



Avaya Solution & Interoperability Test Lab

Application Notes for Geomant Buzzeasy Agent Desktop 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 for Geomant Buzzeasy Agent Desktop to interoperate with Avaya Aura[®] Communication Manager 8.1 and Avaya Aura[®] Application Enablement Services 8.1. Buzzeasy Agent Desktop provides a cloud-based service that allows an attendant to monitor and manipulate calls and devices.

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 for Geomant Buzzeasy Agent Desktop to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1.

Geomant Buzzeasy Cloud Services is a cloud application which, using the Telephony Services Applications Programmers Interface (TSAPI) of Avaya Aura® Application Enablement Services, allows an attendant to monitor, and manipulate calls and devices.

2. General Test Approach and Test Results

The general test approach was to configure Geomant Buzzeasy on-premise connector to communicate with the Avaya Aura® Communication Manager 8.1, Avaya Aura® Application Enablement Services 8.1 via TSAPI and communicate with Buzzeasy Cloud Service. Testing was performed by calling inbound to an available agent and using HTTPS Buzzeasy Cloud Service to monitor, and manipulate calls and devices.

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 Buzzeasy did not include use of any specific encryption features as requested by Geomant.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third-party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third-party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third-party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The testing focuses on the following areas:

- **Change Agent state** – Agent connect to Extension for receive Voice, Calls, Auto Mode, Take a Break using Geomant Buzzeasy Agent Desktop.
- **Inbound Calls** – Answer calls using Geomant Buzzeasy Agent Desktop.
- **Outbound Calls** – Make calls using Geomant Buzzeasy Agent Desktop.
- **Hold/Transfer**– Place callers on hold and transfer using Geomant Buzzeasy Agent Desktop.
- **Failover Testing** - Verify the ability of Geomant Buzzeasy Buzzeasy Agent Desktop to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All test cases were completed successfully with the following observations.

- Geomant Buzzeasy Agent Desktop does not support Conference.
- Geomant Buzzeasy Agent Desktop does not show an error when connect to Invalid Extension.

2.3. Support

Technical Support can be obtained for Geomant products from the following.

Web: www.geomant.com

Email: products@geomant.com

Telephone: +441789 387900

3. Reference Configuration

The configuration shown in **Figure 1** was used during the compliance test of Buzzeasy Cloud Services with Avaya Aura® Communication Manager and Application Enablement Services.

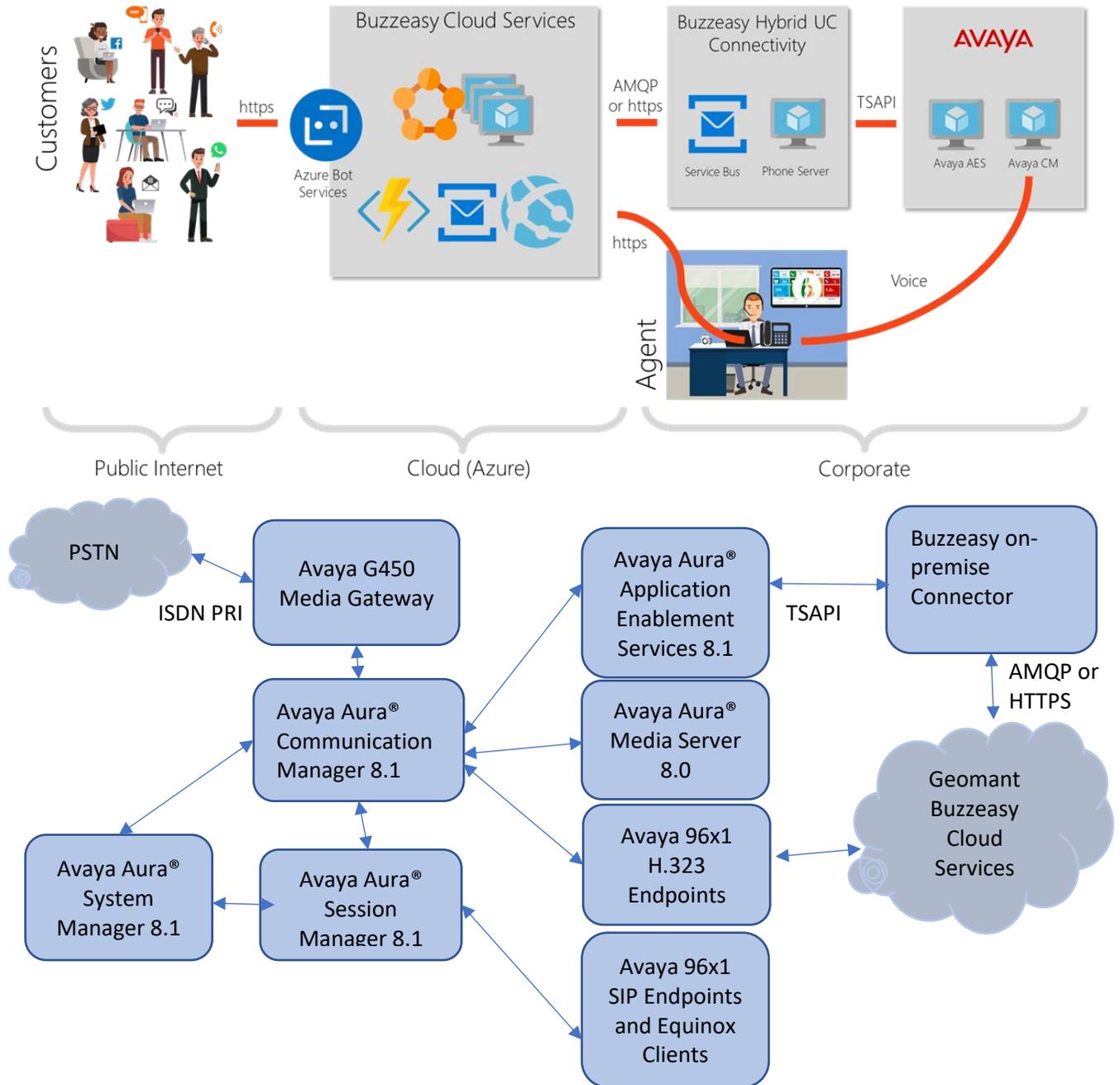


Figure 1: Buzzeasy with Avaya Aura® Communication Manager and Application Enablement Services.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.0.1 – SP1
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	8.1.0.0.0.9-1
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya Aura® Application Enablement Services TSAPI Clients	8.1.9
Geomant Buzzeasy on-premise Connector Geomant Buzzeasy Agent Desktop	1.3.1

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link

5.1. Verify License

Log 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: aes8
    COR: 1
```

6. Configure Avaya Aura® Application Enablement Services

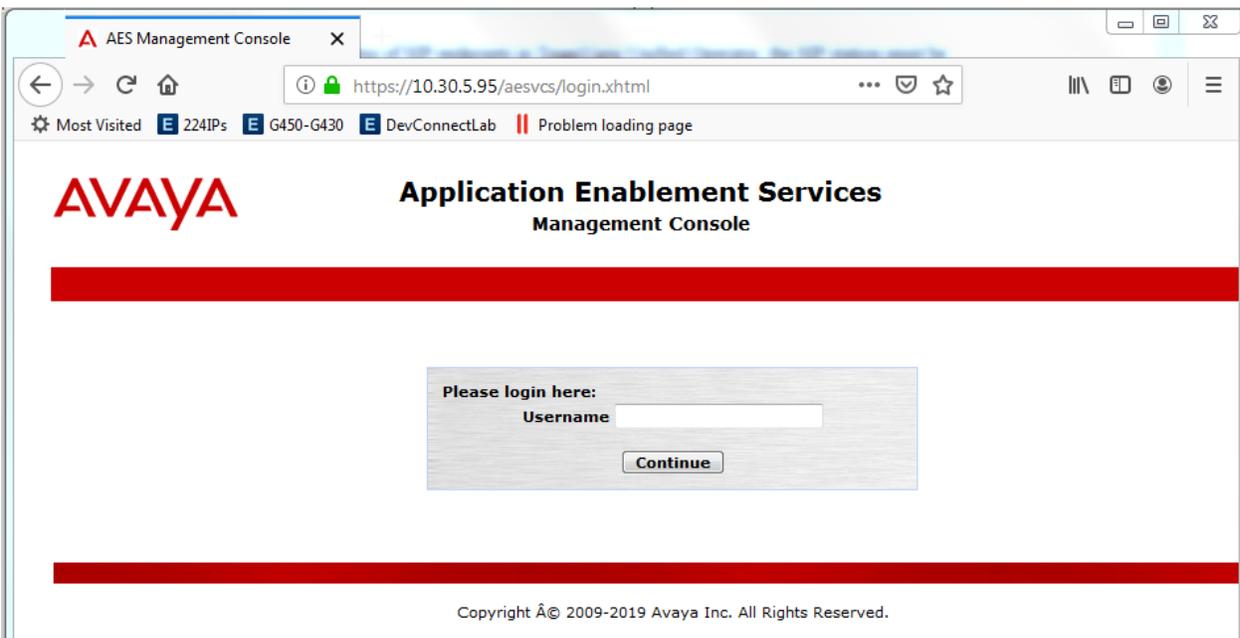
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The Welcome to OAM screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar is red with 'Home' on the left and 'Home | Help | Logout' on the right. A left sidebar contains a menu with items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and contains the following text:

Welcome: User cust
Last login: Thu Aug 15 15:41:45 2019 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: 8.1.0.0.0.9-1
Server Date and Time: Fri Aug 16 13:19:44 IST 2019
HA Status: Not Configured

Welcome to OAM

This AE Services server is using a default installed server certificate. Default installed certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates.

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 © 2009-2019 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).

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' menu item selected in the left sidebar. The main content area is titled 'Licensing' and contains the following text:

Welcome: User cust
Last login: Thu Aug 15 15:41:45 2019 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: 8.1.0.0.0.9-1
Server Date and Time: Fri Aug 16 13:20:56 IST 2019
HA Status: Not Configured

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 and Device Media and Call Control**, as shown below. The TSAPI license is used for device monitoring and the DMCC license is used for the virtual IP softphones. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**, which is needed for adjunct routing.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Application Enablement (CTI) - Release: 8 - SID: 10503000'. Below the title, it indicates the current location: 'Licensed Products > Application_Enablement > View License Capacity'. The license was installed on June 26, 2019, at 4:19:06 PM +07:00. The license file host ID is V6-8D-06-02-18-AC-01. The 'Licensed Features' section shows 13 items with a table listing features, their expiration dates, and licensed capacities.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	500
AES HA LARGE VALUE_AES_HA_LARGE	permanent	500
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	500
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	500
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	500
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	500
DLG VALUE_AES_DLG	permanent	500
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	500
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	500

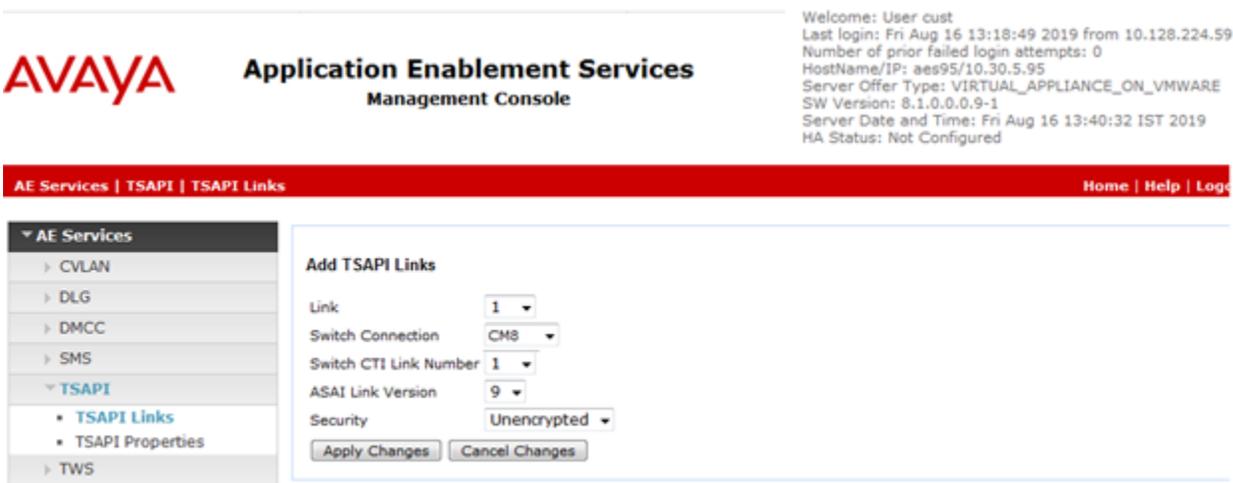
6.3. Administer TSAPI Link

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 **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 “CM8” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “CM”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.0.9-1, Server Date and Time: Fri Aug 16 13:40:32 IST 2019, HA Status: Not Configured. The main navigation pane on the left includes AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, Maintenance, and Networking. The central content area is titled 'Switch Connections' and features an 'Add Connection' button and a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> CM8	Yes	30	1

Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.30.5.93” as shown below. Click **Add Name or IP**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.0.9-1, Server Date and Time: Fri Aug 16 13:40:32 IST 2019, HA Status: Not Configured. The main navigation pane on the left includes AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, and Maintenance. The central content area is titled 'Edit H.323 Gatekeeper - CM8' and features a text input field containing '10.30.5.93', an 'Add Name or IP' button, and 'Delete IP' and 'Back' buttons.

6.5. Administer Buzzeasy 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 Aug 16 13:30:24 2019 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: 8.1.0.0.9-1
Server Date and Time: Fri Aug 16 14:38:06 IST 2019
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ **User Management**
 - ▶ Service Admin
 - ▼ **User Admin**
 - **Add User**
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- ▶ Utilities
- ▶ Help

Add User

Fields marked with * can not be empty.

* User Id	<input type="text" value="buzzeasy"/>
* Common Name	<input type="text" value="buzzeasy"/>
* Surname	<input type="text" value="buzzeasy"/>
* User Password	<input type="password" value="••••••"/>
* Confirm Password	<input type="password" value="••••••"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>

6.6. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. 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 Buzzeasy user from **Section 6.5**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User cust, Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.0.9-1, Server Date and Time: Fri Aug 16 13:40:32 IST 2019, HA Status: Not Configured.

The main interface features a red navigation bar with "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various services, with "Security Database" expanded to show "Control".

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane. In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



Application Enablement Services
Management Console

Welcome: User cust
 Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.9-1
 Server Date and Time: Fri Aug 16 13:40:32 IST 2019
 HA Status: Not Configured

Networking | Ports
Home | Help | Logout

- > AE Services
- > Communication Manager
- > Interface
- > High Availability
- > Licensing
- > Maintenance
- > Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP/TLS Settings
- > Security
- > Status
- > User Management
- > Utilities
- > Help

Ports

CVLAN Ports		Enabled	Disabled
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>	<input type="radio"/>	<input type="radio"/>

DLG Port	TCP Port	Value
		5678

TSAPI Ports		Enabled	Disabled
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
Encrypted TLINK Ports			
TCP Port Min	<input type="text" value="1066"/>		
TCP Port Max	<input type="text" value="1081"/>		

DMCC Server Ports		Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>	<input type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>	<input type="radio"/>	<input type="radio"/>

H.323 Ports	
TCP Port Min	<input type="text" value="20000"/>
TCP Port Max	<input type="text" value="29999"/>
Local UDP Port Min	<input type="text" value="20000"/>
Local UDP Port Max	<input type="text" value="29999"/>

6.8. Administer TCP Settings

Select **Networking** → **TCP/TLS Settings** from the left pane, to display the **TCP/TLS Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration (6)**, as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". In the top right corner, a welcome message is shown: "Welcome: User cust", "Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.0.9-1", "Server Date and Time: Fri Aug 16 13:40:32 IST 2019", and "HA Status: Not Configured".

A red navigation bar at the top contains "Networking | TCP / TLS Settings" on the left and "Home | Help | Logout" on the right. On the left side, a vertical menu lists various sections: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking" (which is expanded to show "AE Service IP (Local IP)", "Network Configure", "Ports", and "TCP/TLS Settings"), "Security", "Status", "User Management", "Utilities", and "Help".

The main content area is titled "TCP / TLS Settings". It includes the following sections:

- TLSv1 Protocol Configuration:** Three checkboxes are present: "Support TLSv1.0 Protocol" (unchecked), "Support TLSv1.1 Protocol" (unchecked), and "Support TLSv1.2 Protocol" (checked).
- TCP Retransmission Count:** Two radio buttons are present: "Standard Configuration (15)" (unchecked) and "TSAPI Routing Application Configuration (6)" (checked).

Below these settings are three buttons: "Apply Changes", "Restore Defaults", and "Cancel Changes".

A note at the bottom of the settings area reads: "Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications." A warning follows: "Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution."

6.9. 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](#)

6.10. 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.

In this case, the associated Tlink name is “AVAYA#**CM8**#CSTA#**AES8**”. Note the use of the switch connection “CM8 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 system information: Welcome: User cust, Last login: Fri Aug 16 13:18:49 2019 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: 8.1.0.0.0.9-1, Server Date and Time: Fri Aug 16 13:40:32 IST 2019, HA Status: Not Configured.

The main interface features a red navigation bar with "Security | Security Database | Tlinks" and "Home | Help | Logout". On the left, a sidebar menu lists various services, with "Security Database" expanded to show "Tlinks" selected. The main content area, titled "Tlinks", displays a single Tlink entry with the name "AVAYA#CM8#CSTA#AES8" and a "Delete Tlink" button.

7. Configure Geomant Buzzeasy Agent Desktop on premise connector

This section provides the procedures for configuring Buzzeasy Agent Desktop on premise connector. The procedures include the following areas:

- Install Avaya TSAPI Client
- Install Buzzeasy Avaya Call connector

7.1. Install Avaya TSAPI Client

The Avaya TSAPI client is available for download from the DevConnect Support Site. Double click on the **setup** application and follow the intuitive instructions. When the **AE Services Server Configuration** screen is displayed, enter the **IP Address** of the Application Enablement Services Server, and **Port Number 450** and click **Add to List**, as shown below.

Avaya Application Enablement Services TSAPI Client - InstallShield Wizard

AE Services Server Configuration
Configure your PC for AE Services TSAPI access.

AVAYA

For each AE Services server that you wish to use, enter the server's host name or IP address (for example, aeserver.mydomain.com or 198.51.100.24) and the TSAPI Service port number.
The configured AE Services servers will be saved in the TSLIB.INI file.

Host Name or IP Address: 10.30.5.95 Port Number: 450 Add to List

Configured AE Services Servers:
10.30.5.95=450 Delete

InstallShield

< Back Next > Cancel

Click **Next** and follow the instructions to complete the installation of the TSAPI client.

7.2. Install Buzzeasy Avaya Call connector

Follow these steps to install the on-premise call connector

1. Download the "**CallControllerWinSvc.zip**" ZIP file from Geomant website
2. Extract ZIP file content in the folder you want to install the Call Controller e.g. **C:\ProgramFiles\Buzzeasy Avaya Call Controller**
3. Start Powershell with Administrator privileges
4. Navigate to Call Controller folder e.g. cd 'C:\Program Files\Buzzeasy Avaya Call Controller\'
5. Authorize non digitally signed Powershell scripts to run by executing the following command:
Set -ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

6. When prompted choose Y
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust.
Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at <https://go.microsoft.com/fwlink/?LinkID=135170>.
Do you want to change the execution policy ?[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
7. Run the *Install-CallController.ps1* Powershell script, specifying the following parameters:
 - a. TSAPI link id, used to connect to the Avaya AES server
 - b. TSAPI user name and account that is administered as a CT user on Avaya Application Enablement Services server
 - c. Service Bus connection string - Get in touch with Geomant DevOps to get a hold of your connection string.

```
.\Install-CallController.ps1  
TsapiLinkId='AVAYA#CM8#CSTA#AES8'TsapiUserName='buzzeasy'  
TsapiPassword='Avaya321'ServiceBusConnectionString='Endpoint=myEndpoint;Shared  
SecretIssuer=myWrapAuthenticationName;SharedSecretValue=myWrapPassword;
```

8. Verification Steps

8.1. 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 agent, in this case “1”.

The screenshot shows the Avaya Aura® Application Enablement Services (AES) interface. The top navigation bar displays "Status | Status and Control | TSAPI Service Summary" and "Home | Help | Logout". The left navigation menu is expanded to "Status and Control", with "TSAPI Service Summary" selected. The main content area is titled "TSAPI Link Details" and includes a checkbox for "Enable page refresh every 60 seconds". Below this is a table with the following data:

	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	CM8	1	Talking	Mon May 20 18:12:03 2019	Online	18	1	6450	6461	30

Below the table are buttons for "Online" and "Offline". At the bottom, there is a section for "For service-wide information, choose one of the following:" with buttons for "TSAPI Service Status", "TLink Status", and "User Status".

8.2. 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 buzzeasy user with the **Tlink**.

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**

CTI User Status

Enable page refresh every 60 seconds

CTI Users: All Users

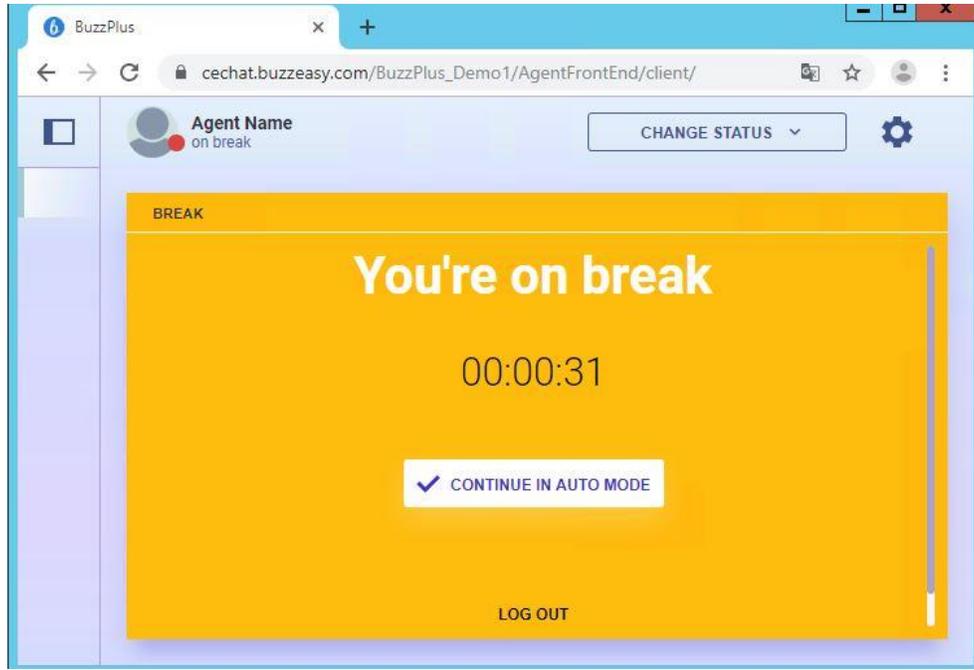
Open Streams: 3
Closed Streams: 0

Open Streams

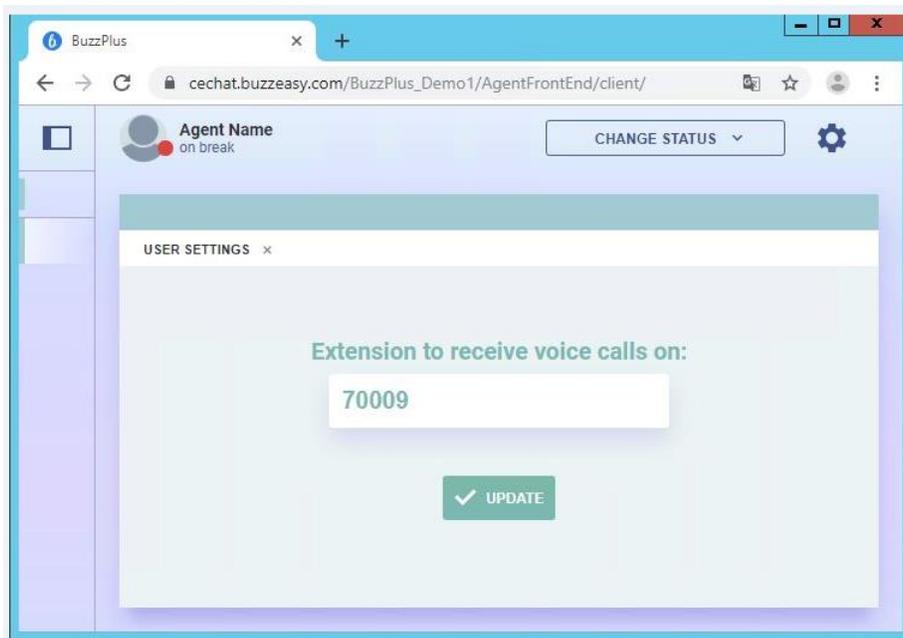
Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Thu 06 Jun 2019 05:06:07 PM +07		AVAYA#CM8#CSTA#AES8
DMCCLCSUserDoNotModify	Thu 06 Jun 2019 05:06:07 PM +07		AVAYA#CM8#CSTA#AES8
buzzeasy	Thu 06 Jun 2019 05:07:30 PM +07		AVAYA#CM8#CSTA#AES8

8.3. Verify Buzzeasy Cloud Services handling and user status

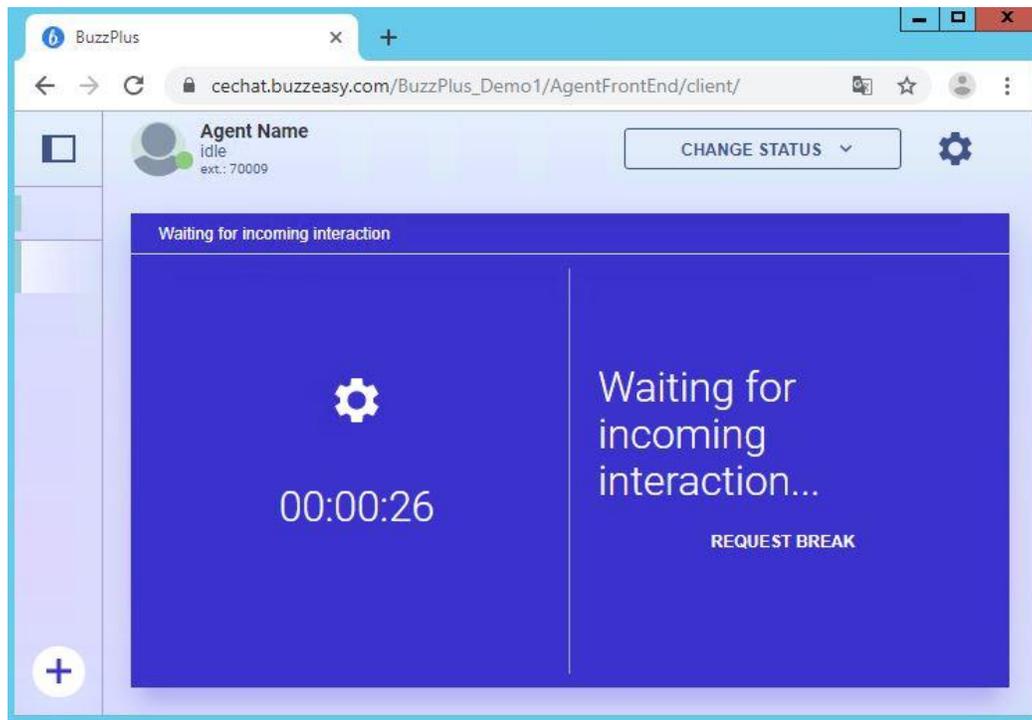
From the agent PC, launch an Internet browser window and enter Buzzeasy Cloud Services URL. Log in with the user credentials provided by the end customer (not shown). Once signed in, the Buzzeasy Cloud Service will be shown as below:



In the right settings pane, select **User Settings** (not shown). Enter the relevant Extension to receive voice calls and press **UPDATE**.



Verify that the left pane is updated showing relevant extension, as shown below. Press **Continue in auto Mode** to start handling the call.



Make an incoming call to this extension. Verify that the incoming call pane show with incoming number (not shown). Click on the answer icon to answer the call. Verify that the agent is connected to the PSTN caller with two-way talk paths

9. Conclusion

These Application Notes describe the compliance tested configuration of the Geomant Buzzeasy Cloud Services with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. All tests passed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Geomant 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 Buzzeasy can be requested from <http://kb.buzzeasy.com/>

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.