



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

---

# **Application Notes for Sestek Voice Biometrics with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1 using CCT Open Interfaces and DMCC Multiple Registration – Issue 1.1**

## **Abstract**

These Application Notes describe the configuration steps required for Sestek Voice Biometrics with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1. Sestek Voice Biometrics is an advanced voice biometrics solution that verifies customer identity quickly and intuitively by voice. Sestek Voice Biometrics integrates with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services by streaming voice from Avaya telephony using Multiple Registration method.

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 Sestek Voice Biometrics to interoperate with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1 using CCT Open Interfaces and Multiple Device Registration method.

Sestek Voice Biometrics is an advanced voice biometrics solution that verifies customer identity quickly and intuitively by voice. In this compliance test, it uses Avaya Aura® Communication Manager's Multiple Device Registration feature via Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio for call streaming, and capture call details from Avaya Aura® Contact Center using CCT Open Interfaces. The application uses the Avaya Aura® Application Enablement Services DMCC service to register the extensions that are to be streamed. When the extension receives an event pertaining to the start of a call, the application receives the extensions RTP media stream.

## 2. General Test Approach and Test Results

The feature test cases were performed manually in a variety of scenarios using DMCC Multiple Registration.

For the manual part of the testing, each call was handled manually on the extension telephone with generation of unique audio content for the streaming. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Sestek Voice Biometrics.

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 Sestek Voice Biometrics utilized enabled capabilities of secure DMCC interface and Open CCT interface.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and streaming calls in different call scenarios with checking good voice biometrics. The tests included:

- **Inbound/Outbound calls** – Test call streaming for inbound and outbound calls to the Avaya Aura® Contact Center to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call streaming for calls transferred to and in conference with PSTN callers.
- **Feature calls** - Test call streaming for calls that are parked or picked up using Call Park, Call Pickup, Bridged Appearance and Service Observing.
- **Serviceability testing** - The behaviours of Sestek Voice Biometrics under different simulated failure conditions.

## 2.2. Test Results

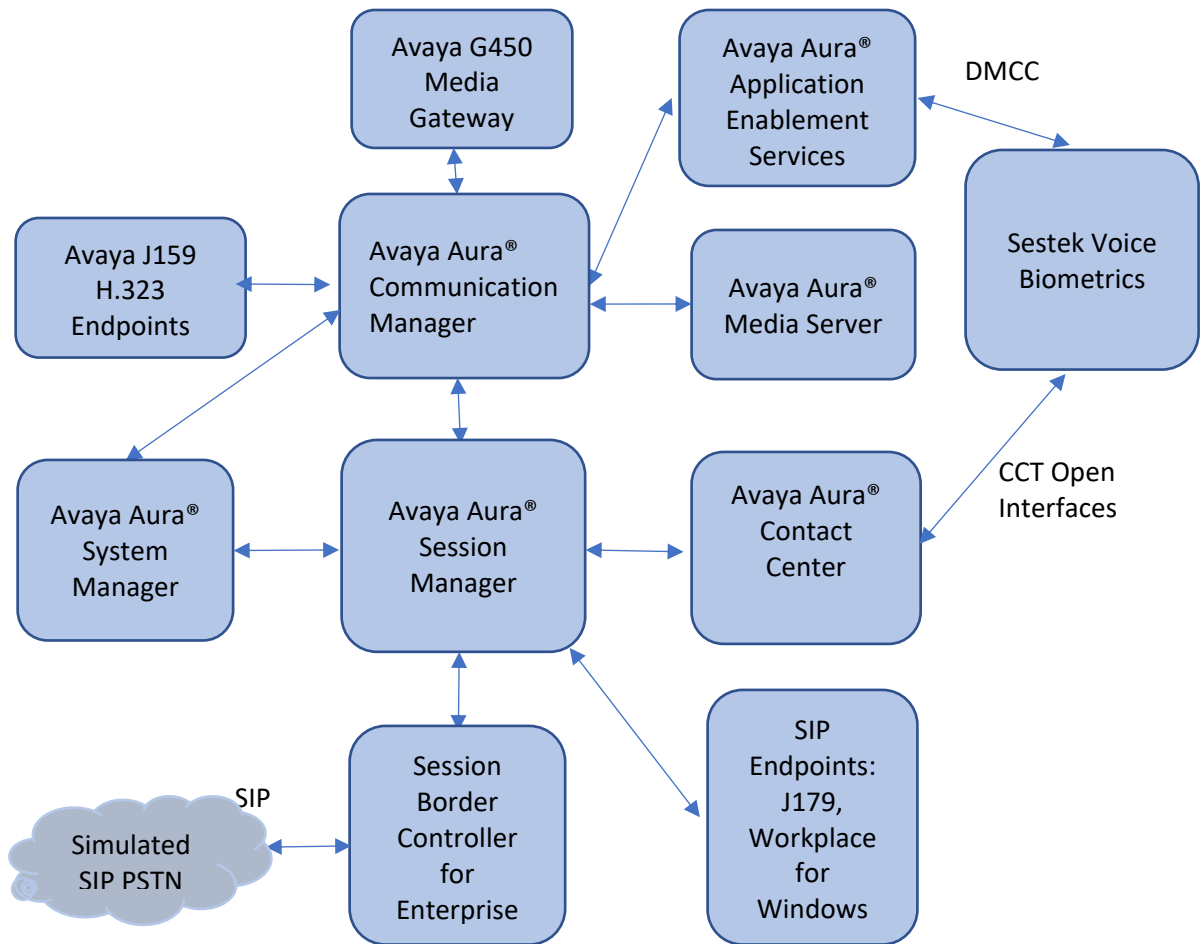
All test cases were executed and verified successfully.

## 2.3. Support

Technical support on Sestek Voice Biometrics can be obtained through the following:

- Support: <https://support.sestek.com/>
- Phone: +90 212 286 25 45
- Web: <https://www.sestek.com/>

### 3. Reference Configuration



**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                     | 10.1.0.0.537353                     |
| Avaya Aura® Session Manager in Virtual Environment                    | 10.1.0.1.1010105                    |
| Avaya Aura® Communication Manager in Virtual Environment              | 10.1.0.1 SP1 Build 01.0.974.0-27372 |
| Avaya G450 Media Gateway  | 41.34.1                             |
| Avaya Aura® Media Server in Virtual Environment                       | 10.1.0.77                           |
| Avaya Aura® Application Enablement Services in Virtual Environment    | 10.1.0.1.0.7                        |
| Avaya Session Border Controller for Enterprise in Virtual Environment | 10.1                                |
| Avaya Aura® Contact Center  | 7.1.2                               |
| Avaya Workplace Client for Windows                                    | 3.25.0.73                           |
| Avaya J179 IP Phone (SIP)   | 4.0.12.1                            |
| Avaya J159 IP Deskphone (H.323)                                       | 6.8.5                               |
| Sestek Voice Biometrics   | 11.0.7                              |

## 5. Configure Avaya Aura® Communication Manager

The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, and Contact Center are not the focus of these Application Notes and will not be described. This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Administer CTI link
- Configure H.323 Stations for Multi-Registration
- Configure SIP Stations for Multiple Registration

A 2-party call is expected to consume 3 DSP resources when an Avaya Media Gateway is used or 3 Media Processing Units (MPU) when an Avaya Media Server is used. For example, a 2-party call using a G711 codec will consume 1 resource per active call participant, and 1 resource for the DMCC custom media streaming of the customer channel.

### 5.1. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

|                  |             |
|------------------|-------------|
| add cti-link 1   | Page 1 of 3 |
| CTI LINK         |             |
| CTI Link: 1      |             |
| Extension: 79999 |             |
| Type: ADJ-IP     |             |
|                  | COR: 1      |
| Name: aes95      |             |

## 5.2. Configure H.323 Stations for Multi-Registration

All endpoints that are to be monitored by Sestek will need to have IP Softphone set to **y**. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where **x** is the extension number of the station to be monitored. Also note this extension number for configuration required during the Sestek setup in **Section 7**. Note the Security Code and ensure that **IP SoftPhone** is set to **y**.

|                           |  |             |
|---------------------------|--|-------------|
| change station 70010      |  | Page 1 of 5 |
| STATION                   |  |             |
| <b>Extension:</b> 70010   | Lock Messages? n                             | BCC: 0      |
| <b>Type:</b> 9641         | <b>Security Code:</b> 111222                 | TN: 1       |
| Port: S000004             | Coverage Path 1:                             | COR: 1      |
| <b>Name:</b> H323 Ext1    | Coverage Path 2:                             | COS: 1      |
|                           | Hunt-to Station:                             | Tests: y    |
| STATION OPTIONS           |  |             |
| Loss Group: 19            | Time of Day Lock Table:                      |             |
|                           | Personalized Ringing Pattern: 1              |             |
| Speakerphone: 2-way       | Message Lamp Ext: 70010                      |             |
| Display Language: english | Mute Button Enabled? y                       |             |
| Survivable GK Node Name:  | Button Modules: 0                            |             |
| Survivable COR: internal  | Media Complex Ext:                           |             |
| Survivable Trunk Dest? y  | <b>IP SoftPhone? y</b>                       |             |
|                           | IP Video Softphone? n                        |             |
|                           | Short/Prefixed Registration Allowed: default |             |
|                           | Customizable Labels? Y                       |             |

For compliance testing, two H323 extensions were administered : **70010** and **70011**.

### 5.3. Configure SIP Stations for Multiple Registration

Each Avaya SIP endpoint or station that needs to be monitored for call streaming will need to have **Type of 3PCC Enabled** is set to **Avaya** and **IP Softphone** set to **Yes**. Changes to SIP phones on Communication Manager by enter command **change station x** where **x** is the extension number of the station.

|                           |  |             |
|---------------------------|--|-------------|
| change station 70000      |  | Page 1 of 6 |
| STATION                   |  |             |
| <b>Extension:</b> 70000   | Lock Messages? n                             | BCC: 0      |
| <b>Type:</b> J179         | <b>Security Code:</b> 111222                 | TN: 1       |
| Port: S000010             | Coverage Path 1:                             | COR: 1      |
| <b>Name:</b> SIP Ext1     | Coverage Path 2:                             | COS: 1      |
|                           | Hunt-to Station:                             | Tests: y    |
| STATION OPTIONS           |  |             |
| Loss Group: 19            | Time of Day Lock Table:                      |             |
|                           | Personalized Ringing Pattern: 1              |             |
| Speakerphone: 2-way       | Message Lamp Ext: 70000                      |             |
| Display Language: english | Mute Button Enabled? y                       |             |
| Survivable GK Node Name:  | Button Modules: 0                            |             |
| Survivable COR: internal  | Media Complex Ext:                           |             |
| Survivable Trunk Dest? v  | <b>IP SoftPhone? y</b>                       |             |
|                           | IP Video Softphone? n                        |             |
|                           | Short/Prefixed Registration Allowed: default |             |
|                           | Customizable Labels? Y                       |             |

Go to **Page 6**. Ensure that **Type of 3PCC Enabled** is set to **Avaya**.

|   |      |                 |   |
|---|------|-----------------|---|
| change station 70000                              | Page | 6 of            | 6 |
| STATION   |      |                 |   |
| SIP FEATURE OPTIONS                               |      |                 |   |
| Type of 3PCC Enabled: <b>Avaya</b>                |      | SIP Trunk: aar  |   |
| Enable Reachability for Station Domain Control: s |      |                 |   |
| SIP URI: 70000@aura.com                           |      |                 |   |
| Primary Session Manager                           |      |                 |   |
| IPv4 Address: 10.128.224.18                       |      | IPv6 Address:   |   |
| IPv4 Node Name: smsip18                           |      | IPv6 Node Name: |   |
| Secondary Session Manager                         |      |                 |   |
| IPv4 Address:                                     |      | IPv6 Address:   |   |
| IPv4 Node Name:                                   |      | IPv6 Node Name: |   |
| Third Session Manager                             |      |                 |   |
| IPv4 Address:                                     |      | IPv6 Address:   |   |
| IPv4 Node Name:                                   |      | IPv6 Node Name: |   |
| Fourth Session Manager                            |      |                 |   |
| IPv4 Address:                                     |      | IPv6 Address:   |   |
| IPv4 Node Name:                                   |      | IPv6 Node Name: |   |

For compliance testing, two SIP extensions were administered : **70000** and **70001**.



## 6. Configure Avaya Aura® Application Enablement Services

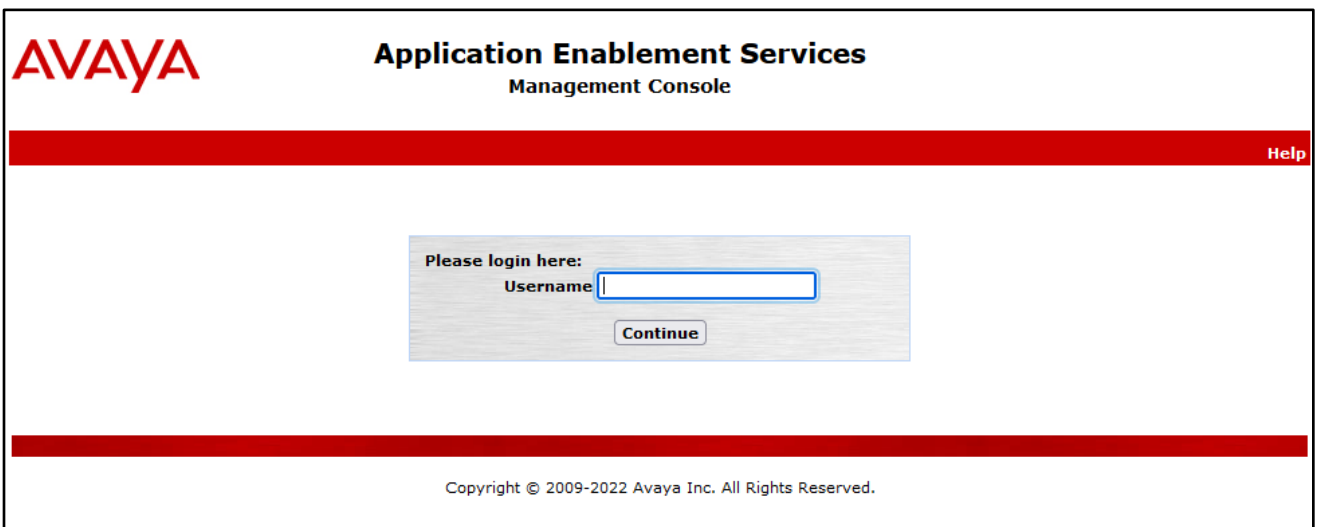
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer sestek user
- Enable CTI User
- Administer security database
- Restart services

### 6.1. Launch OAM Interface


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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page, with a "Help" link in the top right corner. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another thick red horizontal bar is present, with the copyright notice "Copyright © 2009-2022 Avaya Inc. All Rights Reserved." centered below it.

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



# Application Enablement Services Management Console

Welcome: User cust  
Last login: Mon Jun 27 16:37:37 2022 from 172.16.8.16  
Number of prior failed login attempts: 0  
HostName/IP: aes95/10.30.5.95  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Jul 05 06:22:34 EDT 2022  
HA Status: Not Configured

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

## Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2022 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: Tue Jul 5 17:22:35 2022 from 172.16.8.167  
Number of prior failed login attempts: 0  
HostName/IP: aes95/10.30.5.95  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Jul 05 07:20:30 EDT 2022  
HA Status: Not Configured

LicensingHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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

Copyright © 2009-2022 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 **Device Media and Call Control**, as shown below.

**AVAYA**  
Aura® System Manager 10.1

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
- AVAYA AURAWEBGATEWAY
- ▶ AVAYA AURAWEBGATEWAY
- AVP
- ▶ AVP
- CALL\_CENTER\_ELITE\_MULTICHANNEL
- ▶ Call\_Center\_Elite\_Multichannel
- Configure Centralized Licensing
- CCTR
- ▶ ContactCenter
- CE
- ▶ COLLABORATION\_ENVIRONMENT
- COMMUNICATION\_MANAGER
- ▶ Call\_Center
- ▶ Communication\_Manager
- Configure Centralized Licensing
- ▶ Dialog\_Designer
- IPO
- ▶ IP\_Office
- MESSAGING

**Application Enablement (CTI) - Release: 10 - SID: 10503000** Standard Li

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

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

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

**Licensed Features**

13 Items Show All ▾

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

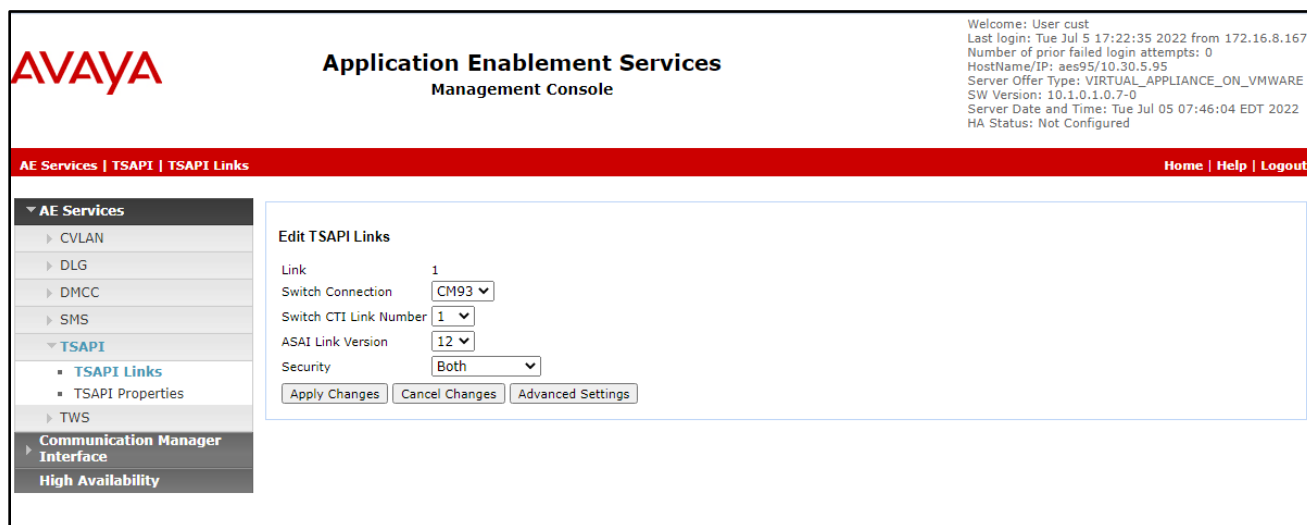
SmallServerTypes:  
s8300c;s8300d;icc;premio;tn8400;laptop;CtiS  
MediumServerTypes:  
ibm;206;ibm;206;mid;1050;vse;h370;h370

### 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 **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.1**. Retain the default values in the remaining fields.



## 6.4. Administer Sestek 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.

**User Management | User Admin | List All Users**

**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**

**Edit User**

\* User Id: sestek

\* Common Name: sestek

\* Surname: sestek

User Password: .....

Confirm Password:

Admin Note:

Avaya Role: None

Business Category:

Car License:

CM Home:

Cms Home:

CT User: Yes

Department Number:

Display Name:

Employee Number:

Employee Type:

Enterprise Handle:

Given Name:

Home Phone:

## 6.5. Enable CTI User

Navigate to the CTI Users screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. In the CTI Users window, select the user that was set up in **Section 6.4** and select the **Edit** option.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. The left sidebar contains a tree view with categories like AE Services, Communication Manager, High Availability, Licensing, Maintenance, Networking, and Security. The "Security" category is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and CTI Users. The "CTI Users" item is selected, and the "List All Users" link is active. The main content area displays a table titled "CTI Users" with columns: User ID, Common Name, Worktop Name, and Device ID. The table lists three users: redbox, sestek, and tma. The "sestek" user is selected with a radio button. Below the table are "Edit" and "List All" buttons.

| User ID                                 | Common Name | Worktop Name | Device ID |
|---|-------------|--------------|-----------|
| <input type="radio"/> redbox            | redbox      | NONE         | NONE      |
| <input checked="" type="radio"/> sestek | sestek      | NONE         | NONE      |
| <input type="radio"/> tma               | tma         | NONE         | NONE      |

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot shows the "Edit CTI User" screen in the Avaya Application Enablement Services Management Console. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled "Edit CTI User" and displays the configuration for the selected user "sestek". The "User Profile" section shows the User ID, Common Name, Worktop Name, and a checked "Unrestricted Access" checkbox. The "Call and Device Control" section shows "Call Origination/Termination and Device Status" set to "None". The "Call and Device Monitoring" section shows "Device Monitoring" set to "None", "Calls On A Device Monitoring" set to "None", and "Call Monitoring" set to "None". The "Routing Control" section shows "Allow Routing on Listed Devices" set to "None". At the bottom are "Apply Changes" and "Cancel Changes" buttons.

| Edit CTI User                                  |                                     |  |
|--|-------------------------------------|--|
| <b>User Profile:</b>                           |                                     |  |
| User ID  | sestek                              |  |
| Common Name                                    | sestek                              |  |
| Worktop Name                                   | NONE                                |  |
| Unrestricted Access                            | <input checked="" type="checkbox"/> |  |
| <b>Call and Device Control:</b>                |                                     |  |
| Call Origination/Termination and Device Status | None                                |  |
| <b>Call and Device Monitoring:</b>             |                                     |  |
| Device Monitoring                              | None                                |  |
| Calls On A Device Monitoring                   | None                                |  |
| Call Monitoring                                | <input type="checkbox"/>            |  |
| <b>Routing Control:</b>                        |                                     |  |
| Allow Routing on Listed Devices                | None                                |  |

## 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 sestek 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 the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various service categories, 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", along with an "Apply Changes" button.



## 6.7. Restart Services

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

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167  
Number of prior failed login attempts: 0  
HostName/IP: aes155.aura.com/10.128.226.155  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Tue Sep 20 15:27:30 ICT 2022  
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ 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 checked="" 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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

## 7. Configure Avaya Aura® Contact Center

It is implied that a working Avaya Aura® Environment, which includes System Manager, Session Manager, Communication Manager, Media Server, and Contact Center, is already in place with the necessary licensing. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 11**.

This section shows the steps required to add a new CCT Agent on Avaya Aura® Contact Center. The following sections give step by step instructions on how to add the following.

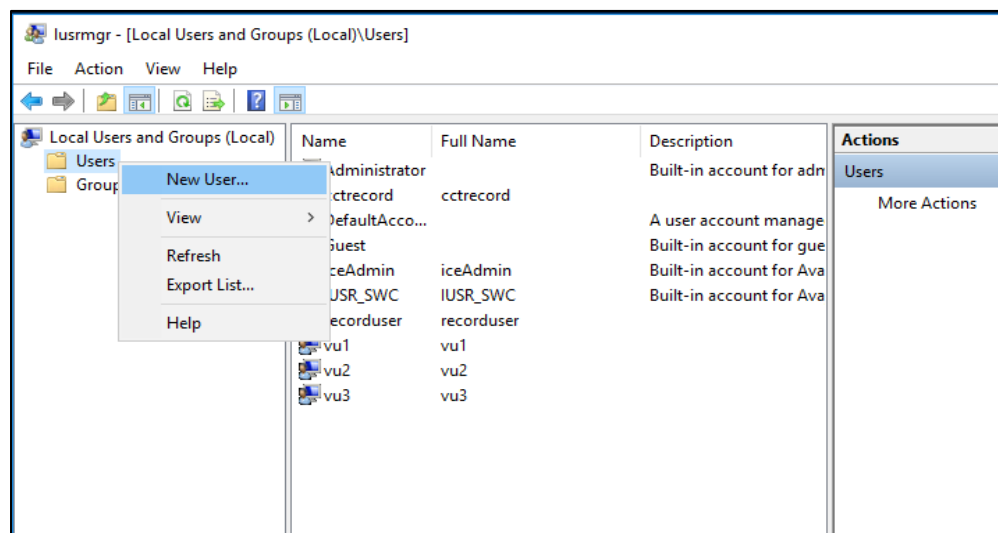
- Create a Windows user on the Avaya Aura® Contact Center Server
- Login to Avaya Aura® Contact Center Manager
- Configure a Contact Center CCT Agent
- Verify CCT User Association
- Verify CCT Web Services

### 7.1. Create a Windows user on the Avaya Aura® Contact Center Server

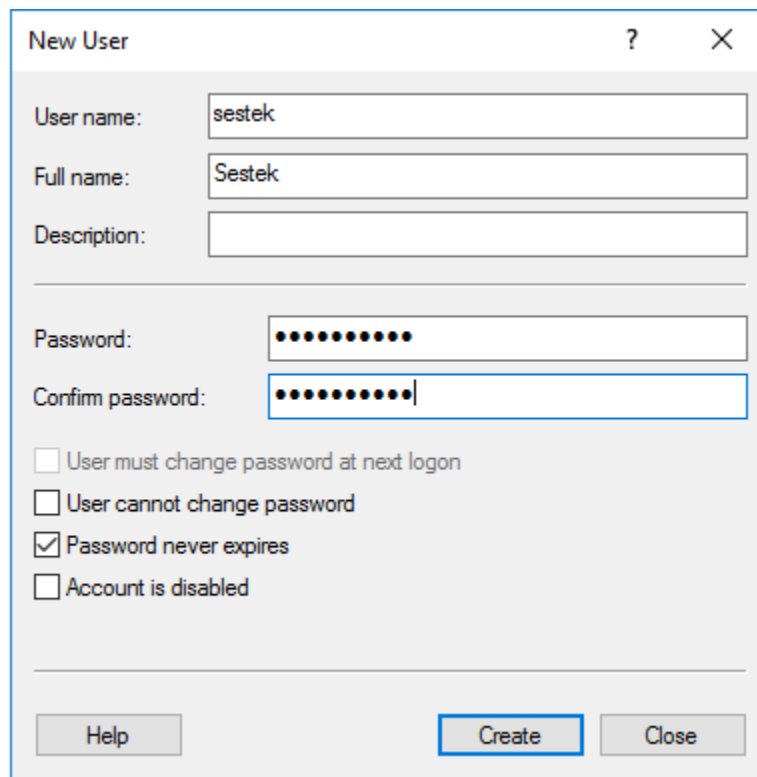
All CCT users must be associated with a user account on Windows Active Directory/Domain User account. When a Contact Center user is created there is an option to create a CCT user and there is an association made there with a Windows domain user, see **Section 7.3**. Users who can access multiple domains can also access the CCT client as long as trust is established between the domains; the user does not have to log on to separate domains to use the CCT client.

If there is no Active Directory already in place, then a windows user must be added to the Contact Center server before a CCT user is added. In the example below a new user called **sestek** was created on the local Windows server. To add a new windows user, navigate to Computer Management. On Windows 2016 server simply type in Computer Management on the screen and the program will appear.

From Computer Management, in the left window, expand **System Tools → Local Users and Groups → Users** and right click on **Users** and select **New User** as shown below.



Enter the **User name** and **Password** noting that this same username and password will be required in configuring the Contact Center CCT Agent. Ensure that **Password never expires** is ticked. Click on **Create** once the information is filled in correctly.



**New User**

User name:

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

## 7.2. Login to Avaya Aura® Contact Center Manager

Launch URL: **http://<IP Address of AACC>** and login to the Contact Center Management Administration with administrative credentials. The Contact Center Launch pad is displayed.



## 7.3. Configure a Contact Center CCT Agent

In the Launch pad, click **Contact Center Management** (not shown). In the left pane, click the Contact Center Manager to which the agent is to be added. On the top menu, select **Add → Agent**. The following highlighted fields were configured:

- **User Type:** Select Agent as User Type.
- **Login ID:** The number the agent enters to logon to the phone. In this case the field is set to the extension (75000).
- **Primary Supervisor:** Select Default Supervisor from the list.
- **Voice URI:** The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent (use Extension@SIPdomain, where SIPdomain is the CCMS Local SIP Subscriber Domain name. For example, [sip:75000@aura.com](mailto:sip:75000@aura.com)).
- **Create CCT Agent:** Tick on this check box to associate the agent with CCT. As the **Create CCT Agent** is selected, the **Associate User Account** section will be displayed. Expand this section, select **Search local operating system**, and click on **List All** button, it will list all local operating system users including the Windows user **Sestek** created in the section above. Select the **Sestek**, the **Sestek** is now displayed in the **CCT Agent Login Details**.

Click **Contact Types** (not shown), which is then expanded. Select the check box beside each **Contact Type** to assign to the agent (for example, **Voice**).

The screenshot displays the CCT Agent configuration interface. The **User Details** section includes fields for First Name (Sestek), Last Name (Sestek), Title, Department, Language (English), and Comment. The **Associate User Account** section has three radio buttons: **Search local operating system** (selected), **Search local security server**, and **Search domain users**. Below these is a search filter with a dropdown for 'Full Name', a 'starts with' input, and an 'includes' dropdown set to 'all users'. A **List All** button is present. A table lists user accounts with columns for User Name, Full Name, and Status. The **Sestek** user is selected. The **CCT Agent Login Details** section shows the Domain as AACC199 and the User ID as Sestek.

| User Name                               | Full Name (11) | Status    |
|---|----------------|-----------|
| <input type="radio"/> DefaultAccount    |                | Available |
| <input type="radio"/> Guest             |                | Available |
| <input type="radio"/> iceAdmin          | iceAdmin       | Available |
| <input type="radio"/> IUSR_SWC          | IUSR_SWC       | Available |
| <input type="radio"/> recorduser        | recorduser     | Available |
| <input checked="" type="radio"/> Sestek | Sestek         | Available |
| <input type="radio"/> vu1               | vu1            | Available |

Click the **Skillsets** heading to expand the branch. Click **List All** to list all skillsets configured on the server. From the **Priority** list for each skillset to assign to the agent, select the priority levels (For example select **Voice** and set the priority level 48).


▼ [Skillsets](#)

| Skillset Name (1) | Contact Type | Priority |
|-------------------|--------------|----------|
| Default_Skillset  | Voice        | 48 ▼     |

► [Assign Skillsets](#)






## 7.4. Verify CCT User Association






To check to see that the CCT User and Contact Center Agent are associated correctly, navigate to **Configuration** on the Launchpad as shown below.

 **Contact Center - Manager** [About](#) | [Audit Trail](#) | [Change Password](#) | [Logout](#)

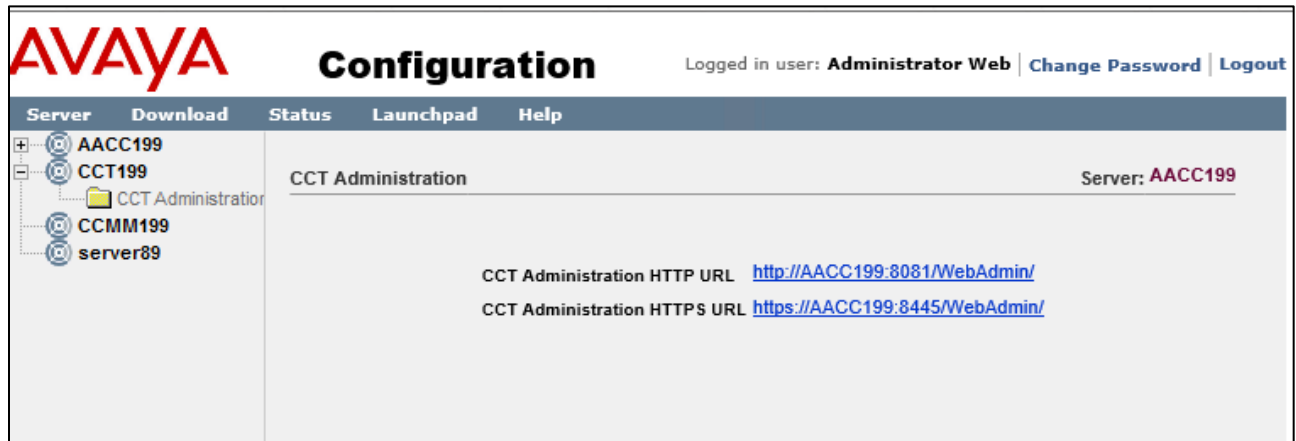
Launchpad

### Launchpad

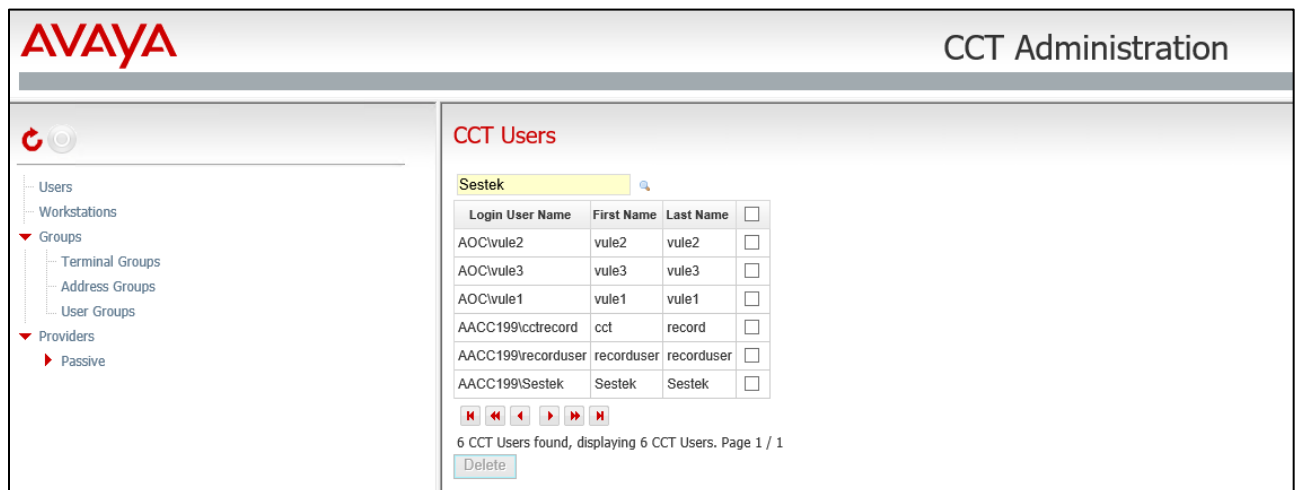
 **Contact Center Management**  
 **Access and Partition Management**  
 **Real-Time Reporting**  
 **Historical Reporting**  
 **Call Recording and Quality Monitoring**  
 **Prompt Management**

 **Configuration**  
 **Scripting**  
 **Emergency Help**  
 **Outbound**  
 **Multimedia**

Expand the CCT Server in the left window and click on **CCT Administration**. Click on **CCT Administration URL** in the main window.



The **CCT Administration** window opens in a separate browser session. Click on **Users** in the left window and double-click on the user added from **Section 7.3**.



The agent **75000** is associated with this user. There are no changes required in this section only to observe that the association is correct.

## Update CCT User

User Details

Login User Name

AACC199\Sestek

First Name

Sestek

Last Name

Sestek

Address Assignments

Terminal Assignments

Terminal Group Assignments

Address Group Assignments

Agent Assignments

Agents available

| <input type="checkbox"/> | Agents |
|--------------------------|--------|
| <input type="checkbox"/> | 20005  |
| <input type="checkbox"/> | 20004  |
| <input type="checkbox"/> | 20001  |
| <input type="checkbox"/> | 50004  |

4 Agents found. Page 1 / 1

Agents mapped

| <input type="checkbox"/> | Agents |
|--------------------------|--------|
| <input type="checkbox"/> | 75000  |

1 Agents found. Page 1 / 1

Save

## 8. Configure Sestek Voice Biometrics

This section addresses the administrative steps to be performed on the Sestek Voice Biometrics solution. The installation of the Sestek Voice Biometrics solution software, as well as the initial configuration is beyond the scope of this document. The procedures include the following areas:

- Configure Sestek Falcon Services
- Configure Sestek Voice Biometrics Services

### 8.1. Configure Sestek Falcon Services

To configure Falcon services, use Falcon Configurator tool installed in Sestek Biometrics server. Default path: C:\Program Files\Sestek\Falcon\CallRecorder\Configurator.

#### 8.1.1. Configuring host's file

Open "C:\Windows\System32\drivers\etc\hosts" file with text editor. Add the IP address of the Contact Center as shown in the example below as **aacchost**.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1            localhost
192.168.10.178    aacchost
```



### 8.1.2. Creating Cti Source for DMCC

Open **Sestek Falcon Configuration Tool**, click **Cti Sources** and click add (+) button and configure settings as described below.

- **Type:** AvayaDMCC
- **Name:** Give it proper name
- **Host1:** AES hostname or IP address
- **Port1:** DMCC server port that was enabled in **Section 6.7**
- **Username/password:** Username and password created in **Section 6.3**
- **SwitchName:** Switch name configured in **Section 6.2**
- **Protocol version:** DMCC xml protocol version. For this version should be “C”

The screenshot shows the Sestek Falcon Configurator interface. On the left is a sidebar with various menu items. The main area is titled 'Cti Sources' and contains a table with columns: Type, Name, Host 1, Port 1, Host 2, Port 2, Username, and Password. An 'Update CtiSourceDto' dialog box is open, displaying the following configuration: Type: AvayaDmcc, Name: AvayaDmcc, Host 1: avayaaes, Port 1: 0, Username: sestekcti, Password: (masked), SwitchName: AVAYAACM, and ProtocolVersion: C. 'Update' and 'Cancel' buttons are at the bottom of the dialog.

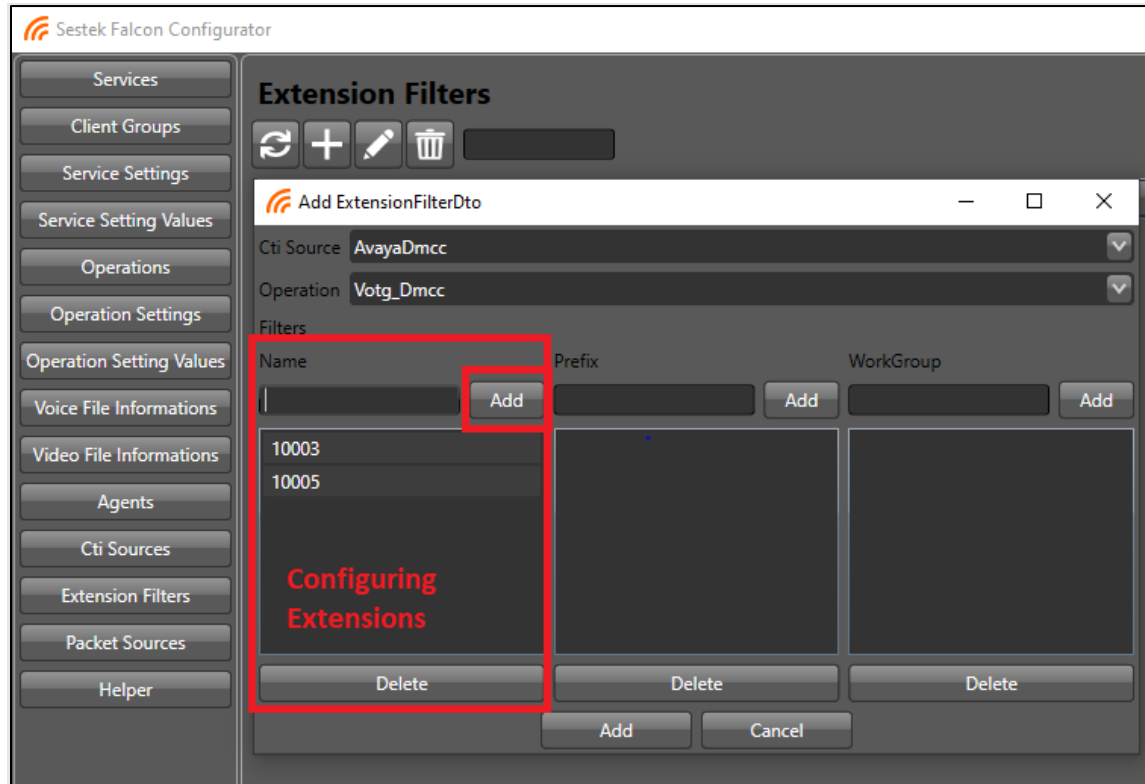
### 8.1.3. Creating Operation

To create new operation, click **Operations** button in the left panel and press add button and **Name** it in the opening form. Click **Add** to save changes.

The screenshot shows the Sestek Falcon Configurator interface. In the left sidebar, the 'Operations' button is highlighted with a red rectangle. In the main area, the 'Operations' section is active, showing a table with columns: Id, Name, and Settings. The '+' (add) button is also highlighted with a red rectangle. An 'Add OperationDto' dialog box is open, with the 'Name' field containing 'Votg\_Dmcc' and highlighted by a red rectangle. 'Add' and 'Cancel' buttons are at the bottom of the dialog.

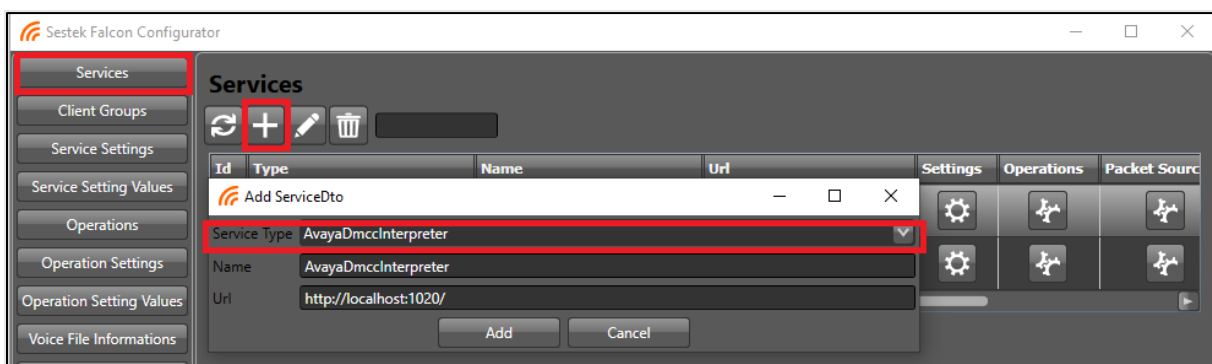
#### 8.1.4. Creating ExtensionFilter

To create an extension filter, Click the **ExtensionFilter** button in the left panel, click the **Add** button (+), select the cti source created in **Section 8.2**, and select operation created in **Section 8.3**. And configure extension numbers using the screenshot below.

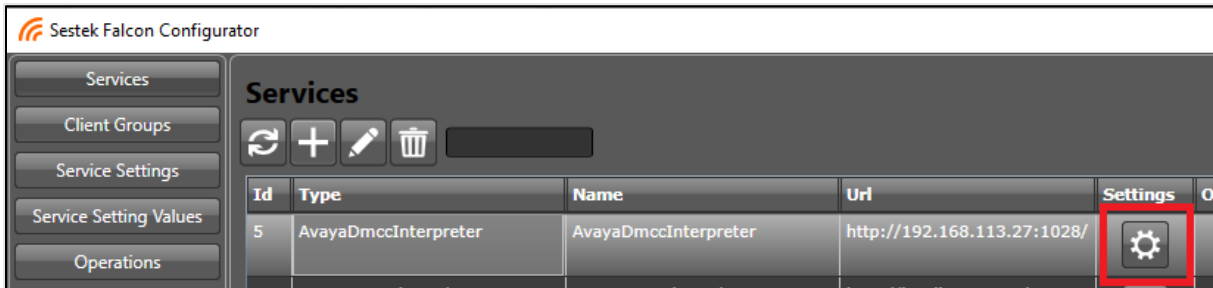


#### 8.1.5. Configuring DMCC Interpreter

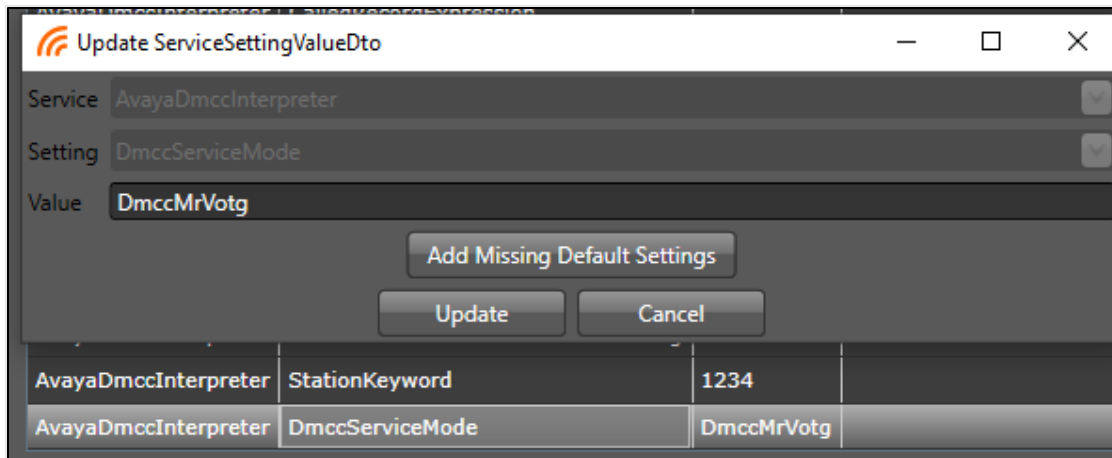
- Open **Sestek Falcon Configurator** Tool to configure Falcon services.
- Navigate to **Services** and click the **Add** button and select service type as **AvayaDMCCInterpreter**, give the service a proper name and update localhost with the server IP address in the URL section. Click **Add** button to save.



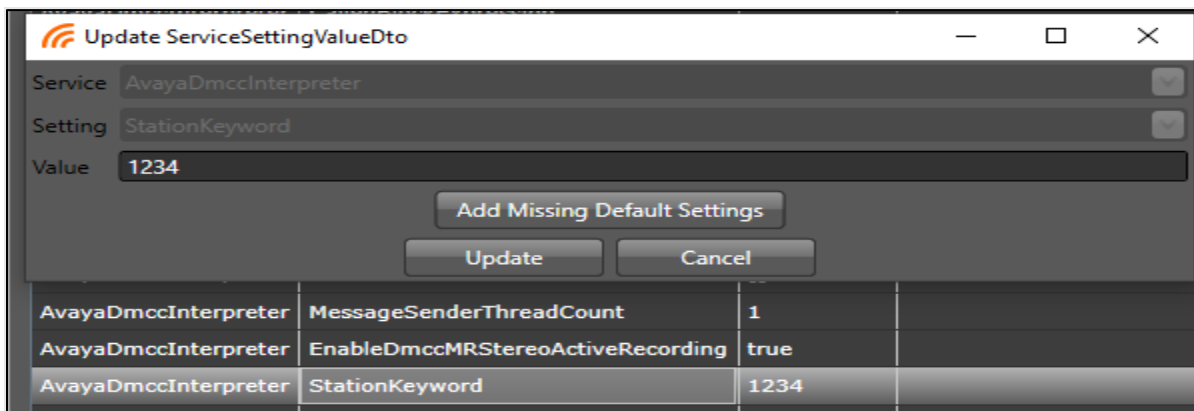
- After adding a service, **AvayaDMCCInterpreter** service will appear in the services section. Click **Settings** button to configure service setting parameters.



- Select **DMCCServiceMode** setting and update it to **DMCCMrVotg** in the opening form.



- Select the **StationKeyword** setting and update it to extension security code created in **Section 5.6**.



- Select **ShouldBeHandleAvayaCctCallEvents** setting and update it to **true**.

|                      |                                  |       |
|----------------------|----------------------------------|-------|
| AvayaDmccInterpreter | ShouldBeHandleAvayaCctCallEvents | false |
|----------------------|----------------------------------|-------|

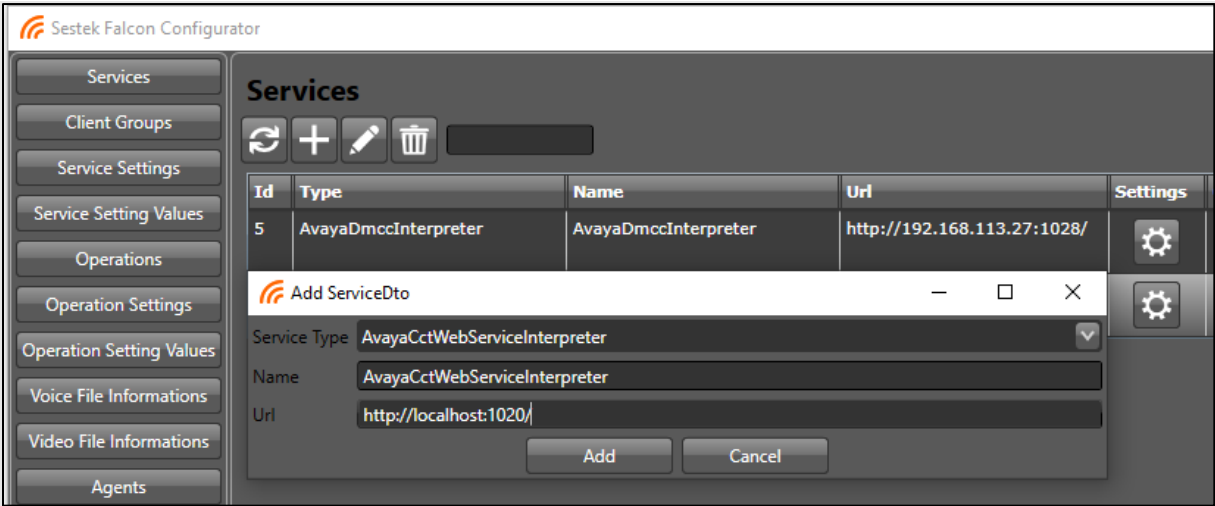
- To connect service to operation, go to **Services** and select **DMCCInterpreter** and the button under the **Operations** column.

| Id | Type                          | Name                          | Url                         | Settings | Operations | Packet Sources | Services | Update Settings |
|----|-------------------------------|-------------------------------|-----------------------------|----------|------------|----------------|----------|-----------------|
| 5  | AvayaDmccInterpreter          | AvayaDmccInterpreter          | http://192.168.113.27:1028/ |          |            |                |          |                 |
| 6  | AvayaCctWebServiceInterpreter | AvayaCctWebServiceInterpreter | http://localhost:1028/      |          |            |                |          |                 |

- In the opening form, select operation created in **Section 8.3** and click the right arrow (->) to connect service to operation. Press to **Save** button to save changes.

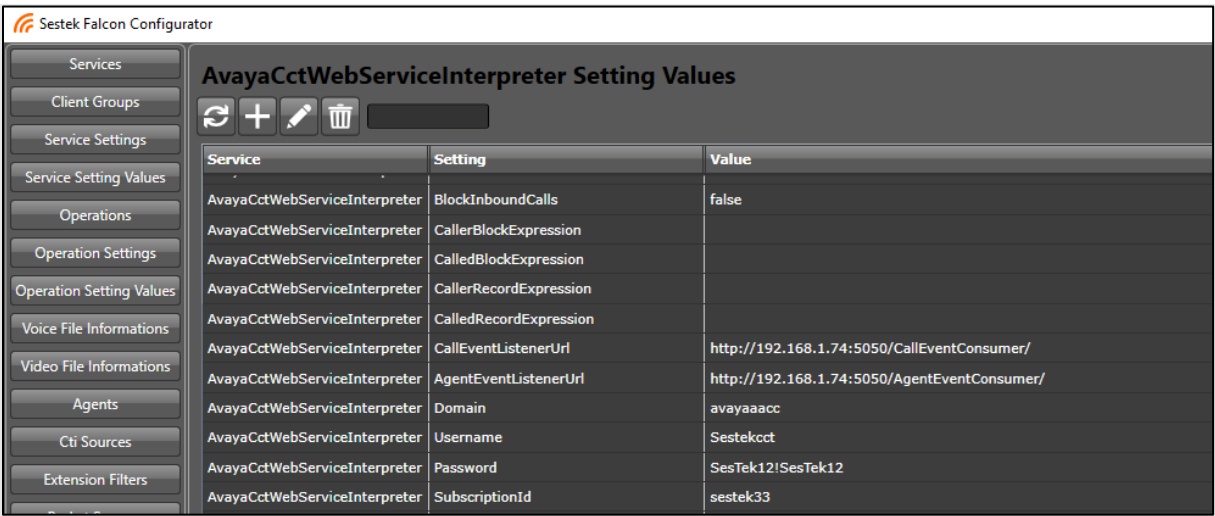
### 8.1.6. Create and Configure CctWebServiceInterpreter

Navigate to **Services** and click the **Add** button and select **Service Type** as **AvayaCctWebServiceInterpreter**, name the service and update localhost with the server IP address in the URL section. To save, click **Add** button.

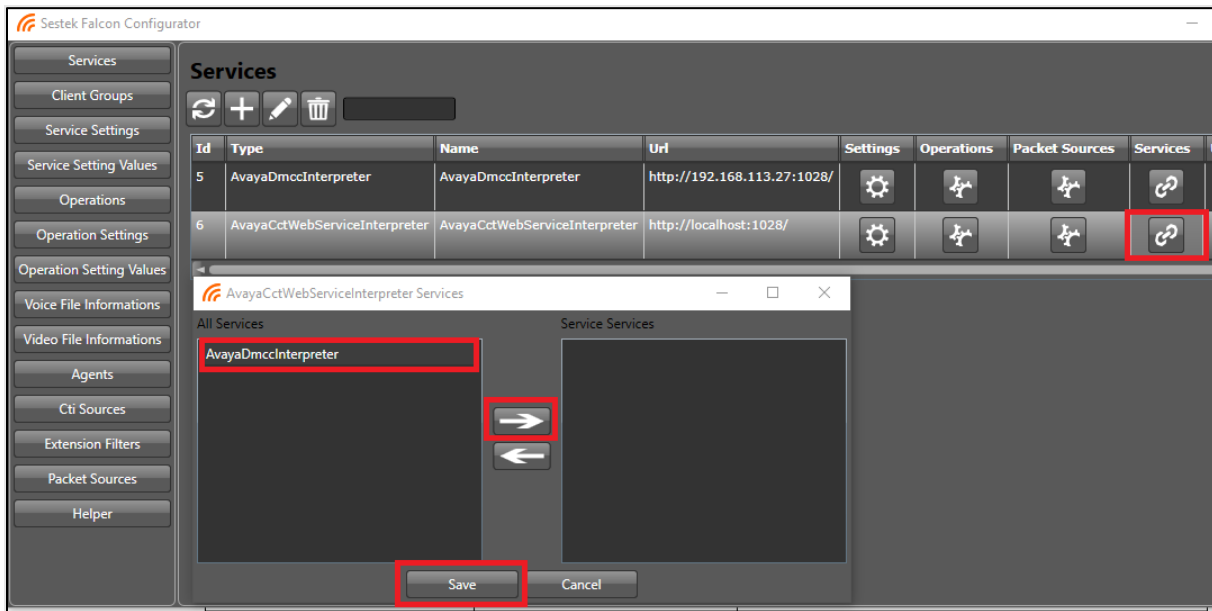


After creating service, select created service and press button under the settings column and update service settings as described below.

- **CallEventListenerUrl**: Change IP address to server IP installed Sestek services.
- **AgentEventListenerUrl**: Change IP address to server IP installed Sestek services.
- **Domain**: CCT user domain created in **Section 7.3**.
- **Username**: CCT username created in **Section 7.3**.
- **Password**: CCT username’s password created in **Section 7.3**.



- To connect **CCTInterpreter** to **DMCCInterpreter** select **CctWebInterpreterService** and click the chain button under the services column.
- Select **AvayaDMCCInterpreter** and press the right arrow (->) to connect service. Press the Save button to save changes.



### 8.1.7. Firewall Configuration

Firewall configuration is outside the scope of these application notes, but it is mentioned here for awareness. If there is a Firewall between the Avaya and Sestek servers, firewall rules need to be in place to allow traffic between them. A user needs to verify the IP Addresses, ports, and protocols used, and configure firewall rules to allow the traffic flow.

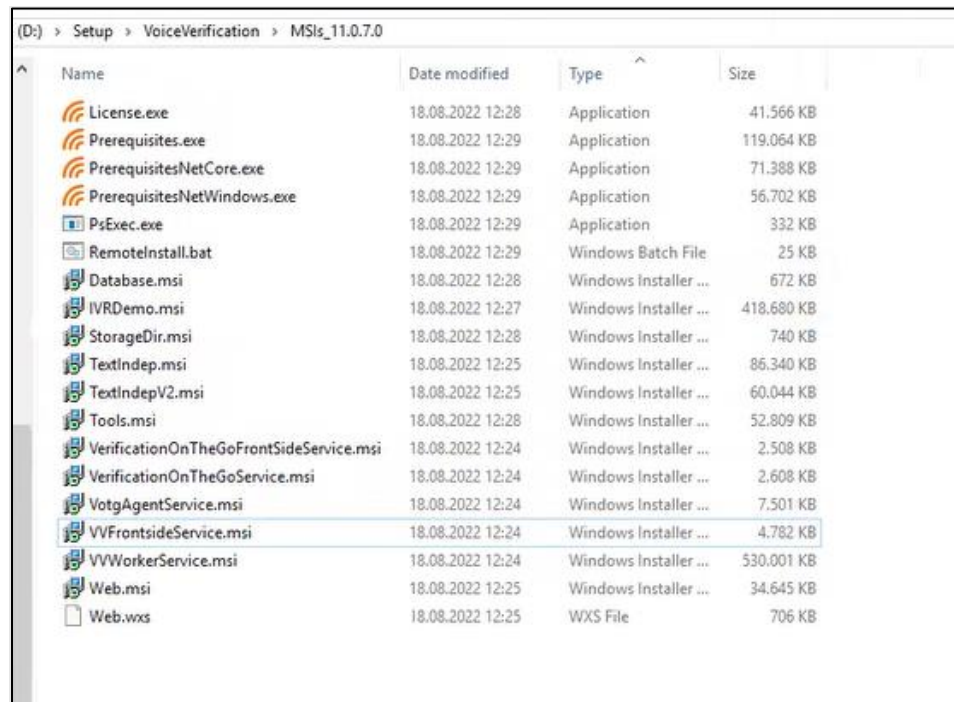
## 8.2. Configure Sestek Voice Biometrics Services

To configure Voice Biometrics Services services, navigate to Voice Biometrics Services installation folder. Default path: **C:\Program Files\Sestek\VoiceVerification\**.

### 8.2.1. Configure RemoteInstall.bat

Remote install bat is a script to automate and configure MSI packet installations.

- Open MSI zip and edit **RemoteInstall.bat** parameters.



- Customize MSI source and installation directories. Also add the admin username and password. These are set under the **Server Credentials** as **set user** and **set password**.

```
4 set programfiles_VV=C:\Program Files\Sestek\VoiceVerification
5 set programdata_VV=D:\ProgramData\Sestek\VoiceVerification
6
7 :: Set the folder containing MSI files.
8 set msifolder=D:\Setup\VoiceVerification\MSIs_11.0.7.0
9 cd %msifolder%
10
11 :: Set the connection string of DB.
12 set connectionString=Server=localhost;;Database=VoiceVerification;;User Id=VVUser;;Password=1q2w3e4r*;;
13
14 :: Set the "storageDirParent" folder where storageDir sits.
15 set storageDirParent=%programdata_VV%
16 set storageDir=%storageDirParent%\StorageDir
17
18 :: Set the "configDir" to a custom folder when desired. The default config folder is the "storageDir"
19 set configDir=
20
21 :: ----- Server Credentials -----
22 :: Set the credentials for remote access to installation servers.
23 set user=Administrator
24 set password=1q2w3e4r*
```



- Set the installation component flags to be installed.

```

27 :: ----- Installation Component Flags -----
28 :: Set to 1 or 0 for component selection. (1=install / 0=do not install)
29 set installFlag_Database=1
30 set installFlag_StorageDir=1
31 set installFlag_IvrDemo=0
32 set installFlag_TextIndep=0
33 set installFlag_TextIndepV2=1
34 set installFlag_Worker=1
35 set installFlag_FrontSide=1
36 set installFlag_Votg=1
37 set installFlag_VotgFrontSide=1
38 set installFlag_VotgAgent=0
39 set installFlag_Web=1
40 set installFlag_Tools=1

```

- Customize server IPs for each component.

```

10 :: ----- Server IPs -----
11 :: Set server IPs. On each provided server, an instance of the setup will be run (except CallRecorder server, which is kept only for updating VotG config respectively).
12 set stageServer_Database=192.168.10.68
13 set stageServer_StorageDir=192.168.10.68
14 set servers_VvWorker=192.168.10.68
15 set servers_VvFrontSide=192.168.10.68
16 set servers_VotgFrontSide=192.168.10.68
17 set servers_VotgAgent=192.168.10.68
18 set servers_Web=192.168.10.68
19 set servers_Tools=192.168.10.68
20 :: Votg and CallRecorder servers should match one-to-one in given order.
21 :: If N VotG servers are set, then N CallRecorder servers should be specified.
22 set servers_Votg=192.168.10.68
23 set servers_CallRecorder=192.168.10.68
24

```

- Global notification client must be specialized to work with PoC tool.

```

150 :: ----- StorageDir Configuration -----
151 :: In case of VotG notification need, uncomment and set following fields as in examples below. Multiple entries should be separated with ^| characters.
152 :: Global notification clients are in hostname:port format, whereas soap notification clients are in http://hostname:port/servicename format
153 :: set globalNotificationClients=10.0.0.0:9090^|10.0.0.1:9090
154 :: set filteredGlobalNotificationClients=10.0.0.0:9090^|10.0.0.1:9090
155 :: set votgAgentServers=http://10.0.0.0:8150^|http://10.0.0.1:8150
156 :: set soapNotificationClients=http://10.0.0.0:9090/BasicHttpBinding_VotGNotificationServiceWcf^|http://10.0.0.1:9090/BasicHttpBinding_VotGNotificationServiceWcf
157 :: set filteredSoapNotificationClients=http://10.0.0.0:9090/BasicHttpBinding_VotGNotificationServiceWcf^|http://10.0.0.1:9090/BasicHttpBinding_VotGNotificationServiceWcf
158 set globalNotificationClients=192.168.10.68:7767
159

```

- Configure the audio format to Mulaw.

```

62 :: ----- IvrDemo, TextIndep and TextIndepV2 Configuration -----
63 :: Available samplingRate options: 8000, 16000
64 set samplingRate=8000
65 :: Available audioFormat options: Lin16, Mulaw and Alaw
66 set audioFormat=Lin16
67 set blacklistEnabled=False

```

Log files and service ports can leave as default.



## 8.2.2. Voice Biometrics Service Configuration

These configuration files are in program files directory of Windows. Example path shared below:  
C:\Program Files\Sestek\VoiceVerification\<Service Name>

- **VerificationOnTheGo.exe.config** configuration: Falcon streamer URL must be replaced with DMCC URL. **VotgWebServiceUri** and **FalconStreamerCallMessageReceiveEndpoint**, and **FalconStreamerUrl** must have the same server IP.

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <appSettings>
4     <add key="StorageDir" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
5     <!-- Local Server Settings -->
6     <add key="LocalIp" value="192.168.10.68" />
7     <add key="LocalStreamingMessagePort" value="7099" />
8     <add key="UdpLocalNotificationPort" value="7096" />
9     <!-- Service Settings -->
10    <add key="VotgWebServiceUri" value="http://192.168.10.68:8080/VotgOperations" />
11    <add key="HttpApiVersion" value="v1" />
12    <add key="AudioReceivePortBegin" value="10000" />
13    <add key="AudioReceivePortEnd" value="15000" />
14    <add key="UseAgentId" value="false" />
15    <add key="FalconStreamerUrl" value="http://192.168.10.68:1050/" />
16    <add key="FalconStreamerCallMessageReceiveEndpoint" value="http://192.168.10.68:8080/VotgOperations/v1/call/message" />
17    <add key="serilog:minimum-level" value="Information" />
18    <add key="Serilog.File.Path" value="D:\ProgramData\Sestek\VoiceVerification\VerificationOnTheGo\VerificationOnTheGoLog.txt" />
19    <add key="Serilog.File.OutputTemplate" value="{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} [{Level:u3}] {Message:l1} {Properties:j}{NewLine}{Exception}" />
20    <add key="Serilog.File.SizeLimitBytes" value="10000000" />
21    <add key="Serilog.File.RetainedCountLimit" />
22  </appSettings>
23  <startup>
24    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
25  </startup>
26 </configuration>
```

- **VerificationOnTheGoFrontSide.exe.config**: Server address should be checked in **LocalIp** and **VerificationOnTheGoFrontSideEndpoint**.

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <appSettings>
4     <add key="StorageDir" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
5     <!-- Service Settings -->
6     <add key="VerificationOnTheGoFrontSideEndpoint" value="http://192.168.10.68:8090/VotgFrontSideOperations" />
7     <add key="HttpApiVersion" value="v1" />
8     <add key="LocalIp" value="192.168.10.68" />
9     <add key="UdpLocalRegistrationPort" value="7098" />
10    <add key="UdpLocalNotificationPort" value="7097" />
11    <add key="serilog:minimum-level" value="Information" />
12    <add key="Serilog.File.Path" value="D:\ProgramData\Sestek\VoiceVerification\VerificationOnTheGoFrontSide\VerificationOnTheGoFrontSideLog.txt" />
13    <add key="Serilog.File.OutputTemplate" value="{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} [{Level:u3}] {Message:l1} {Properties:j}{NewLine}{Exception}" />
14    <add key="Serilog.File.SizeLimitBytes" value="10000000" />
15    <add key="Serilog.File.RetainedCountLimit" />
16  </appSettings>
17  <startup>
18    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
19  </startup>
20 </configuration>
```

- **VVFrontSideWcfWinSvc.exe.config**: **BaseAddress** should be checked. License keys must be defined here.

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <appSettings>
4     <add key="LicenseName" value="vb" />
5     <add key="StorageDir" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
6     <add key="BaseAddress" value="http://192.168.10.68:8040" />
7     <add key="HttpApiVersion" value="v1" />
8     <!--Possible values are "Library" and "Wcf"-->
9     <add key="MachineType" value="Wcf" />
10    <add key="serilog:minimum-level" value="Information" />
11    <add key="Serilog.File.Path" value="D:\ProgramData\Sestek\VoiceVerification\VVFrontSide\VVFrontSideWcfWinSvcLog.txt" />
12    <add key="Serilog.File.OutputTemplate" value="{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} [{Level:u3}] {Message:lj} {Properties:j}{NewLine}{Exception}" />
13    <add key="Serilog.File.SizeLimitBytes" value="10000000" />
14    <add key="Serilog.File.RetainedCountLimit" />
15    <add key="EnrollmentSwitch" value="E25D1F4CC835B154B5C63CE5E8B62AA88A9CC774719C59B1EC4323B3FA865A0"/>
16    <add key="IdentificationSwitch" value="6205EF52AC298BE2D58FF0AC5F2561E00088B41F997D09245888A511EF0001570102A152FC3E112A417858803E47113"/>
17    <add key="BlacklistSwitch" value="09A0F509FD52DA65274BF5CE161693BFFA9CF6F37EDB6788618FC74E4400507F"/>
18    <add key="RefundVoiceprintsSwitch" value="00AC0168BF678537EF08FA81FF07FB16842A077FA98E97975D58B0720D6C3B588FB887185910CC7C4D75591DAC7A7722"/>
19  </appSettings>
20  <startup>
21    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
22  </startup>
23 </configuration>

```

- **VVWorkerWcfWinSvc.exe.config**: **BaseAddress** should be checked.

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <appSettings>
4     <add key="RootDirPath" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
5     <add key="LicenseName" value="vb" />
6     <!--For legacy licenses-->
7     <add key="LicenseName.IsPath" value="false" />
8     <add key="StorageDir" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
9     <add key="ProjectDir" value="D:\ProgramData\Sestek\VoiceVerification\ProjectDir" />
10    <add key="BaseAddress" value="http://192.168.10.68:8041" />
11    <add key="HttpApiVersion" value="v1" />
12    <add key="serilog:minimum-level" value="Information" />
13    <add key="Serilog.File.Path" value="D:\ProgramData\Sestek\VoiceVerification\VVWorker\VVWorkerWcfWinSvcLog.txt" />
14    <add key="Serilog.File.OutputTemplate" value="{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} [{Level:u3}] {Message:lj} {Properties:j}{NewLine}{Exception}" />
15    <add key="Serilog.File.SizeLimitBytes" value="10000000" />
16    <add key="Serilog.File.RetainedCountLimit" />
17  </appSettings>
18  <startup>
19    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
20  </startup>
21 </configuration>

```

- **Votg.PocTool.dll**: **VotgFsBaseUrl** should be checked. It must match with **Votg FrontSideWcWinSvc**.

```

1 <?xml version="1.0"?>
2 <configuration>
3   <appSettings>
4     <add key="VotgFsBaseUrl" value="http://192.168.10.68:8090/VotgFrontSideOperations/" />
5     <add key="GlobalNotificationReceiverLocalPort" value="7767"/>
6     <add key="serilog:minimum-level" value="Debug"/>
7     <add key="serilog:using:File" value="Serilog.Sinks.File"/>
8     <add key="serilog:write-to:File.path" value="Log\VotgPocTool.log"/>
9     <add key="serilog:write-to:File.outputTemplate" value="{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} [{Level:u3}] {Message:lj} {Properties:j}{NewLine}{Exception}" />
10  </appSettings>
11 </configuration>

```

- Web config: **WebUiOperationsBaseuri** must match with **BaseAddress** in **VVFrontSideWcfWinSvc.exe.config**.

```

46 <!--StorageDir: Path of voice files required by WavRetriever-->
47 <add key="StorageDir" value="D:\ProgramData\Sestek\VoiceVerification\StorageDir" />
48 <!--WebUiOperationsBaseUri: Base uri for voice biometrics service-->
49 <add key="WebUiOperationsBaseUri" value="http://192.168.10.68:8040" />
50 <!--WebSiteUrl: Address of this website... Use externalIP if exists. Never use localhost or 127.0.0.1-->
51 <add key="WebSiteUrl" value="http://192.168.10.68:8042" />
52 <!--DomainName: The active domain to authorize user logins -->
53 <add key="DomainName" value="sestek.com.tr" />
54 <!--SingleSession: When "1" only one concurrent login per user. Default value: 0-->
55 <add key="SingleSession" value="1" />
56 <!--UserAuditLogAlert: When "1" a modal dialog will be shown to user, lists recent login information. When "2" dialog shows last unsuccessful login attempts. Default value:0 -->
57 <add key="UserAuditLogAlert" value="1" />
58 <!--TempFilePath: Uploaded files will be stored in here. So directory access should be granted for IUSR-->
59 <add key="TempFilePath" value="C:\Temp" />

```

- If web interface will be used, **requireSSL** attribute must be set to false in **httpCookies** and forms elements.

```

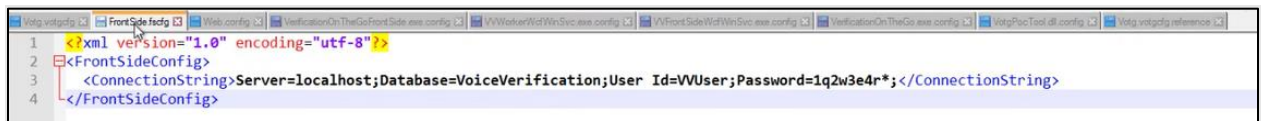
89 <system.web>
90 <hostingEnvironment shadowCopyBinAssemblies="false" />
91 <httpRuntime enableVersionHeader="false" maxRequestLength="102400" targetFramework="4.7.2" />
92 <!-- Should only be enabled when hosting over HTTPS -->
93 <httpCookies httpOnlyCookies="true" requireSSL="false" />
94 <compilation debug="false" targetFramework="4.7.2">
95 <assemblies>
96 <add assembly="System.Web.Abstractions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
97 <add assembly="System.Web.Helpers, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
98 <add assembly="System.Web.Routing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
99 <add assembly="System.Web.Mvc, Version=5.2.9.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
100 <add assembly="System.Web.WebPages, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
101 </assemblies>
102 </compilation>
103 <customErrors defaultRedirect="/ErrorPage?" mode="On" redirectMode="ResponseRedirect">
104 <error statusCode="403" redirect="/ErrorPage/Forbidden?403" />
105 <error statusCode="404" redirect="/ErrorPage/NotFound?404" />
106 <error statusCode="500" redirect="/ErrorPage/InternalServerError?500" />
107 </customErrors>
108 <authentication mode="Forms">
109 <forms loginUrl "~/Account/LogIn" requireSSL="false" timeout="86400" />
110 </authentication>
111 <globalization enableClientBasedCulture="true" culture="auto" uiCulture="auto" />
112 <pages controlRenderingCompatibilityVersion="4.0">
113 <namespaces>
114 <add namespace="System.Web.Helpers" />
115 <add namespace="System.Web.Mvc" />
116 <add namespace="System.Web.Mvc.Ajax" />
117 <add namespace="System.Web.Mvc.Html" />
118 <add namespace="System.Web.Routing" />
119 <add namespace="System.Web.WebPages" />
120 </namespaces>
121 </pages>
122 <sessionState timeout="120"></sessionState>
123 </system.web>

```



### 8.2.3. Voice Biometrics Shared Configurations

- FrontSide.fscfg: Connection string should be configured as needed.

A screenshot of a text editor showing the XML configuration for FrontSide.fscfg. The XML is as follows:

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <FrontSideConfig>
3   <ConnectionString>Server=localhost;Database=VoiceVerification;User Id=VVUser;Password=1q2w3e4r*</ConnectionString>
4 </FrontSideConfig>
```

- Navigate to **Votg.votgcfg** file located in **StorageDir** directory and edit **VotgEndpoints**, **GlobalNotificationClient**, **VVOperationsBaseUri**.

A screenshot of a text editor showing the XML configuration for the edited file. The XML is as follows:

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <VotgConfig>
3   <!-- List of Verification on the Go SOAP endpoints, each given as http://hostname:port/VotgOperations-->
4   <VotgEndpoints>http://192.168.10.68:8080/VotgOperations</VotgEndpoints>
5   <NotificationConfig>
6     <!--Global clients must be given as a pipe (|) separated list of endpoints, each given as hostname:port-->
7     <GlobalNotificationClients>192.168.10.68:7767</GlobalNotificationClients>
8   </NotificationConfig>
9   <VadConfig>
10    <!--Available values are: MULAW, ALAW, PCM-->
11    <OutputAudioFormat>PCM</OutputAudioFormat>
12  </VadConfig>
13  <VbClientConfig>
14    <VvOperationsBaseUri>http://192.168.10.68:8040</VvOperationsBaseUri>
15    <ContentCode>TextIndep</ContentCode>
16    <ChannelCode>Mixed</ChannelCode>
17  </VbClientConfig>
18 </VotgConfig>
```

Once these steps are completed, log directory will create logs like the example below:  
“Sestek.VerificationOnTheGoFrontSide.ServiceImpl.VotgFrontSideWebService is open and has the following endpoints:..”

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Sestek Voice Biometrics.

### 9.1. Verify Avaya Aura® Communication Manager


On Communication Manager, verify the status of the administered CTI link by using the **statusaesvcs cti-link** command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.1**, as shown below.

```
status aesvcs cti-link
```

| AE SERVICES CTI LINK STATUS |         |          |                    |               |           |           |
|-----------------------------|---------|----------|--------------------|---------------|-----------|-----------|
| CTI Link                    | Version | Mnt Busy | AE Services Server | Service State | Msgs Sent | Msgs Rcvd |
| 1                           | 12      | no       | aes95              | established   | 1780      | 1780      |

### 9.2. Verify Avaya Aura® Application Enablement Services

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary → Session Summary** screen is displayed. Verify the **User** column shows an active session with the Sestek user name from **Section 6.4**, and that the **# of Associated Devices** column reflects the total number of monitored extensions from **Section 5.2** and **Section 5.3**.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Aug 23 16:06:09 2022 from 172.16.8.167  
Number of prior failed login attempts: 0  
HostName/IP: aes155.aura.com/10.128.226.155  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.0.1.0.7-0  
Server Date and Time: Mon Oct 17 18:43:58 ICT 2022  
HA Status: Not Configured

Status | Status and Control | DMCC Service Summary

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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
Generated on Mon Oct 17 18:43:58 ICT 2022

Service Uptime: 53 days, 4 hours 29 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 214

Number of Existing Devices: 11

Number of Devices Created Since Service Boot: 328

|                          | Session ID                               | User   | Application          | Far-end Identifier | Connection Type | # of Associated Devices |
|--------------------------|--|--------|----------------------|--------------------|-----------------|-------------------------|
| <input type="checkbox"/> | 4EA3C633F96188DC6<br>39EA3E349ADC6AB-211 | redbox | Red Box Recorder     | 10.128.224.10      | XML Encrypted   | 8                       |
| <input type="checkbox"/> | AFE4E926F1C8A5E79<br>1E38CAB6F7851AA-214 | sestek | SestekFalconRecorder | 10.103.1.50        | XML Encrypted   | 3                       |

Terminate Sessions | Show Terminated Sessions

Click on active **Session ID** with the sestek username to show number of monitored extensions.

**DMCC Service Summary - Session Detail**  
☐ Enable page refresh every  seconds

**Detailed Session View**  
Generated on Mon Nov 21 19:26:43 ICT 2022  
Session ID: 6911DC794447A3178D9CA959F74BA04E-4999  
State: Active  
Time Established: Mon, Nov 21, 2022 07:16:11 PM GMT+07:00  
Uptime: 0 days, 0 hours, 10 minutes, and 31 seconds  
Cleanup Delay Timer: 5 seconds  
Session Duration Timer: 600 seconds  
Time of Most Recent Timer Reset: Mon, Nov 21, 2022 07:26:11 PM ICT  
Reconnect Counter: 0  
Terminate Sessions

**Devices Associated with Session**

|                          | Device ID             | State |
|--------------------------|-----------------------|-------|
| <input type="checkbox"/> | 81002:CM145:0.0.0.0:2 | IDLE  |
| <input type="checkbox"/> | 81003:CM145:0.0.0.0:2 | IDLE  |
| <input type="checkbox"/> | 81001:CM145:0.0.0.0:2 | IDLE  |

Terminate Selected Devices Back

Item 1-3 of 3

### 9.3. Verify Sestek Voice Biometrics

On Sestek server, open **Sestek VotG POC Tool** provide by Sestek, the POC show as below:

The screenshot displays the Sestek VotG POC Tool interface. It features a top navigation bar with 'Active Calls' and 'Call Simulation' tabs. Below the tabs is a 'Refresh' button with a circular arrow icon and the text 'FS'. The main area is divided into two columns. The left column, titled 'Call Operations', contains input fields for 'Call ID', 'Agent ID', 'Phone Number', 'User Code', and 'User\_001'. Below these fields are four buttons: 'Enroll Begin' (green), 'Enroll Com' (blue), 'Enroll Canc' (red), and 'Authenticati' (green). The right column, titled 'Operation Progress', displays transaction details: 'Transaction ID -', 'Transaction Type -', 'Transaction State -', 'Total Speech / Required Speech' (0 / 0), 'Discarded Speech 0', 'Process Result -', 'Speech Result -', 'Result Code -', and 'Result Text'.

| Call Operations |             | Operation Progress             |
|-----------------|-------------|--------------------------------|
| Call ID         |             | Transaction ID -               |
| Agent ID        |             | Transaction Type -             |
| Phone Number    |             | Transaction State -            |
| User Code       |             | Total Speech / Required Speech |
| User_001        |             | 0 / 0                          |
| Enroll Begin    | Enroll Com  | Discarded Speech 0             |
| Enroll Canc     |             | Process Result -               |
| Authenticati    | Authenticar | Speech Result -                |
|                 |             | Result Code -                  |
|                 |             | Result Text                    |

From PSTN, place a call to AACC. Verify that AACC can receive incoming call, and POC Toll shows a new call in **Active Call** tag. Select **Enroll Begin** to start enrollment for new user biometrics.

The screenshot displays the Sestek VotG POC Tool interface. The top bar shows 'Active Calls' and 'Call Simulation' tabs. Below the tabs is a 'Refresh' button. The 'Active Calls' section lists a call with 'Call ID: 7' and 'Phone # 81002'. The 'Call Operations' section contains input fields for 'Call ID', 'Agent ID', 'Phone Number', 'User Code', and 'User\_001'. Below these fields are buttons for 'Enroll Begin', 'Enroll Cancel', 'Authenticate', and 'Authenticate'. The 'Operation Progress' section shows fields for 'Transaction ID', 'Transaction Type', 'Transaction State', 'Total Speech / Required Speech' (displaying '0 / 0'), 'Discarded Speech', 'Process Result', 'Speech Result', 'Result Code', and 'Result Text'.



## 10. Conclusion

These Application Notes describe the configuration steps required for Sestek Voice Biometrics to successfully interoperate with Avaya Aura® Contact Center 7.1.2 and Avaya Aura® Application Enablement Services 10.1 using Multiple Registration. All feature and serviceability test cases were completed successfully with all test cases are passed.

## 11. Additional References

This section references the Avaya and Sestek Voice Biometrics 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 10.1.x, Issue 1, Dec 2021
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022
4. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 4, April 2022

Product Documentation for Sestek products may be found at <https://www.sestek.com/>.

---

**©2023 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).