



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for AGC Networks Flair Agent Workspace 1.0 with Avaya Aura® Communication Manager 8.1 using Avaya Aura® Application Enablement Services 8.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for AGC Networks Flair Agent Workspace 1.0 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

The compliance testing focused on the voice integration of AGC Networks Flair Agent Workspace with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Java Telephony 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 AGC Networks Flair Agent Workspace 1.0 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

The compliance testing focused on the voice integration of AGC Networks Flair with Communication Manager via the Application Enablement Services Java Telephony Application Programming Interface (JTAPI).

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

AGC Networks Flair is a browser-based agent workspace, which provides telephony and control functionality to agents. The application provides the ability to handle inbound calls and consultation calls and provides additional components as required by the use case.

The Flair Agent Workspace solution consists of two main application components. Typically, the two components are deployed on a single windows server provided by the customer:

- Flair Server: The server application has the JTAPI interface for communicating with Application Enablement Services. It works as an interface between Enablement Services and the Flair Client browser application.
- Flair Client: Also referred to as the Flair Workspace application, the browser application is deployed on the application server, and is access by the agent through a browser from the agent's workstation. It provides the GUI for the agent to handle the incoming calls and perform telephony controls.

## 2. General Test Approach and Test Results

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

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 AGC Networks Flair Agent Workspace did not include use of any specific encryption features as requested by AGC Networks.

## 2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

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

## 2.2. Test Results

All test cases were executed. The following were observations on Flair Agent Workspace from the compliance testing.

- Flair Agent Workspace does not support origination of a new call, but it can transfer/conference/consulted call that it has received and answered.

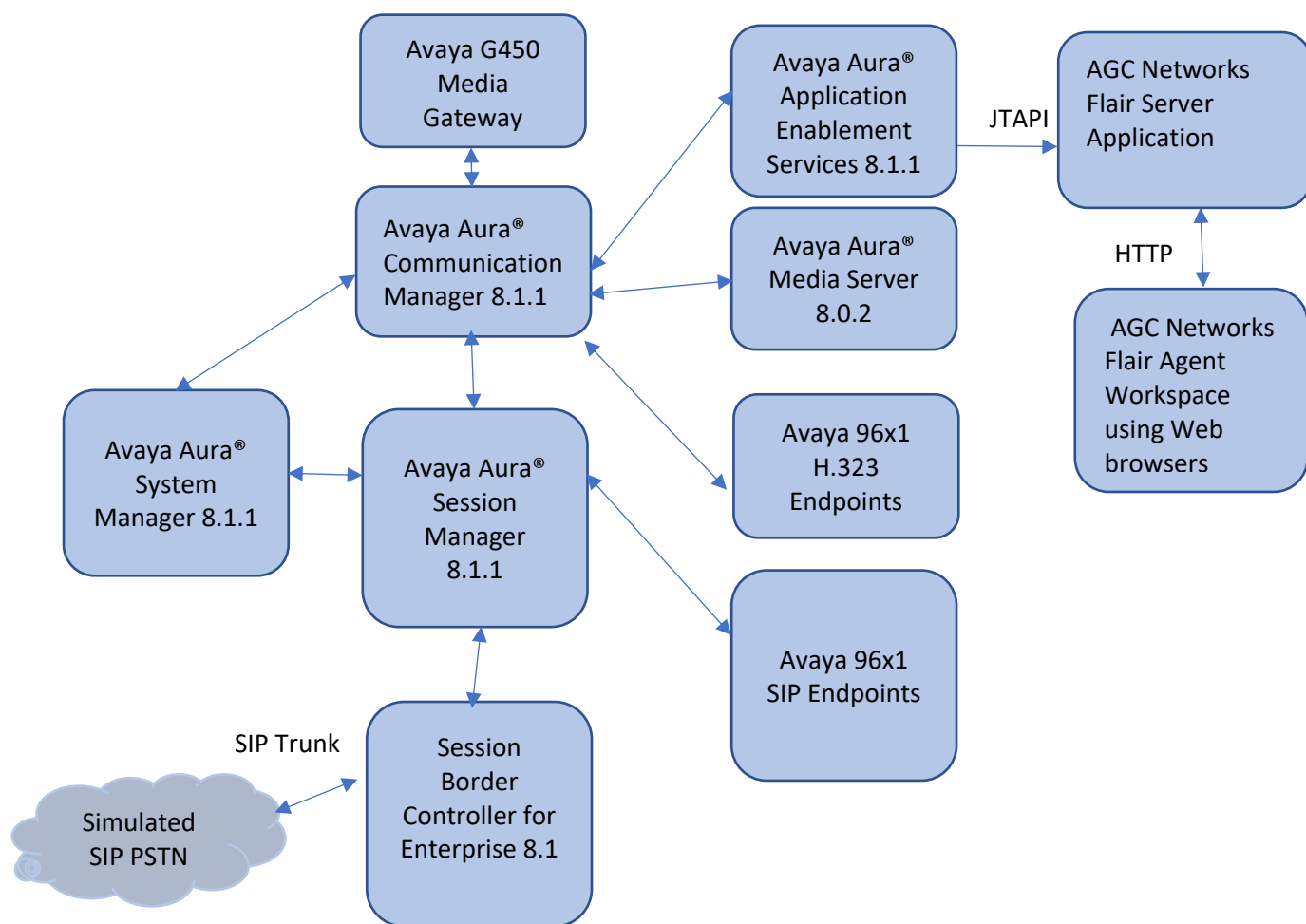
## 2.3. Support

Technical support can be obtained for the Flair Agent Workspace solution as follows:

**Email:** [AppsSupport.Group@agcnetworks.com](mailto:AppsSupport.Group@agcnetworks.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.



**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	8.1.1
Avaya Aura® Session Manager in Virtual Environment	8.1.1
Avaya Aura® Communication Manager in Virtual Environment	8.1.1-FP1
Avaya G450 Media Gateway	41.9.0
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.1
Avaya Session Border Controller for Enterprise	8.0.1.1
Avaya 9621G & 9641G IP Desk phone (SIP)	7.1.8
Avaya 9608G & 9641G IP Desk phone (H.323)	6.8.3
AGC Networks Flair Agent Workspace	1.0.0

## 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	<b>Computer Telephony Adjunct Links? y</b>	
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		
<b>Extension: 79999</b>		
<b>Type: ADJ-IP</b>		
<b>Name: aes95</b>	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 **100** 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**.

<b>add hunt-group 2</b>	Page 1 of 4
HUNT GROUP	
Group Number: 2	ACD? y
Group Name: Voice Service	Queue? y
Group Extension: 88100	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.

<b>add hunt-group 2</b>	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.

<b>add agent-loginID 80000</b>		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 **2** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.

<b>add agent-loginID 80000</b>		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: 2	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.

## 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

A login form with a light blue border. It contains the text "Please login here:" followed by "Username" and a text input field. Below the input field is a button labeled "Continue".

Copyright © 2009-2019 Avaya Inc. All Rights Reserved.

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

# AVAYA Application Enablement Services

## Management Console

Welcome: User cust  
Last login: Thu Feb 20 13:22:10 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Thu Feb 20 13:45:33 IST 2020  
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.

## 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 20 13:22:10 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Thu Feb 20 13:46:53 IST 2020  
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

▶ Security

**Licensing**

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰ | admin

Home | **Licenses**

Licenses ^

Licensed products

APPL\_ENAB

▼ Application\_Enablement

View license capacity

View peak usage

CE

► COLLABORATION\_ENVIRONMENT

COLLABORATION\_DESIGNER

► Collaboration\_Designer

MESSAGING

► Messaging

MSR

► Media\_Server

SYSTEM\_MANAGER

► System\_Manager

SessionManager

► SessionManager

Uninstall license

Server properties

Shortcuts

Help for Licensed products

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: December 28, 2018 11:22:53 AM +07:00

**License File Host IDs:** V0-55-3B-33-B4-26-01


**Licensed Features**

13 Items Show All ▾

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

### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Feb 20 13:22:10 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Thu Feb 20 13:53:17 IST 2020  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services


- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<div>Add LinkEdit LinkDelete Link</div>				

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.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 16 07:24:52 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Mon Mar 16 07:37:10 IST 2020  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link1

Switch ConnectionCM93

Switch CTI Link Number1

ASAI Link Version9


SecurityBoth

Apply ChangesCancel ChangesAdvanced Settings

## 6.4. Administer Avaya 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: Thu Feb 20 13:22:10 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Thu Feb 20 13:58:35 IST 2020  
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 Idavaya

\* Common Nameavaya

\* Surnameavaya

\* 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

## 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 Avaya user from **Section 6.4**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Thu Feb 20 13:22:10 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Thu Feb 20 14:00:10 IST 2020  
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

**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 Flair Workspace.

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: Mon Mar 16 07:24:52 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Mon Mar 16 07:41:58 IST 2020  
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#CM93#CSTA#AES95

Delete Tlink

## **7. Configure AGC Networks Flair Agent Workspace**

This section provides the procedures for configuring AGC Networks Flair Agent Workspace. The procedures include the following areas:

- Flair Server Configuration
- Flair Agent Workspace Application Configuration

### **7.1. Flair Server Configuration**

This section outlines the steps required to configure the connections from Flair Server to Application Enablement Services. These Application Notes assume that Flair Server is already installed.

In order to do this, go to the installation folder of the Flair Server application.

*C:\Program Files\AGC Networks\Flair\FlairServer*

Locate the file named Flair.properties. This is the configuration file which has all the information needed to run the flair server application. Below show configuration values:

Configuration	Description
CTI_LINK:	TSAPI Link (TLINK) for connecting to the TSAPI link as configured in <b>Section 6.3</b>
CTI_USER_ID:	User ID created while generating the TSAPI Link as configured in <b>Section 6.4</b>
CTI_PASSWORD	Password created while generating the TSAPI Link as configured in <b>Section 6.4</b>
AGENT_HUNT_GROUPS	Agent Hunt Groups that are to be monitored as configured in <b>Section 5.3.1</b>
WEB_SOCKET_PORT	Port on which flair server application should run. (Default 9092)

```

# Main Configuration File for AGC FLAIR

#-----Mumbai CEC new AES-----#
CTI_LINK = AVAYA#CM93#CSTA#AES95
CTI_USER_ID = Avaya
CTI_PASSWORD = Av@ya123

#-- Make sure file exists in classpath with name FLAIRDB.db --#
DATABASE_FILENAME = FLAIRDB

#--Threads allotted for jtaapi event processing --#
MAX_THREADS_FOR_EVENT_LISTENERS = 100

#-- PORT on which websocket server should run. Flair AWS client needs access to the flair server o
WEB_SOCKET_PORT = 9092

#-- This is used to add to Socket.IO, and is added in response header. Used to fix CORS issue--#
FLAIR_CLIENT_HOSTNAME = http://10.30.5.98:8000

#-- List of ACD Addresses to monitor (Add Comma Separated List)--#
AGENT_HUNT_GROUPS = 88100

#-- Frequency for checking JTAapi connection. This is used for re-connecting to JTAapi in case of co
PROVIDER_WATCHDOG_PERIOD_MS = 30000

#-- Frequency for checking JTAapi connection. This is used for re-connecting to JTAapi in case of co
PROVIDER_WATCHDOG_PERIOD_MS = 30000

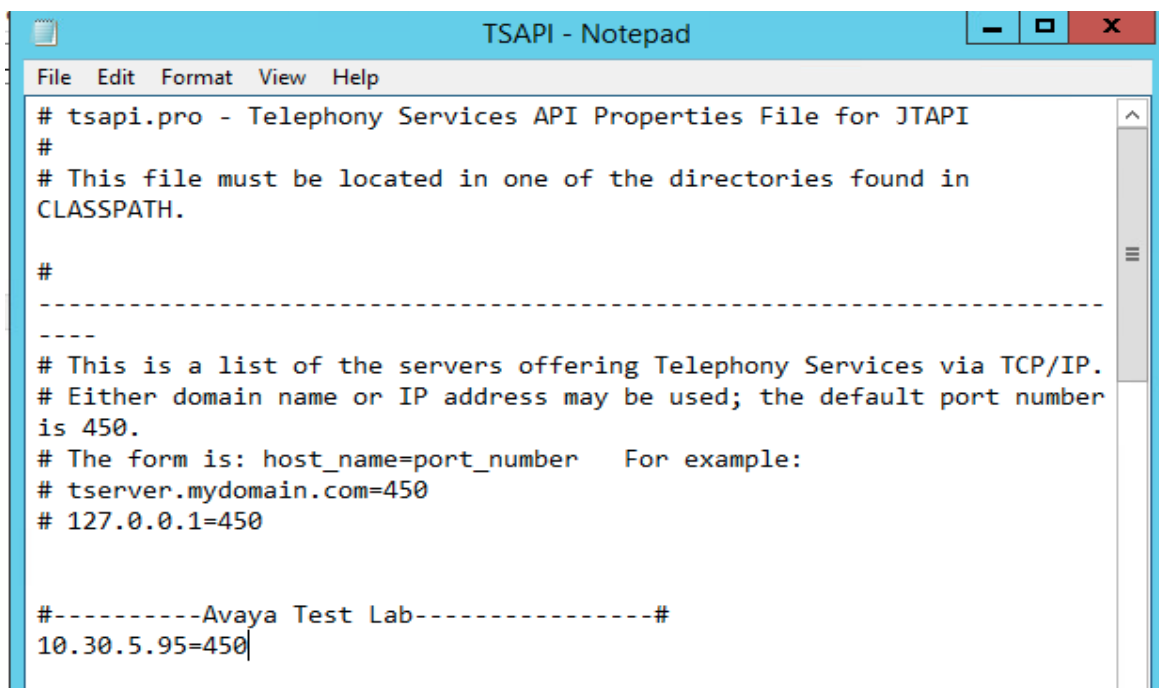
#-- Time in milliseconds after which session will be removed on browser tab or window close --#
SESSION_REMOVE_DELAY = 10000

```

Below properties are used for administrative purposes. If needed, these are configured by the assigned AGC Networks engineer, but for most installations, the default configurations are sufficient.

Configuration	Description
<b>MAX_THREADS_FOR_EVENT_LISTENERS</b>	Threads allotted for JTAPI event processing (Default 100)
<b>FLAIR_CLIENT_HOSTNAME</b>	URL on which flair client application is running. (Check the Flair Client Installation Section for more details on the port)
<b>PROVIDER_WATCHDOG_PERIOD_MS</b>	Frequency for checking JTAPI connection. This is used for re-connecting to JTAPI in case of connectivity or similar issues (Default 30 seconds)

TSAPI.PRO is the standard configuration file which has information related to the AES server required by JTAPI. This file will have the hostname and the port number of the AES server as shown in the figure below:



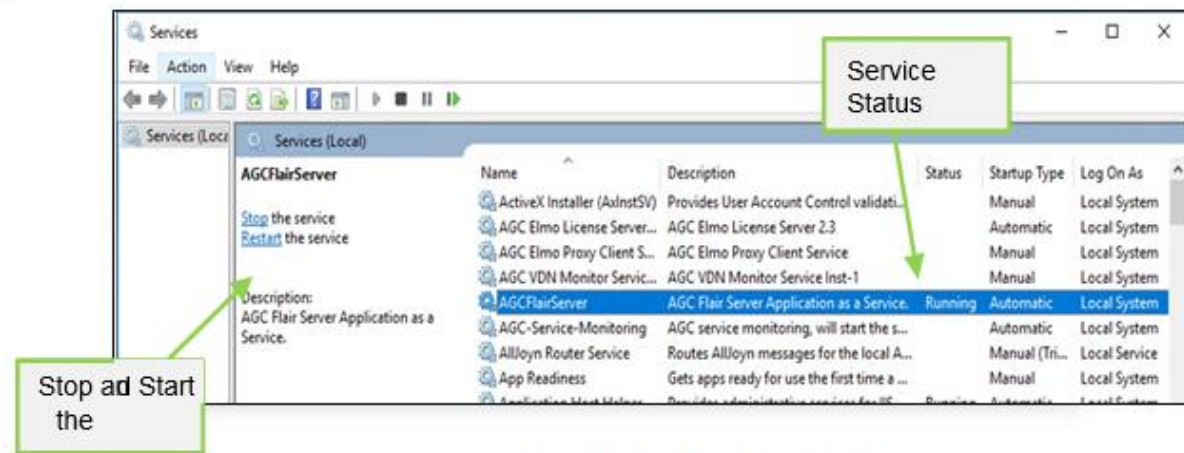
```

# tsapi.pro - Telephony Services API Properties File for JTAPI
#
# This file must be located in one of the directories found in
# CLASSPATH.
#
-----
# This is a list of the servers offering Telephony Services via TCP/IP.
# Either domain name or IP address may be used; the default port number
# is 450.
# The form is: host_name=port_number   For example:
# tserver.mydomain.com=450
# 127.0.0.1=450
#-----Avaya Test Lab-----#
10.30.5.95=450

```

Once the configuration steps are complete, one can now run the application.

- Open the Windows Service Manager - press Win+R and enter Services.msc. Select the **AGCFlairServer** service (see figure below).
- Use the pane on the left and Click on “Start the service”. This starts the service, and the service status changes to Running.
- Once the service is running, this option will change to “Stop the service”. Use this option to stop the application if needed.



## 7.2. Flair Workspace Application Configuration

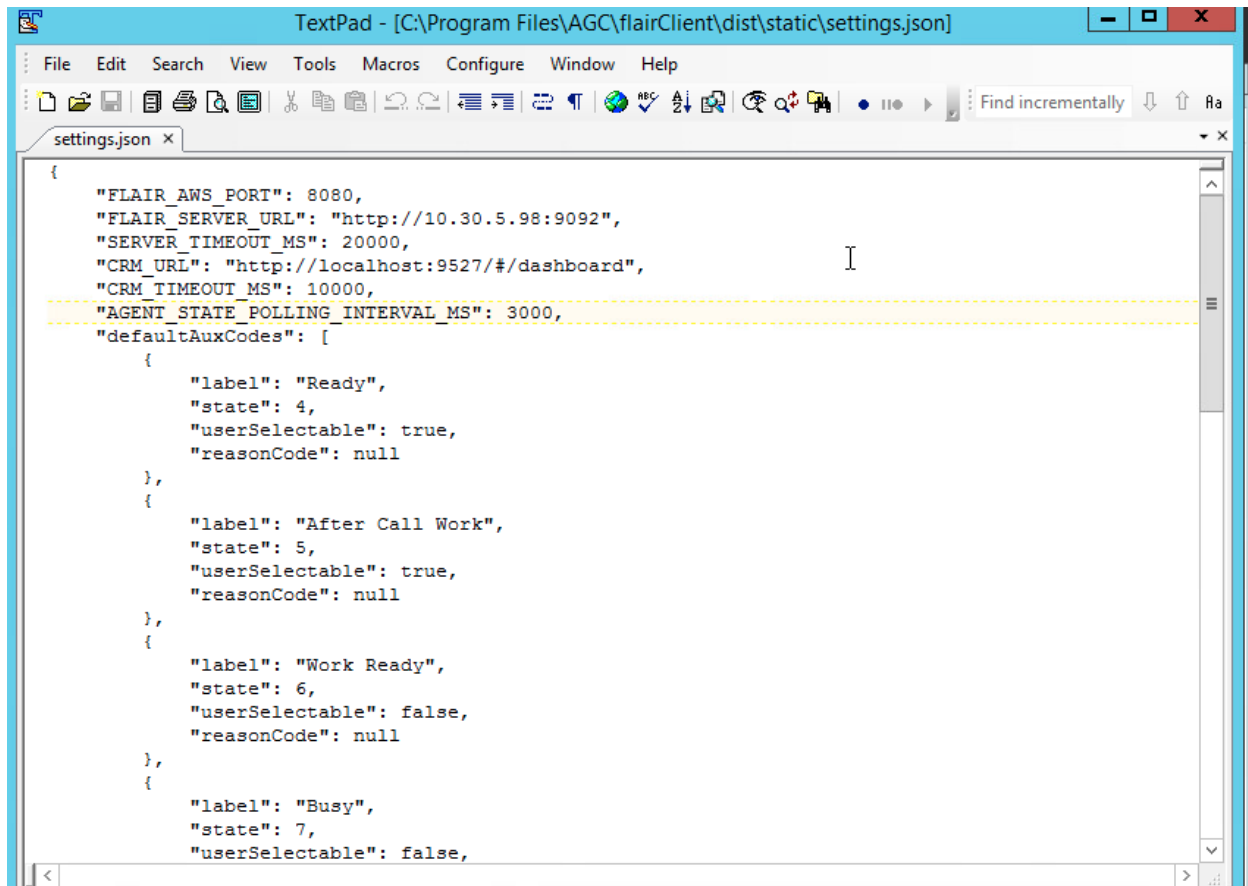
The Flair Workspace application is a browser-based application that is hosted on a central server. In typical deployment configurations, the Flair Server and Workspace applications may be deployed on the same physical or virtual windows server, however they may also be deployed in separate servers. The Application Notes assume that Flair Client is already installed.

Navigate to the location where the Flair Workspace Application is installed. Locate the folder named **public**, which contains the configuration file named settings.json. The following figure shows the configurable parameters, with values below:

Configuration	Description
<b>FLAIR_AWS_PORT</b>	Port on which to run the application. (Default: 8000)
<b>FLAIR_SERVER_URL</b>	URL on which flair server application is running. (Check the FLAIR Server Installation Section for more details on the port) (Default: <ServerIP>:9092)
<b>SERVER_TIMEOUT_MS</b>	Timeout in milliseconds for communication with Flair Server. Default (20000 ms / 20 seconds)
<b>AGENT_STATE_CODES</b>	List of agent states to be displayed in the Agent State Selection Dropdown.
<b>AGENT_STATE_CODES</b> o <b>Label</b>	The label to be displayed to the user in the dropdown selection
<b>AGENT_STATE_CODES</b> o <b>state</b>	The value of the Agent State as specified by Avaya JTAPI specifications
<b>AGENT_STATE_CODES</b> o <b>userSelectable</b>	Boolean flag to indicate whether this state can be manually selected from the dropdown. If false, it can only be set by the system upon certain telephony/agent events
<b>AGENT_STATE_CODES</b> o <b>reasonCode</b>	The Reason code associated with the Agent State. It will be null for all states other than AGENT_NOT_READY (State 3)
<b>AUX_REASON_CODE_LIST</b>	The list of reason codes to be displayed in the agent state selection dropdown, for Aux (Agent Not Ready)
<b>AUX_REASON_CODE_LIST</b> o <b>reasonCode</b>	The value of the reason code configured in Communication Manager (CM)

**AUX\_REASON\_CODE\_LIST**  
**o reasonLabel**

The user friendly display label for the reason code

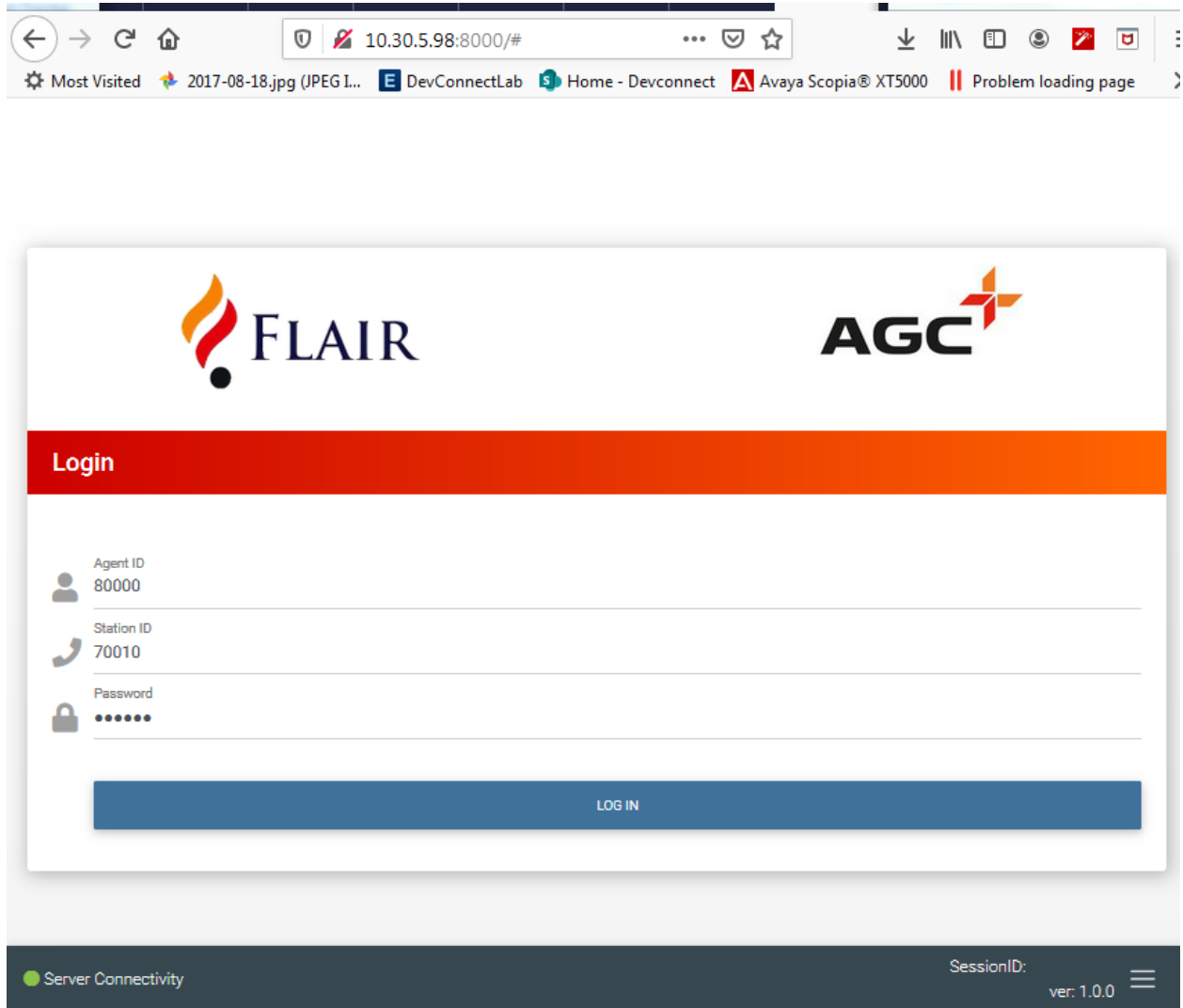


```
TextPad - [C:\Program Files\AGC\flairClient\dist\static\settings.json]
File Edit Search View Tools Macros Configure Window Help
Find incrementally
settings.json x
{
  "FLAIR_AWS_PORT": 8080,
  "FLAIR_SERVER_URL": "http://10.30.5.98:9092",
  "SERVER_TIMEOUT_MS": 20000,
  "CRM_URL": "http://localhost:9527/#/dashboard",
  "CRM_TIMEOUT_MS": 10000,
  "AGENT_STATE_POLLING_INTERVAL_MS": 3000,
  "defaultAuxCodes": [
    {
      "label": "Ready",
      "state": 4,
      "userSelectable": true,
      "reasonCode": null
    },
    {
      "label": "After Call Work",
      "state": 5,
      "userSelectable": true,
      "reasonCode": null
    },
    {
      "label": "Work Ready",
      "state": 6,
      "userSelectable": false,
      "reasonCode": null
    },
    {
      "label": "Busy",
      "state": 7,
      "userSelectable": false,
```



### 7.3. Log-into Flair Agent Workspace with Avaya hard-phone or softphone

Enter the Flair Server URL in the browser. This brings up the **Login** Screen

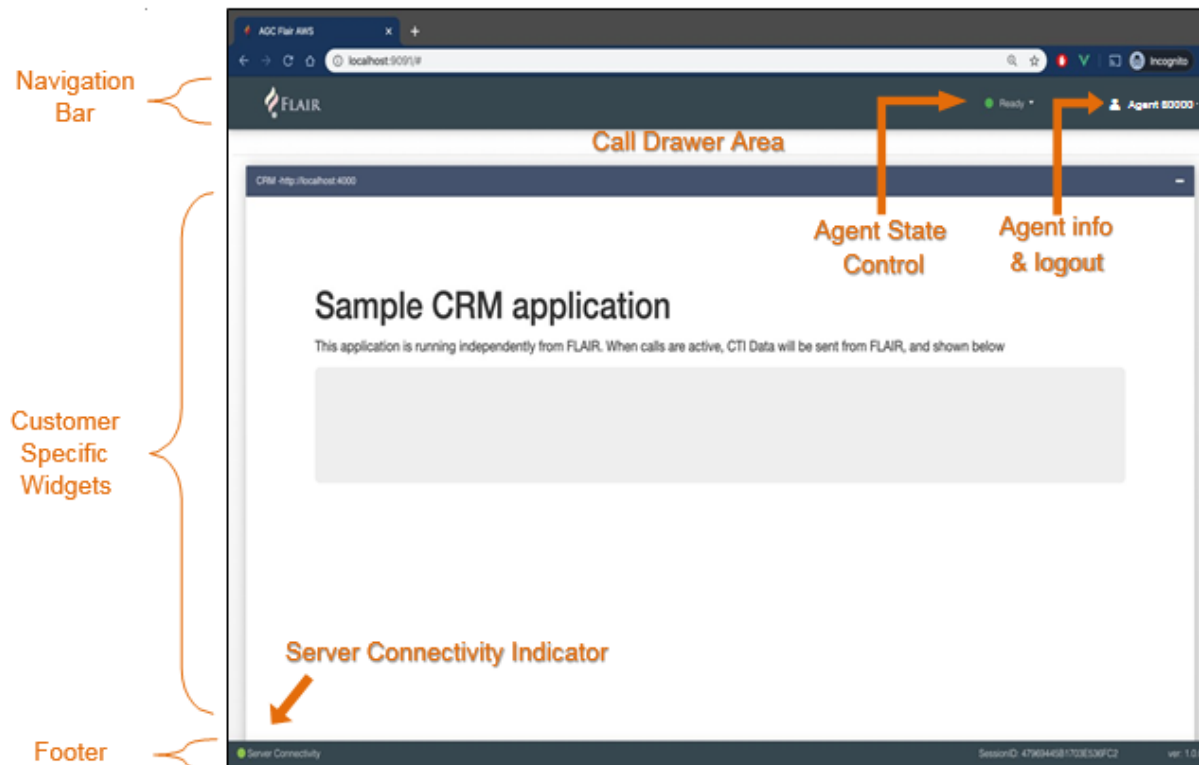


The screenshot shows a web browser window with the address bar displaying "10.30.5.98:8000/#". The browser's tab bar includes "Most Visited", "2017-08-18.jpg (JPEG I...", "DevConnectLab", "Home - Devconnect", "Avaya Scopia® XT5000", and "Problem loading page". The main content area displays the "FLAIR" and "AGC" logos at the top. Below the logos is a red "Login" header. The login form contains three input fields: "Agent ID" with the value "80000", "Station ID" with the value "70010", and "Password" with masked characters ".....". A blue "LOG IN" button is positioned below the password field. At the bottom of the page, a dark grey footer bar shows "Server Connectivity" with a green status indicator, "SessionID:" followed by "ver: 1.0.0", and a hamburger menu icon.

Enter the following:

- The Agent ID as configured in **Section 5.3.2**.
  - Device ID / Extension: This is the extension from which to Log-In.
  - Password: The Avaya Agent Password as configured in CM.
- Click on the LOG-IN button. This will Log you into the application.

Once logged in, one will be presented with the home page of the application, also referred to as the “Dashboard” in this guide.



## 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 AGC Networks Flair Agent Workspace 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** shown in **Section 5.4** is logged-in to extension **70010**.

```
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	70010						1	lvl
	2/01	/	/	/	/	/	/	/	

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	
2/AI	/	/	/	/	/	/	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**, and that the **Associations** column reflects the total number of agents, in this case “2”.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 16 07:35:39 2020 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: 8.1.1.0.0.8-0  
Server Date and Time: Tue Mar 17 07:28:29 IST 2020  
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	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 **Avaya** user with the **Tlink**.

▶ 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

**CTI User Status**

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 3

Closed Streams 7

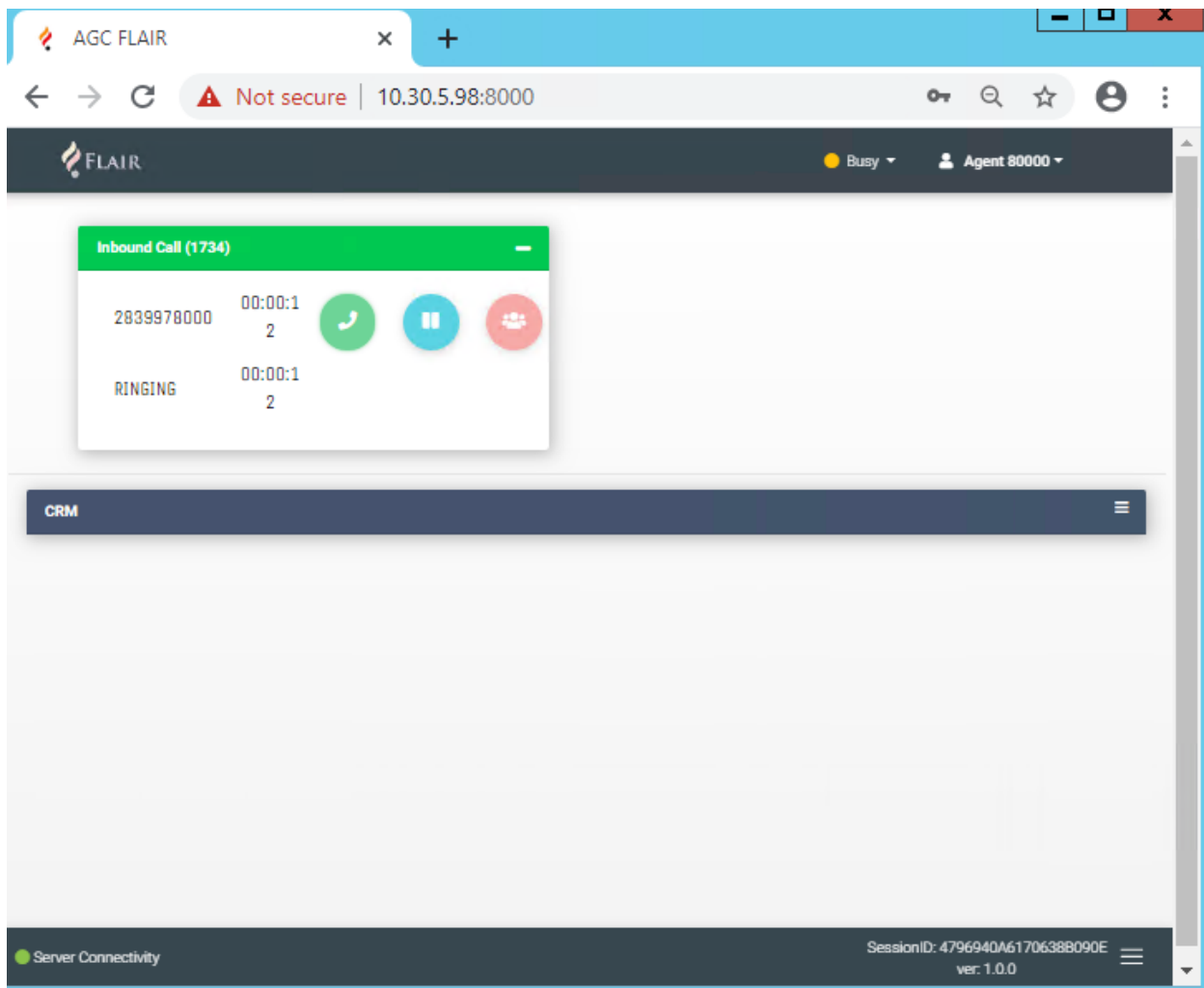
**Open Streams**

Name	Time Opened	Time Closed	Tlink Name
Avaya	Thu 20 Feb 2020 03:18:44 PM IST		AVAYA#CM93#CSTA#AES95
DMCCLCSUserDoNotModify	Tue 04 Feb 2020 03:59:37 PM IST		AVAYA#CM93#CSTA#AES95
DMCCLCSUserDoNotModify	Tue 04 Feb 2020 03:59:37 PM IST		AVAYA#CM93#CSTA#AES95

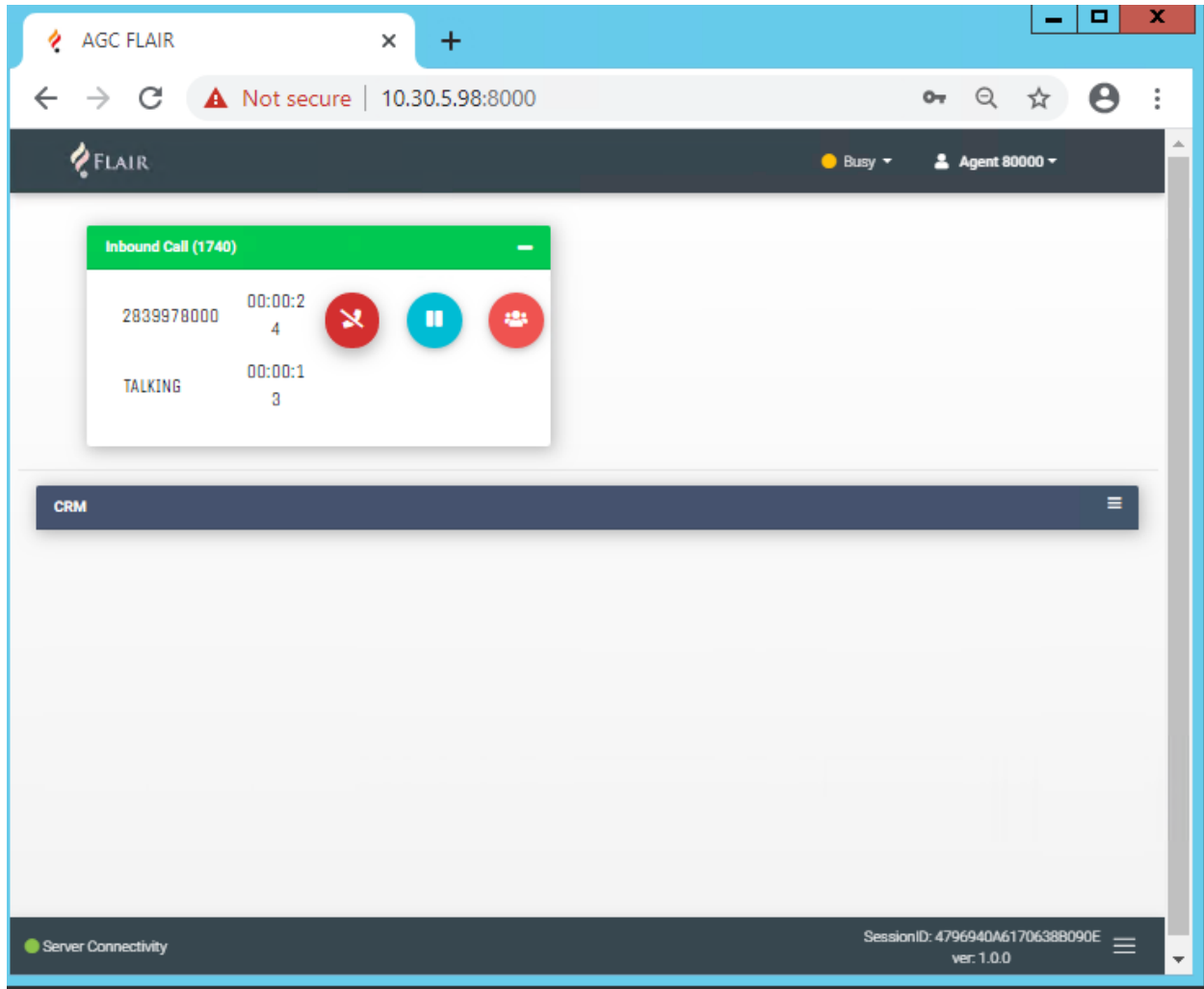
Show Closed StreamsClose All Opened StreamsBack

## 8.4. Verify Flair Agent Workspace call handling and user status

Place a call to VDN/Hunt Group. Verify that Flair Agent Workspace can receive incoming call:



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



## 9. Conclusion

These Application Notes describe the configuration steps required for the AGC Networks Flair Agent Workspace 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 AGC Networks 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, Issue 2.0, Nov 2018*
2. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
3. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.0.1, Issue 2, December 2018*

Product Documentation for AGC Flair Agent Workspace can be requested from AGC Networks:

1. *FLAIR Agent Workspace Installation and Configuration Guide, 2019*



---

**©2020 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](mailto:devconnect@avaya.com).