to voice channel. For login, move mouse cursor on tile of a voice channel and click on a green check mark symbol.



In the following dialog fill in the *Device* – it is the number of the station (*Device Extension*) to which you want to log in by the agent number (*Agent ID*). You press the *Login* button.



A dialog box titled "Login to voice channel" with a red telephone icon. It contains three input fields: "Agent ID" with the value "80001", "Password" with masked characters "*****", and "Device" which is empty. Below the fields are "Login" and "Cancel" buttons. A note at the bottom states: "Note: This login is only for PBX (telephony)".

To evaluate of correct login to voice channel, the whole bar turns yellow/orange (no tile is to be white or grey).

This is the example of a bar after correct login:



8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya Aura Communication Manager, Avaya Aura Enablement Services and AlgoCC solution.

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	9	no	aes95	established	14	14

Enter the command **list agent-loginID** verify that agent **80000** and **80001** shown in **Section 5.4** is logged-in to extension **70010** and **70009**.

```
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	Skil/Lv
80000	Voice Agent	70010					1	lv1	
	1/01	/	/	/	/	/	/		
80001	Voice Agent1	70009					1	lv1	
	1/01	/	/	/	/	/	/		

Enter the command **status station 70010** and on **Page 7** verify that the agent is logged-in to the appropriate skill.


```
status station 70010
```

ACD STATUS							Page	7	of	7
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod				
1/AUX	/	/	/	/	/	/	On ACD Call? no			

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**



Application Enablement Services
Management Console

Welcome: User cust
Last login: Thu Feb 18 14:36:40 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 18:04:34 ICT 2021
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	Mon Mar 16 16:16:51 2020	Online	18	2	15	15	30

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

8.3. Verify Avaya Aura® Application Enablement Services TSAPI Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the TSAPI service by selecting **Status** → **Status and Control** → **TSAPI Service Summary** → **User Status**. The **Open Streams** section of this page displays open stream created by the **alogcc** user with the **Tlink**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Mon Feb 22 17:38:25 2021 from 10.128.224.163
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 18:19:14 ICT 2021
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

User Management

Utilities

Help

CTI User Status

☐ Enable page refresh every 60 seconds

CTI UsersalogccSubmit

Open Streams 5

Closed Streams 29

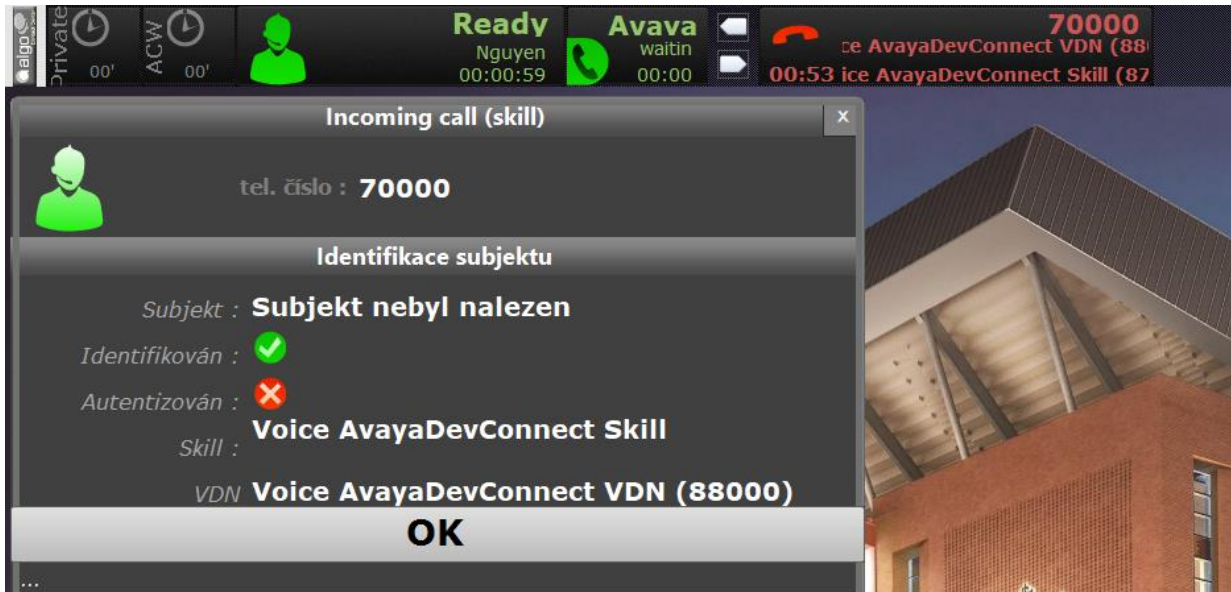
Open Streams

Name	Time Opened	Time Closed	Tlink Name
alogcc	Thu 18 Feb 2021 06:20:23 AM +07		AVAYA#CM93#CSTA#AES95
alogcc	Thu 18 Feb 2021 06:20:26 AM +07		AVAYA#CM93#CSTA#AES95
alogcc	Thu 18 Feb 2021 06:20:29 AM +07		AVAYA#CM93#CSTA#AES95
alogcc	Thu 18 Feb 2021 06:20:31 AM +07		AVAYA#CM93#CSTA#AES95
alogcc	Thu 18 Feb 2021 06:20:32 AM +07		AVAYA#CM93#CSTA#AES95

Show Closed StreamsClose All Opened StreamsBack

8.4. Verify AlgoCC Client call handling and agent status

Place a call to VDN/Hunt Group. Verify that AlgoCC Client can receive incoming call:



Press **OK** to handle the call, verify the correct extension details are displayed:



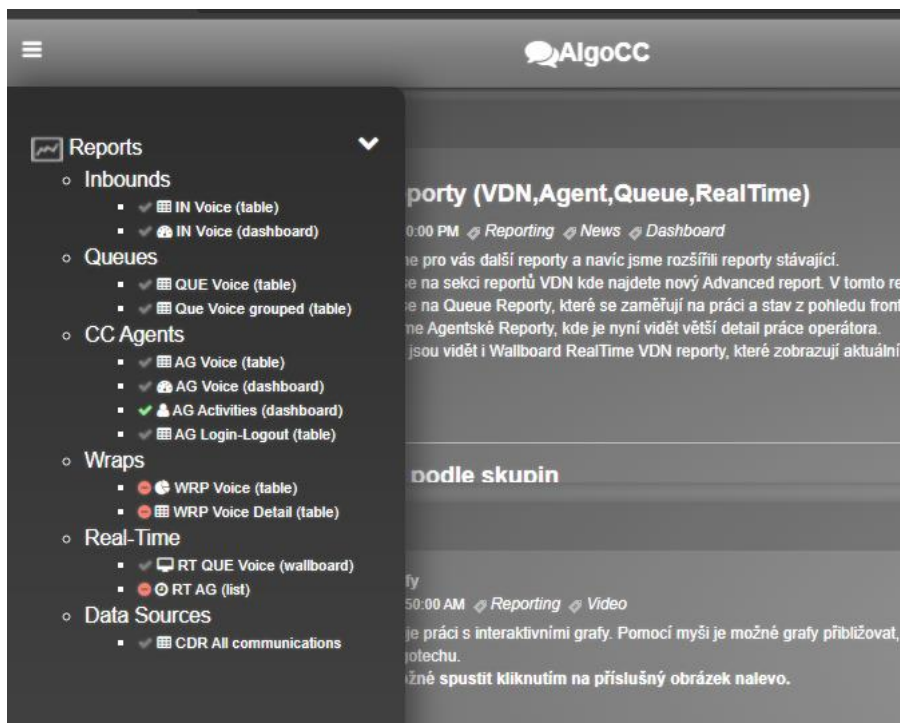
8.5.AlgoCC Reports

Admin can view report data from AlgoCC web portal. To access AlgoCC web portal, open web portal URL on browser: [https://\[Webportal FQDN\]/AlgoCC/](https://[Webportal FQDN]/AlgoCC/)

Login details provided by Algotech for report access.



To view reports, select tables, dashboards or wallboard from **Reports** menu on left. Example Select **Reports** → **Queues** → **QUE Voice (table)**



Select **Display Type**, **Type**, **From**, **To**, **Channel Type** and **Queues** to generate report and press **Generate** button to view report tables as show below:

AlgoCC													
QUE Voice (table)													
Display Type:		Queue-Interval	Type:	Days	From:	2021-02-01	To:	2021-02-22	1 Channel Type	1 Queues			
Total			94	0 %	233 %	34 %	0	94	0	93	61	219	32
Queue Name	Day	List of VDNs	Call Counts	SLA	Answered Rate	Abandoned Rate	SLA Abandoned in time	SLA Call Count	SLA Answered in time	Queued Count	Answered Queue Count	Answered Count	Abandoned Count
Voice AvayaDevConnect Skill 87000 Voice	02/04/2021	(N/A)	93	0 %	235 %	33 %	0	93	0	92	61	219	31
	02/22/2021	(N/A)	1	0 %	0 %	100 %	0	1	0	1	0	0	1
	Sub Total	VDNs	94	0 %	233 %	34 %	0	94	0	93	61	219	32

9. Conclusion

These Application Notes describe the configuration steps required for the AlgoCC Solution to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Algotech 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 8, Nov 2020*
2. *Administering Avaya Aura® Session Manager, Release 8.1.x, Issue 8, Feb 2021*
3. *Administering Avaya Aura® System Manager, Release 8.1.x, Issue 9, Feb 2021*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 9, Feb 2021*

Product Documentation for Algotech AlgoCC can be requested from Algotech:

©2021 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.