**Avaya Solution & Interoperability Test Lab**

# Application Notes for configuring KSV-VOIZIN Self-Service Authentication IVR to interoperate with Avaya Experience Portal and Avaya Aura® Communication Manager - Issue 1.0

## Abstract


These Application Notes describe the configuration steps for KSV-VOIZIN Self-Service Authentication IVR 1.0 to successfully interoperate with Avaya Experience Portal R8.1.1 and Avaya Aura® Communication Manager R10.1.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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.





©2022 Avaya Inc. All Rights Reserved.

# 1. Introduction

These Application Notes describe the compliance tested configuration of KSV-VOIZIN Self-Service Authentication IVR 1.0 with Avaya Experience Portal R8.1.1 and Avaya Aura® Communication Manager R10.1.

The solution from Kaizen Secure Voiz (KSV) consists of the KSV Avaya Integration web application installed on Apache Tomcat Web Server and the user authentication located at KSV cloud where the recorded voice will be posted via REST API to KSV Voice Biometric Engine platform. The Voice Biometric Engine on the platform will verify the recorded voice and returned the result to the web application. KSV Avaya Integration is a piece of middleware between Experience Portal and Voice Biometric Engine platform.

In a typical contact center environment such as banking, a customer would be calling into the system with a given ID. If this is a new customer, the customer's voice will be enrolled by saying a voice phrase. If it is a return customer, the voice will be authenticated before proceeding further for the services offered by the contact center. This particular solution is targeted at business verticals like telephone banking, tele-voting, and credit card services.

# 2. General Test Approach and Test Results

The tested solution contains a web application from KSV, hosted on Apache Tomcat that sends voice audio to the cloud-based Voice Biometric Engine platform for user authentication. The web application is written by KSV engineer using Avaya Orchestration Designer. The Experience Portal is configured to call this web application during a phone call, the web application gathers voice audio and sends it to the KSV's Voice Biometric Engine platform hosted in the cloud to authenticate an existing user or enrolled a new user. In the compliance testing, the Tomcat host was running on a Windows Server 2016 Standard.

The general test approach was to configure the KSV web application to communicate with Experience Portal as implemented on a customer's premises. See **Figure 1** for a network diagram. The interoperability compliance testing included feature and serviceability testing. The feature testing verified the ability of user authentication to process voice recordings made during VoiceXML calls and to analyse their validity. Callers are greeted with a demo script where speaker user ID is verified first. The verification software will then ask speaker for a phrase and determine if the caller is genuine. The serviceability testing introduced simulated LAN failures and server reboots and observing the caller experience after the simulation.

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.


©2022 Avaya Inc. All Rights Reserved.

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 the KSV web applications did not include use of any specific encryption features as requested by KSV.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The testing included:

- **Connectivity** – Test that the KSV Avaya Integration application was installed correctly on Apache Tomcat.
- **Enrolling a new user** – Create a new user and associated phrase.
- **Verify existing enrolment** – Test existing phrase voice verification.
- **Verify imposter is rejected** – Test resilience by saying the phrase with a different voice.
- **Serviceability testing** – Test the experience of the caller and the behaviour of user authentication Voice Biometrics after the web server and Experience Portal MPP are restarted, and also when there is a LAN failure.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully. The following observations were noted.

- The quality of the voice biometrics was not the focus of the compliance testing.
- The Apache Tomcat Web Server is considered a third-party product that hosts web applications such as KSV Avaya Integration.

## 2.3. Support

Technical support can be obtained for Kaizen Secure Voiz as follows:

- Website: sales@kaizenvoiz.com
- Phone: +1 732-573-4377


©2022 Avaya Inc. All Rights Reserved.

# 3. Reference Configuration

**Figure 1** shows the network topology during interoperability testing. Communication Manager was used as the hosting PBX. The KSV Avaya Integration web application was installed on an Apache Tomcat, running on a Windows Server 2016 Standard. Session Manager is used to route calls to Experience Portal which then calls upon the user to input the User ID to check user's validity. The user's voice is either enrolled if it is a new user or authenticated if it is a previously enrolled user.

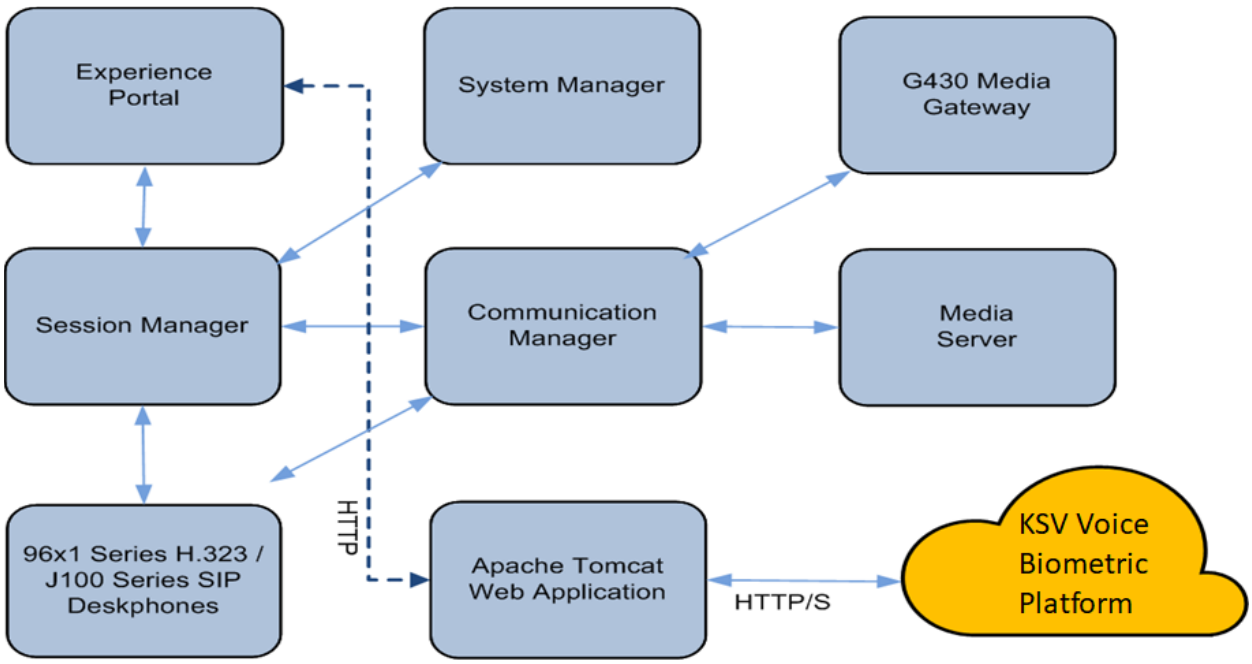



**Figure 1: KSV-VOIZIN Self Service Authentication IVR integrating with Avaya Experience Portal and Avaya Aura® Communication Manager**


©2022 Avaya Inc. All Rights Reserved.

# 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 | 10.1 SP2<br>(10.1.0.2.0.974.27607) |
| Avaya G430 Media Gateway | 42.80 |
| Avaya Aura® System Manager | 10.1 SP2<br>Build 10.1.0.0.537353<br>Hot Fix 1010215160 |
| Avaya Aura® Session Manager | 10.1 SP2<br>(10.1.0.2.1010215) |
| Avaya Aura® Media Server | 10.1.0.101 |
| Avaya Experience Portal | 8.1.1.0.0216 |
| Avaya 96x1 Series Deskphones (H.323) | 9.8532 |
| Avaya J100 Series Deskphones (SIP) | 4.0.13 |
| KSV-VOIZIN Self-Service Authentication IVR | 1.0 |
| Apache Tomcat Web Server<br>Java (64 bit)<br>running on Windows Server Standard | 8.5.23<br>1.8.0_311-b11<br>2016 |

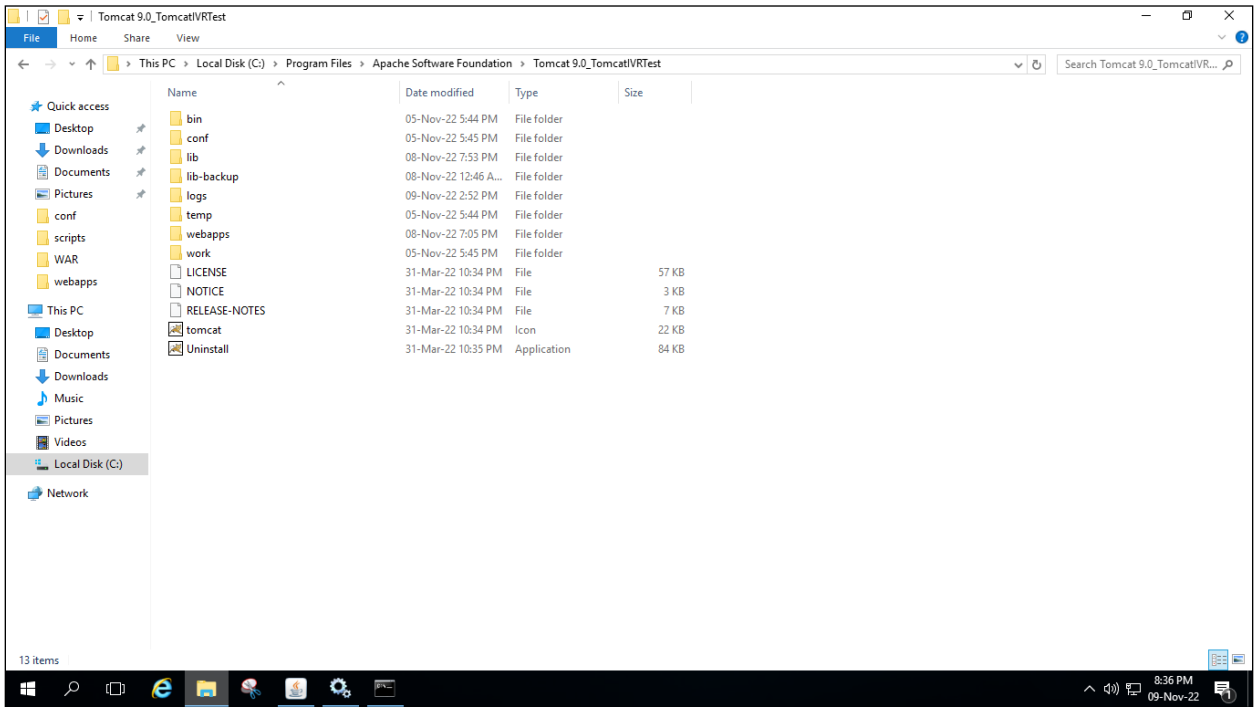

©2022 Avaya Inc. All Rights Reserved.

# 5. Configure KSV-VOIZIN Self-Service Authentication IVR Apache Tomcat Web Application

The Apache Tomcat Web Application is considered a third-party product that hosts web applications such as KSV Avaya Integration. Tomcat can run on the same server as Experience Portal but for this solution, it is hosted on Windows Server 2016.

The installation and configuration of Apache Tomcat is outside the scope of these Application Notes. In a production environment the Windows Service Installer is recommended, but it assumed a client will have their own Tomcat installation standards.

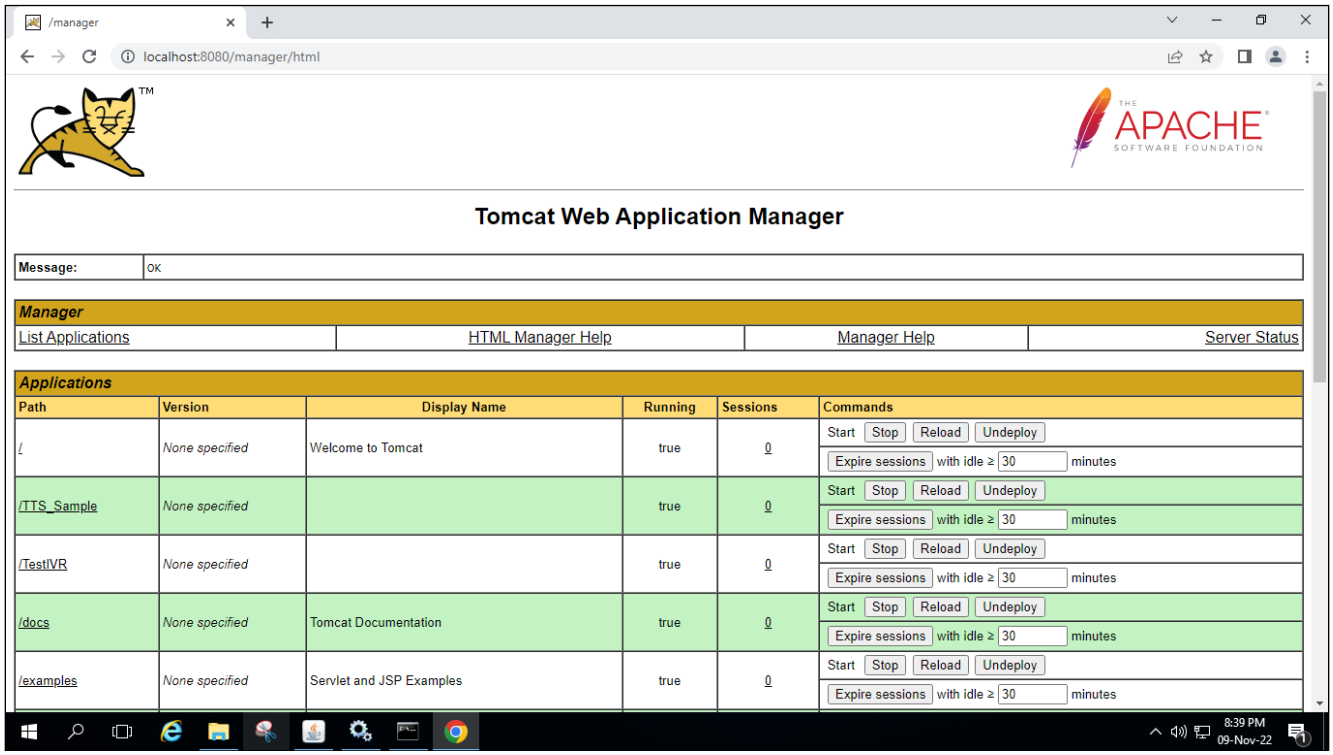
From the Windows machine running Tomcat, locate the Apache tomcat folder. Within this folder navigate to **webapps** and place the **.war** file into the **webapps** folder. Tomcat monitors this webapps directory for changes, and if it finds a new file there, it will attempt to deploy it.





©2022 Avaya Inc. All Rights Reserved.

Login to the Tomcat Web Application Manager as below. Start the application and in this case "TestIVR" by clicking the "Start" button under the "Commands" column in the appropriate row if it is not started.



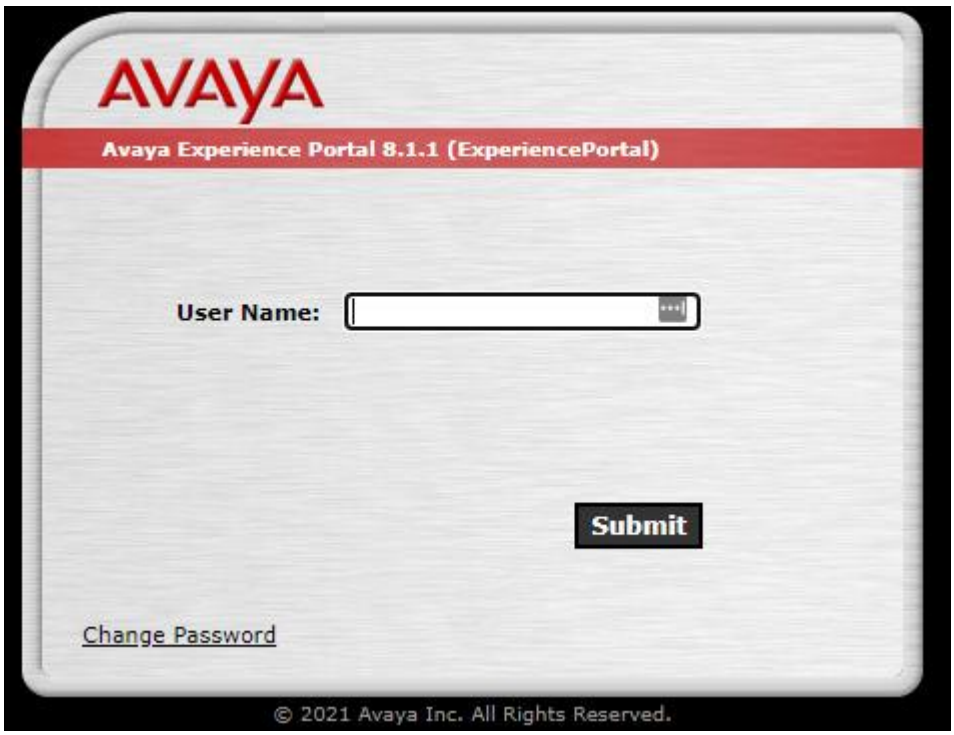


©2022 Avaya Inc. All Rights Reserved.

# 6. Configure Avaya Experience Portal

The information provided in this section describes the configuration of Experience Portal relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Open a web browser and navigate to the Experience Portal address as shown below **https://<ExpPortal IP>/VoicePortal**. Enter the appropriate credentials and click on **Submit**.





©2022 Avaya Inc. All Rights Reserved.

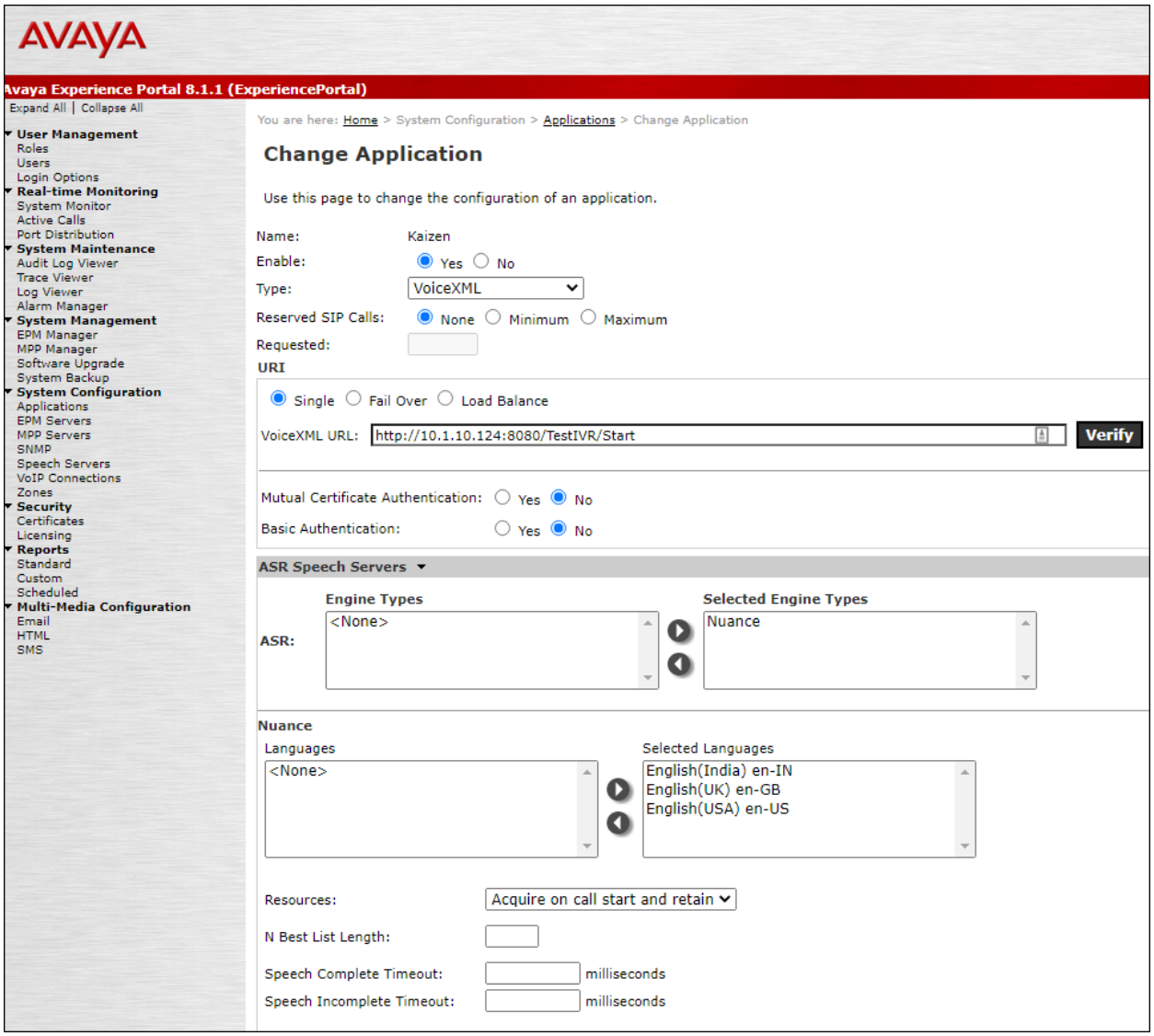
An application is added on Experience Portal as a Voice XML application. This will then call on the KSV Avaya Integration application running on Tomcat. From Experience Portal navigate to **System Configuration → Applications** in the left window. In the main window click on **Add**.

The following information must be added.

- **Name**: Enter a suitable name for the new application in the example on the following page is **Kaizen**.
- **Type**: This is set to **VoiceXML**.
- **VoiceXML URL**: This will be the location of the deployed application. As the tomcat server is running on a Window machine this will be the IP address of the Windows Server address followed by **8080** as this is the port used for the http connection. The application name follows, in this case **TestIVR** followed by **/Start**.
- **ASR Speech Servers**: The speech server is added for the automated speech recognition (ASR), in the example on the following page **Nuance** is the configured **Engine Types**. This Speech Server is already configured as part of the Experience Portal configuration. This Speech Server will have **Languages** already configured and the example on the following page shows the languages available.
- **TTS Speech Servers**: The speech server is added for the text to speech (TTS), in the example on the following page **Nuance** is the configured **Voices**. This Speech Server is already configured as part of the Experience Portal configuration. This Speech Server will have **Voices** already configured and the example on the following page shows the voices available.
- **Called Number**: This is the number assigned to the application i.e., the number that is called which routes the caller into the application. The example below shows that **10392** was chosen.


©2022 Avaya Inc. All Rights Reserved.

All other values can be left as shown as this was default. Click on **Apply** and **Save** at the bottom of the screen to save the new application.



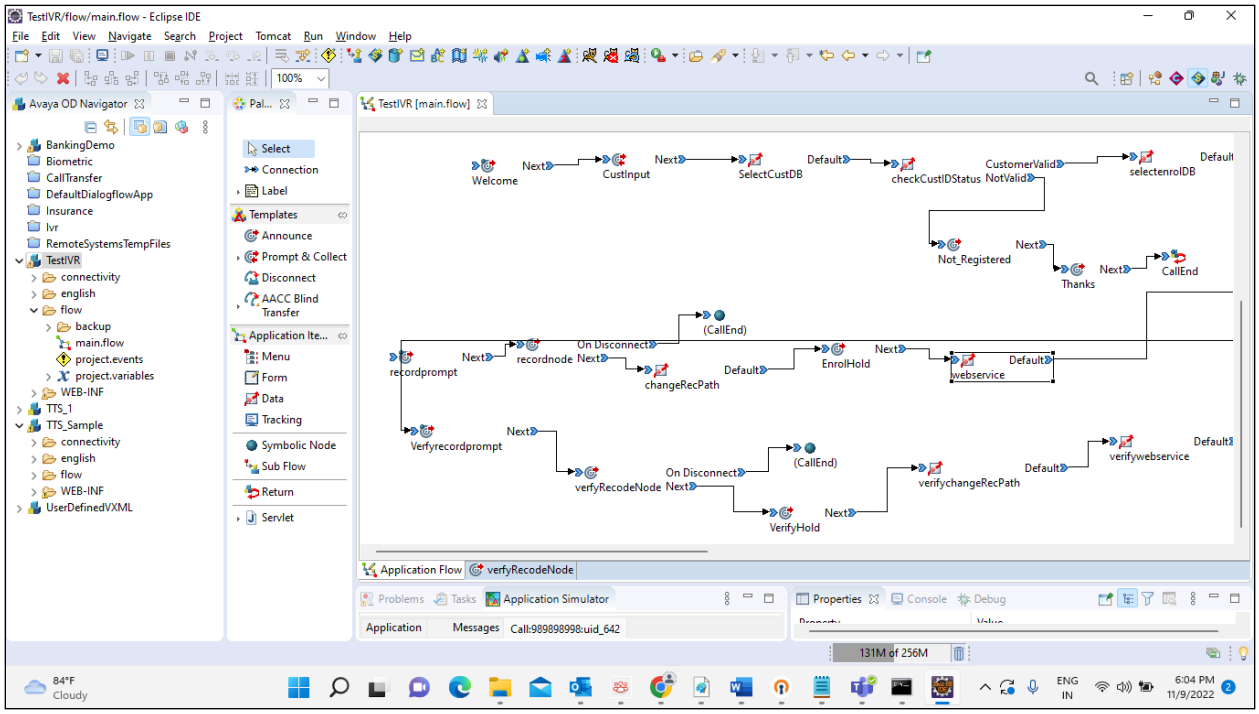


©2022 Avaya Inc. All Rights Reserved.

©2022 Avaya Inc. All Rights Reserved.

# 7. Configure KSV-VOIZIN Self-Service Authentication IVR

The solution from KSV consists of the KSV Avaya Integration installed on Apache Tomcat Web Server and the user authentication located at KSV cloud where the recorded voice will be posted via REST API to KSV Voice Biometric Engine platform. KSV Avaya Integration is a piece of middleware between Experience Portal and Voice Biometric Engine platform. The KSV Avaya Integration consists of a .war file that is created by KSV. The installation of this .war file is outlined in **Section 5** and any further information on this can be obtained directly from KSV using the contact information provided in **Section 2.3**. Below is screenshot of the developed call flow using the Orchestration Designer for the self-service IVR using KSV Voice Biometric authentication.





©2022 Avaya Inc. All Rights Reserved.

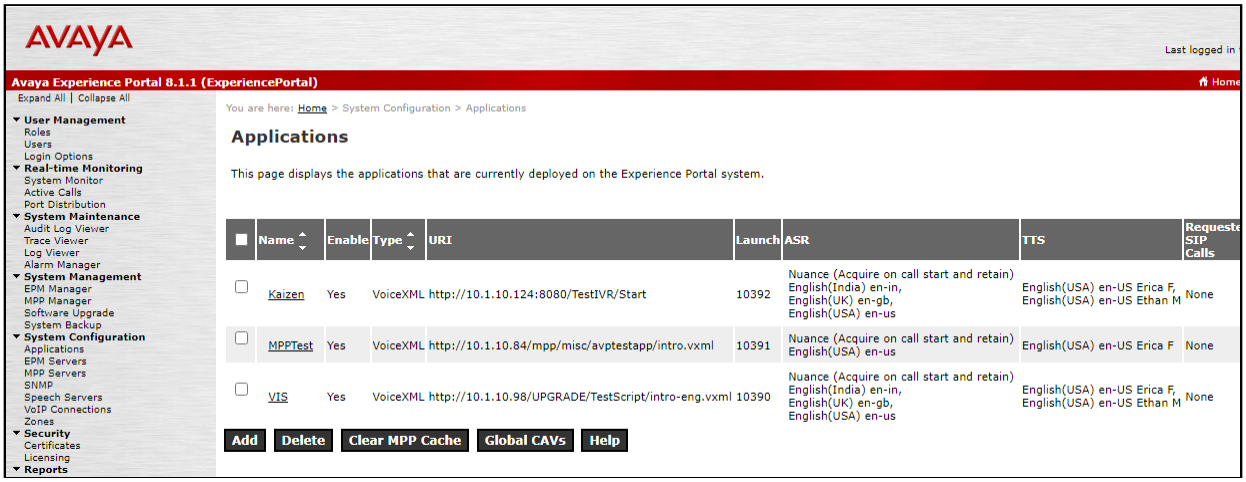
# 8. Verification Steps

This section provides the steps that can be performed to verify correct configuration of Experience Portal with KSV-VOIZIN Self-Service Authentication IVR.

## 8.1. Verify User Authentication Voice Biometric Application on Experience Portal

Log into Experience Portal as per **Section 6**.

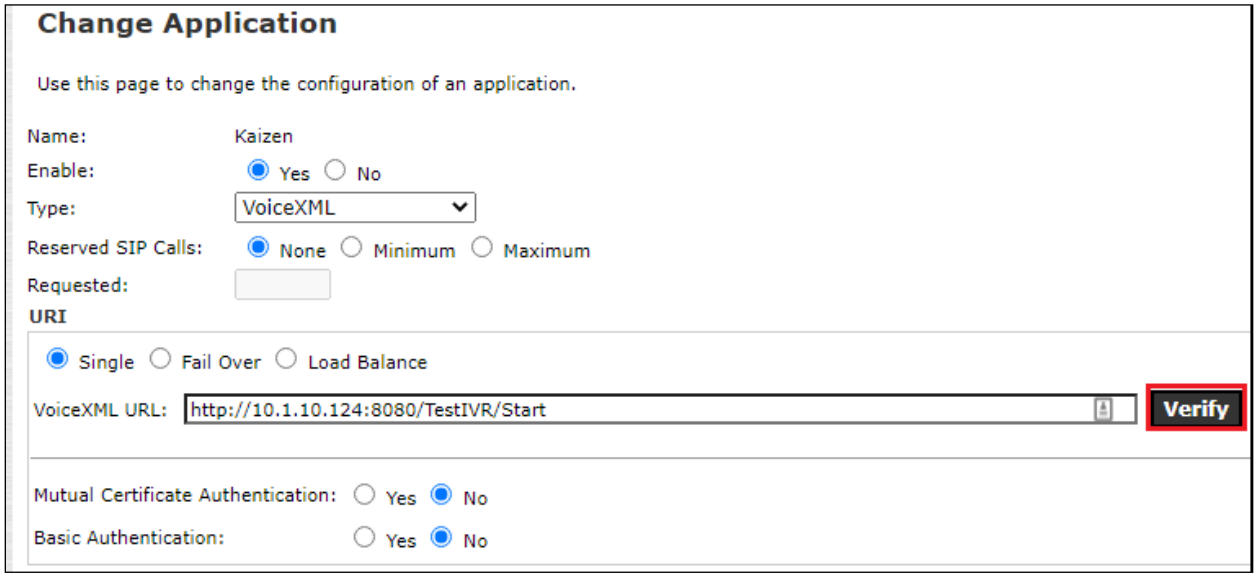
Navigate to **System Configuration → Applications** in the left window (not shown). The **Kaizen** application should be visible in the main window. Click on this application.



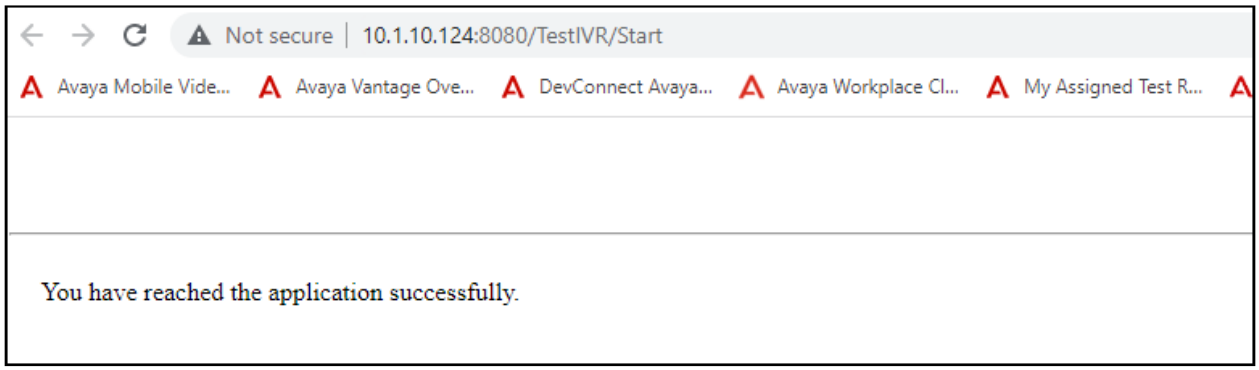


©2022 Avaya Inc. All Rights Reserved.

Click on **Verify** opposite the **VoiceXML URL**.




A new web page should be opened showing the page below stating, "**You have reached the application successfully**". This is a successful verification of the application.




## 8.2. Make a call to the User Authentication Voice Biometric Application

Make a call to the number associated with the Kaizen application in **Section 6**. This is the "Called Number" as per **Section 6**. The caller should be greeted by the application instructing the caller to participate in voice biometric enrolment and/or verification.


©2022 Avaya Inc. All Rights Reserved.

# 9. Conclusion

These Application Notes describe the configuration steps required for KSV-VOIZIN Self-Service Authentication IVR 1.0 to successfully interoperate with Avaya Experience Portal R8.1.1 and Avaya Aura® Communication Manager R10.1. All feature functionality and serviceability test cases were completed successfully, with observations noted in **Section 2.2**.

# 10. Additional References

This section references the Avaya and KSV product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at *https://support.avaya.com*.


[1] *Avaya Experience Portal Overview and Specification*, Release 8.1.1, Issue 2, February 2022

[2] *Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment*, Release 8.1.1, Issue 1, January 2022

[3] *Administering Avaya Experience Portal*, Release 8.1.1, Issue 2, February 2022

[4] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021

[5] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022


Product documentation for Kaizen Secure Voiz products can be obtained from the member from the contact information in **Section 2.3**.


[1] *Voice Biometric Server Edition I-Vector System SDK*, Version 1.0, May 2021

[2] *Voice Biometric Server Edition I-Vector System Core Product Manual*, Version 1.0, May 2021




©2022 Avaya Inc. All Rights Reserved.

**©2022 Avaya Inc. All Rights Reserved.**
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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