



Avaya Solution & Interoperability Test Lab

Application Notes for Utry IVR Optimization Analysis System with Avaya Voice Portal R5.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Utry IVR Optimization Analysis System with Avaya Voice Portal. IVR Optimization Analysis System analyzes and reports on IVR call and application tree navigation data generated by applications running in an Avaya Voice Portal environment.

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 to integrate Utry IVR Optimization Analysis System with Avaya Voice Portal. Utry IVR Optimization Analysis System analyzes and reports on IVR (Interactive Voice Response system) call and application tree navigation data generated by applications running in an Avaya Voice Portal environment.

The main function of Utry IVR Optimization Analysis System is to analyze and report customer behavior when interacting with an IVR system such as Avaya Voice Portal. When a user calls an IVR application, a menu is presented and the user interacts with the IVR application using the telephone keypad or voice. The application server that the IVR application resides logs those IVR interaction information including keys pressed, voice node reached, etc. into text files. To provide the right set of interaction information, Utry has defined the format of the log files for the application to use. The log files are transferred to Utry IVR Optimization Analysis System periodically using FTP, and based upon the log files Utry IVR Optimization Analysis System calculates the KPI (Key Performance Indicator) and evaluates the performance of the IVR application for the purpose of improving and optimizing the structure of the IVR menu. The results are stored in a local database and can be accessed via a web browser.

In the Avaya Voice Portal environment, the applications are developed using Avaya Dialog Designer. During the development phase, Avaya Voice Portal applications have to incorporate code to generate log files that contain call and application tree navigation data following the formats defined by Utry. In the log files, call id, caller id, and callee id items are collected using a CTI Collector provided by Avaya Dialog Designer. The CTI Collector interfaces with Avaya Aura[®] Application Enablement Services to obtain such call related information.

2. General Test Approach and Test Results

This section describes the compliance testing approach used to verify IVR Optimization Analysis System integration with Voice Portal and the test results.

The compliance test used a sample Dialog Designer application that was developed by Utry to perform the test. The application was enhanced to provide call and application tree navigation data as input to IVR Optimization Analysis System.

The focus of the test was to make sure that the sample application is interoperable with the Voice Portal vxml engine and the IVR interactions data was captured and processed correctly by the sample application and IVR Optimization Analysis System.

The test approach was to first identify all the paths of the application menu and make phone calls to exercise all the paths. Once the calls were made and data processed, verified that the log files created and data displayed by IVR Optimization Analysis System matched the calls and the key sequences entered. Conditions where the entered keys were invalid were also verified. In these cases, the keys were ignored.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature test cases were performed manually based upon the following steps:

- From a PSTN phone or an internal phone dial the number that is associated with the Utry sample application.
- Interact with the sample application using a sequence of keystrokes to exercise a particular path of the application tree.
- Verify that the call and the key sequence entered are correctly recorded in the log files.
- Repeat the previous step so all the possible paths of the application tree are exercised.
- Enter a key that is not allowed and observe the behavior.
- Schedule an FTP job on the application server to transfer the log files to IVR Optimization Analysis System.
- On the IVR Optimization Analysis System, schedule a service to import the log data and perform calculation and analysis. The results are stored in a local database.
- Access the web interface of IVR Optimization Analysis System to verify that the displayed data match the calls made and the key sequences entered.

The serviceability testing focused on verifying the ability of the Utry server and Voice Portal to recover from adverse conditions, such as network outages and system reboots.

2.2. Test Results

All test cases passed with the exception of one observation described below.

The file transfer and import function of the Utry solution only transferred files of the previous day. If the log files of a particular day did not get transferred on the following day due to system unavailability or network outage, they would have to be manually handled in order for the data to be transferred and imported to IVR Optimization Analysis System.

2.3. Support

For technical support on IVR Optimization Analysis System, contact Utry via phone, email, or internet.

- **Phone:** +86 400 028 2200
- **Email:** info@utry.cn
- **Web:** www.utry.cn

3. Reference Configuration

Figure 1 illustrates the configuration used for testing. In this configuration, Voice Portal interfaced with Communication Manager via H.323 connections. The Tomcat Application Server hosted the Utry sample application which generated application tree navigation data as the application was executed. The Utry server, which hosted IVR Optimization Analysis System and an accompanying Oracle database, was a VMWare based virtual machine residing on a server blade.

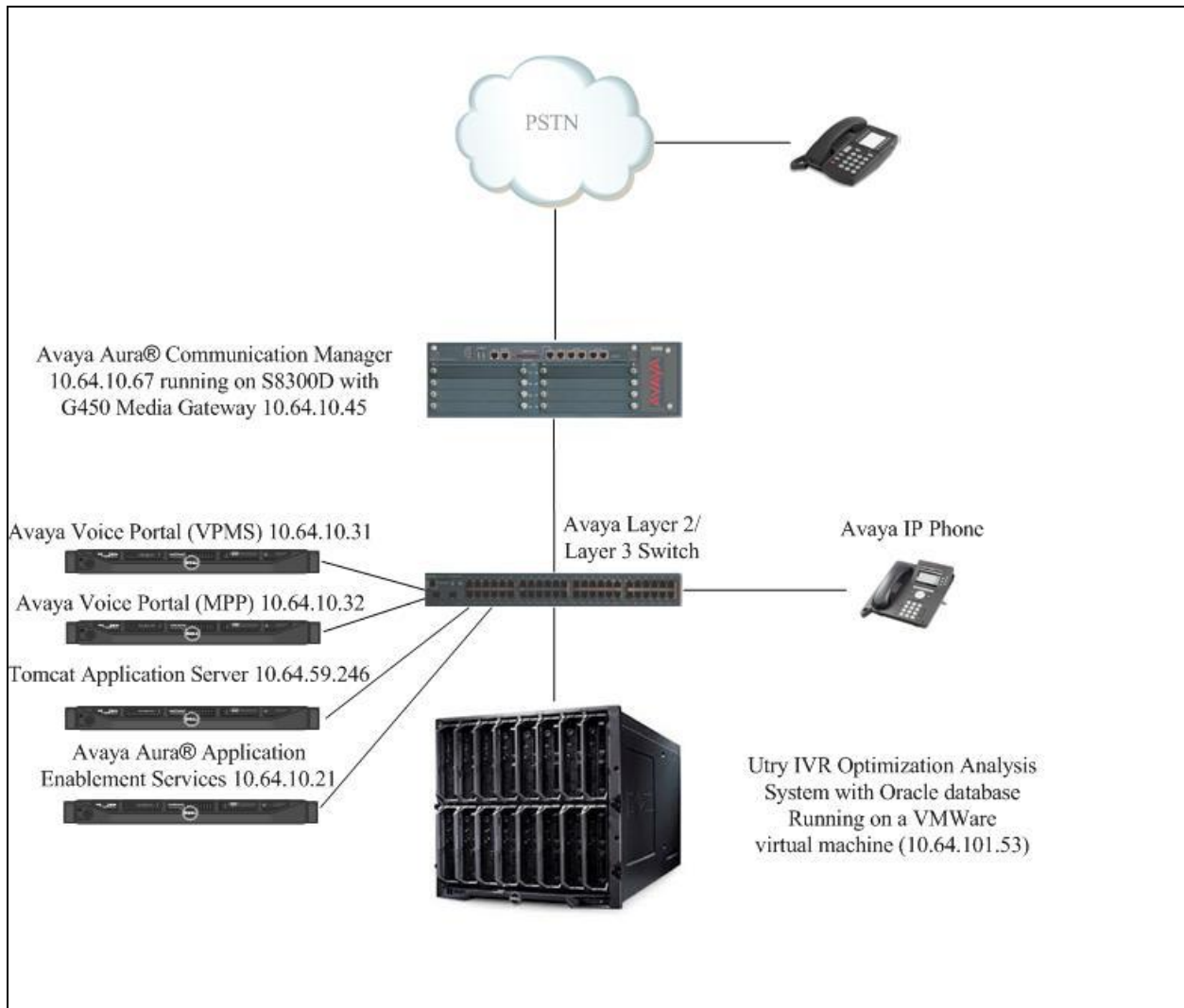


Figure 1: Configuration with Avaya Voice Portal and Utry IVR Optimization Analysis System

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Voice Portal	R5.1 SP3 (5.1.0.3.0502)
Application Server running under Ubuntu OS <ul style="list-style-type: none">• Apache Tomcat• Avaya Dialog Designer WebLM License Server• Sample application developed using Dialog Designer	6.0.35 4.7.1 5.1.11
Avaya S8300D Server running Avaya Aura® Communication Manager	Release 6.2 SP3 (02.0.823.0-20001)
Avaya G450 Media Gateway MGP MM710 T1 Module	HW 1 FW 31.20.0 HW 04 FW 015
Avaya Aura® Application Enablement Services	r6-1-1-30-0
Avaya 96x0 H.323 Telephones	Avaya one-X® Deskphone Release 3.1.5
Avaya 96x1 H.323 Telephones	Avaya one-X® Deskphone Release 6.2.2
Utry IVR Optimization Analysis System <ul style="list-style-type: none">• Windows Server• Oracle database	2.0 2008 R2 10.2.0

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager via the System Access Terminal (SAT). It is assumed that the administration for IP node names, network regions, and IP Codec Set is already in place and will not be discussed here. The procedures include the following area:

- Administer H.323 Stations for Voice Portal
- Administer CTI Link for TSAPI

5.1. Administer H.323 Stations for Avaya Voice Portal

This section describes the configuration of H.323 stations for Voice Portal. The H.323 stations are used for setting up IP connections between Communication Manager and Voice Portal.

From the System Access Terminal (SAT), use the **add station n** command to add an H.323 station, where **n** is an available station extension. In the station form, set the **Type** to **7434ND**, provide a descriptive **Name**, set the **Security Code**, and set the **IP Softphone** field to **y**. The COR specified for this station should allow outgoing trunk calls. Repeat this step with the same **Security Code** for each Voice Portal port.

add station 25508		Page 1 of 6
STATION		
Extension: 25508	Lock Messages? n	BCC: 0
Type: 7434ND	Security Code: 123456	TN: 1
Port: S00023	Coverage Path 1:	COR: 1
Name: AVP Station	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Module? n	Message Lamp Ext: 25508	
Display Module? y		
Display Language: english	Coverage Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	Remote Office Phone? n	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

5.2. Administer CTI Link for TSAPI

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: 6201		
Type: ADJ-IP		
Name: to AES-10.64.10.21		COR: 1

6. Configure Avaya Voice Portal

This section covers the administration of Voice Portal. The following configuration steps are covered:

- Configuring H.323 VoIP Connections
- Configuring Application

Voice Portal is configured via the Voice Portal Management System (VPMS) web interface. To access the web interface, enter **http://<ip-addr>** as the URL in an internet browser, where **<ip-addr>** is the IP address of the VPMS. Log in using appropriate credentials. The screen is shown as follows.

The screenshot displays the Avaya Voice Portal Management System (VPMS) web interface. At the top left is the Avaya logo. At the top right, it says "Welcome, admin" and "Last logged in today at 4:08:03 PM EST". Below this is a red header bar with "Voice Portal 5.1 (VoicePortal)" on the left and "Home", "Help", and "Logoff" links on the right. A left sidebar contains a navigation menu with categories like "User Management", "Real-Time Monitoring", "System Maintenance", "System Management", "System Configuration", "Security", and "Reports". The main content area shows "You are here: Home" and "Voice Portal Management System Version 5.1.0.3.0502". It includes a description of the VPMS and a "Legal Notice" section with copyright information and disclaimers. At the bottom, it shows "Last Login: 1/28/13 4:08:03 PM EST".

6.1. Configure H.323 VoIP Connections

From the left pane, click **System Configurations** → **VoIP Connections** and then click the **H.323** tab followed by the **Add** button. The **Add H.323 Connection** screen is displayed. For the **Name** field, enter a descriptive name. For the **Gatekeeper Address** field, enter the IP address of Communication Manager. Under the **New Stations** section, enter the station extensions and password configured in **Section 5.1** in the **From**, **To**, and **Password** fields, click the **Same Password** radio button, and select **Inbound and Outbound** for the **Station Type** field. Click **Add** to add the stations and **Save** to submit.

AVAYA Welcome, admin
Last logged in 1/31/13 at 4:03:22 PM EST

Voice Portal 5.1 (VoicePortal) Home Help Logoff

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-Time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Alarm Codes
 - Alarm/Log Options
 - Applications
 - MPP Servers
 - Report Data
 - SNMP
 - Speech Servers
 - VoIP Connections
 - VPMS Servers
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > Add H.323 Connection

Add H.323 Connection

Use this page to add a new H.323 connection.

Name:

Enable: ☒ Yes ☐ No

Gatekeeper Address:

Alternative Gatekeeper Address:

Gatekeeper Port:

Media Encryption: ☒ Yes ☐ No

New Stations

From	To
Station: <input type="text" value="25508"/>	<input type="text" value="25509"/>
Password: <input type="password" value="....."/>	
<input checked="" type="radio"/> Same Password <input type="radio"/> Use sequential passwords	
Station Type: <input type="text" value="Inbound and Outbound"/> <input type="text" value="Inbound Only"/> <input type="text" value="Maintenance"/>	

Add

Configured Stations (M for Maintenance, I for Inbound Only)

<No Station>

Remove

Save Cancel Help

6.2. Configure Application

From the left pane, click **System Configurations** → **Applications** to navigate to the **Applications** page and then click the **Add** button. The **Add Application** page is displayed. In the **Name** field, enter a descriptive name. Under the **URL** section, enter the URL to the Utry sample application on the Tomcat Application Server in the **VoiceXML URL** field. In the **Application Launch** section, add a station extension configured in **Section 5.1** and click **Add**. Repeat for the rest of station extensions. The screen below shows that extensions **25508** and **25509** have been added. Click **Save**.

AVAYA Welcome, admin
Last logged in today at 4:08:03 PM EST

Voice Portal 5.1 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

- ▼ **User Management**
 - Roles
 - Users
 - Login Options
- ▼ **Real-Time Monitoring**
 - System Monitor
 - Active Calls
 - Port Distribution
- ▼ **System Maintenance**
 - Audit Log Viewer
 - Trace Viewer
 - Log Viewer
 - Alarm Manager
- ▼ **System Management**
 - MPP Manager
 - Software Upgrade
 - System Backup
- ▼ **System Configuration**
 - Alarm Codes
 - Alarm/Log Options
 - Applications
 - MPP Servers
 - Report Data
 - SNMP
 - Speech Servers
 - VoIP Connections
 - VPMS Servers
- ▼ **Security**
 - Certificates
 - Licensing
- ▼ **Reports**
 - Standard
 - Custom
 - Scheduled

Add Application

Use this page to deploy and configure a new VoiceXML or CCXML application on the Voice Portal system.

Name:

Enable: ☒ Yes ☐ No

Type:

URL

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL: **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR: TTS:

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number: **Add**

Remove

Speech Parameters

▶

Reporting Parameters

▶

Advanced Parameters

▶

Save **Cancel** **Help**

7. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services as follows:

- Launch Avaya Aura® Application Enablement Services Console
- Verify TSAPI Licenses
- Administer TSAPI Link
- Obtain Tlink Name
- Restart TSAPI service
- Administer User for TSAPI
- Change User Access Permission

It is assumed that the switch connection between Application Enablement Services and Communication Manager is already in place and does not need to be specified in this section.

7.1. Launch Avaya Aura® Application Enablement Services Console

Access Application Enablement Services web interface by using the URL **https://<ip-addr>** in a web browser, where **<ip-addr>** is the IP address of the Application Enablement Services server.

The **Welcome to Avaya Application Enablement Services** screen is displayed (not shown). Click **Continue to Login**. The **Please login here** screen is displayed (not shown). Log in using appropriate credentials. The **Welcome to OAM** screen is displayed.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Jan 31 16:51:39 2013 from 10.64.10.51
HostName/IP: aes6_tr1/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Home | Help | Logout

Home

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ 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.
- 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 both domains, or a separate administrator for each domain.

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

7.2. Verify TSAPI Licenses

As an Avaya product Dialog Designer is granted unrestricted access to the TSAPI interfaces. No additional **TSAPI Simultaneous Users** licenses are required for TSAPI access.

7.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**. Note that the TSAPI link used for this test is Link 1 which is already configured. The screen below is for illustration purpose only.

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 'craft' with login details. The left sidebar shows a tree view with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links', and 'TSAPI Properties'. The main content area is titled 'TSAPI Links' and displays a table with one link:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	TR18300	1	5	Both

Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to Application Enablement Services, and may be set to any available number. For the **Switch Connection** field, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **TR18300** is selected. For the **Switch CTI Link Number** field, select the CTI link number configured in **Section 5.2**. For the **Security** field, select **Both**. Retain the default values in the remaining fields, and click **Apply Changes**. Note that the TSAPI link used for this test is Link 1 and is already configured. The screen below is for illustration purpose only.

The screenshot shows the 'Add TSAPI Links' screen in the Avaya Application Enablement Services Management Console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains the following fields:

- Link: 2
- Switch Connection: TR18300
- Switch CTI Link Number: 1
- ASAI Link Version: 4
- Security: Both

At the bottom are buttons for 'Apply Changes' and 'Cancel Changes'.

7.4. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows two Tlink names which were automatically generated when the TSAPI link was added in **Section 7.3**. Locate the Tlink name associated with **CSTA-S**. Make a note of the Tlink name, to be used later for configuring the CTI Connector for the Utry sample application.

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 "craft" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar shows a tree view with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. Under Security, the "Security Database" is expanded, showing sub-items like Control, CTI Users, Devices, Device Groups, and Tlinks. The main content area, titled "Tlinks", lists two entries: "AVAYA#TR18300#CSTA#AES6_TR1" (selected with a radio button) and "AVAYA#TR18300#CSTA-S#AES6_TR1". A "Delete Tlink" button is visible below the list.

7.5. Restart TSAPI Service

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

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 "craft" with login details. A red navigation bar contains "Maintenance | Service Controller" and links for "Home | Help | Logout".

The left sidebar shows a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (selected), Server Data, Networking, Security, Status, and User Management.

The main content area, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

Below the table, a note states: "For status on actual services, please use [Status and Control](#)". At the bottom, there are six buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

7.6. Administer User for TSAPI

Click **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 to allow the Utry sample application to access call related information. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown).

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: 'Welcome: User craft. Last login: Thu Jan 31 17:27:22 2013 from 10.64.10.51. HostName/IP: aes6_tr1/10.64.10.21. Server Offer Type: VIRTUAL_APPLIANCE. SW Version: r6-1-1-30-0'. Below the header is a red navigation bar with 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. The left sidebar contains a tree view with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under User Admin, 'Add User' is selected. The main content area shows the 'Add User' form with fields for User Id, Common Name, Surname, User Password, Confirm Password, Admin Note, Avaya Role (set to None), Business Category, Car License, CM Home, Cms Home, CT User (set to Yes), Department Number, Display Name, and Employee Number. A note states 'Fields marked with * can not be empty.'.

Add User	
Fields marked with * can not be empty.	
* User Id	<input type="text" value="utry"/>
* Common Name	<input type="text" value="utry"/>
* Surname	<input type="text" value="utry"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Cms Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>

7.7. Change User Access Permission

Click **Security** → **Security Databases** → **CTI Users** → **List All Users** from the left pane to display the **CTI Users** screen. Select the user configured in **Section 7.6** and click **Edit**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Security Database' > 'CTI Users' > 'List All Users'. The main area displays a table of CTI Users. The user 'utry' is selected.

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> acqueon	acqueon	NONE	NONE
<input type="radio"/> calabrio	Calabrio	NONE	NONE
<input type="radio"/> devconn	Developer	NONE	NONE
<input type="radio"/> DevConnect	DevConnect	NONE	NONE
<input type="radio"/> interop	interop	NONE	NONE
<input type="radio"/> qfiniti	Autonomy	NONE	NONE
<input type="radio"/> rtitele1	rtitele1	NONE	NONE
<input checked="" type="radio"/> utry	utry	NONE	NONE
<input type="radio"/> vhtaes	vhtaes	NONE	NONE

Buttons: [Edit] [List All]

Check the **Unrestricted Access** checkbox in the **User Profile** section. Click **Apply Changes**.

The screenshot shows the 'Edit CTI User' form for the user 'utry'. The 'Unrestricted Access' checkbox is checked. The 'Apply Changes' button is highlighted.

User Profile:	
User ID	utry
Common Name	utry
Worktop Name	NONE
Unrestricted Access	<input checked="" type="checkbox"/>

Call and Device Control:	
Call Origination/Termination and Device Status	None

Call and Device Monitoring:	
Device Monitoring	None
Calls On A Device Monitoring	None
Call Monitoring	<input type="checkbox"/>

Routing Control:	
Allow Routing on Listed Devices	None

Buttons: [Apply Changes] [Cancel Changes]

8. Configure Tomcat Application Server

This section describes the configuration required on the Tomcat Application Server for running the Utry sample application. It is assumed that Apache Tomcat has already been installed, run-time support files and FTP script files for the Utry sample application have been copied into the Tomcat server, and three .war files (runtimeconfig, cticonnector, and Proj_yuanchuan) have been deployed to the Tomcat server environment. The run-time support files are required in order to support the Dialog Designer application to run (for this compliance test environment, the run-time support files were in runtimeSupportTomcat6.zip and were copied to the /opt/apache-tomcat-6.0.35/lib directory on the Tomcat Application Server). In this section the following configuration steps on the Tomcat Application Server are covered:

- Assign and Verify Dialog Designer License
- Configure CTI Connector
- Configure FTP Parameters
- Schedule FTP Jobs
- Restart Tomcat

8.1. Assign and Verify Dialog Designer License

The Utry sample application is a Dialog Designer application. A valid Dialog Designer license is required to run Dialog Designer applications with Voice Portal. This section shows how to assign a Dialog Designer license to the run time configuration for the Utry sample application. It is assumed that a Dialog Designer license has been created ahead of time and is stored on a WebLM license server.

From a web browser, enter **http://<ip-address>:8080** where <ip-addr> is the IP address of the Tomcat Application Server. The Apache Tomcat main page is displayed (not shown). Click **Tomcat Manager** under **Administration** in the left pane to display the **Tomcat Web Application Manager** page. The three .war files deployed for this compliance test are highlighted with red circles.



Tomcat Web Application Manager

Message: OK

Manager
[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Applications				
Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/AvayaVVR		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/MultilingualHelloWorld		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/OutboundCall		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/Proj_yuanchuan		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/SpeakVar		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/UserDefinedVXML		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/UserDefinedVXML2		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/cticonnector	CTIConnector War	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/eCI_CTI_DD1		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/eCI_CTI_DD2		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/eCI_DD1		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/eCI_DD2		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/runtimeconfig		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Click **/runtimeconfig** item in the **Path** column to bring up the Dialog Designer login page.



The image shows a login page for Avaya Dialog Designer. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Dialog Designer 05.01.11". The main area is white and contains two input fields: "Username:" and "Password:". Below these fields is a "Login" button. At the bottom, there is a copyright notice: "© 2010 Avaya Inc. All Rights Reserved."

Enter **ddadmin** as the username and relevant password to log in. The following page is displayed.



The image shows the "Dialog Designer Application Server Configuration" page. The top header includes the Avaya logo and the text "Welcome, ddadmin" and "Last logged in Tue Jan 29 13:19:44 MST 2013". Below this, a red banner displays "Dialog Designer 05.01.11" and a "Logoff" button. The main content area is divided into a left sidebar with a menu (License Server, Proxy Settings, Certificates, CTI, IR Channel Map, IC Common, IC VOX, IC VRUSM/HTTPVOX, Users) and a main panel. The main panel has a breadcrumb "You are here: Home" and a title "Dialog Designer Application Server Configuration Version 05.01.11". It contains a description of the application and a "Legal Notice" section. The "Legal Notice" section includes a copyright notice "© 2005 - 2010 Avaya Inc. All Rights Reserved.", a "Notice" paragraph, and a "Documentation disclaimer" paragraph. At the bottom, it shows "Last Login: Tue Jan 29 13:19:44 MST 2013".

Click **License Server** in the left pane. The **License Server** page is displayed. Enter the URL to the license server where the Dialog Designer license is stored. In this compliance test, the license server on Voice Portal was used. Click **Update**. Verify that both the **Runtime enabled** and **CTI enabled** fields show **true**. If not, contact an authorized Avaya sales representative to add the necessary capabilities.

The screenshot shows the Avaya Dialog Designer web interface. At the top, the Avaya logo is on the left, and the user 'ddadmin' is logged in on the right. Below the header, a red navigation bar contains 'Dialog Designer 05.01.11' and a 'Logoff' button. A left-hand menu lists various configuration options, with 'License Server' selected. The main content area is titled 'Licensing Server' and includes a breadcrumb trail 'You are here: Home > License Server'. It contains a text box for the 'License URL' with the value 'https://10.64.10.31:8443/WebLM/LicenseServer' and a 'Verify' button. Below this, three status fields are shown: 'Runtime enabled : true', 'CTI enabled : true', and 'IC enabled : true'. An 'Update' button is located at the bottom of the configuration section.

AVAYA

Welcome, ddadmin
Last logged in Tue Jan 29 13:19:44 MST 2013

Dialog Designer 05.01.11 Logoff

You are here: [Home](#) > License Server

Licensing Server

Enter the URL to the license server host. For example [http://myhost:8080/](#) . If you leave the license URL blank, the license server the VPMS uses will be used for Dialog Designer licensing (Voice Portal only).

License URL: **Verify**

Runtime enabled : true
CTI enabled : true
IC enabled : true

Update

8.2. Configure CTI Connector

The Utry sample application uses a CTI Collector provided by Dialog Designer to collect Call ID, Caller ID, and Callee ID information for calls arriving at the application. The CTI Collector acts as a JTAPI client to access such information from Application Enablement Services.

To configure the CTI Collector, click **CTI** on the left pane. The **CTI** page is displayed. Enter the following values:

- **Name:** a descriptive name for the CTI collector
- **Service Name:** the secure tlink noted in **Section 7.4**
- **User Name:** the user configured in **Section 7.6**
- **Password:** password of the above user
- **Confirm Password:** repeat the password

Click **Add TServer/AES**.

AVAYA Welcome, ddadmin
Last logged in Tue Jan 29 14:03:19 MST 2013

Dialog Designer 05.01.11 Logoff

You are here: [Home](#) > CTI

CTI

Timeout: Time in ms to wait for TServer/AES to obtain the call. Do not end the input with 'ms'.

Trace Verbosity: Amount of debug output: 0-off - 3 full.

Update

Type	Name	Service Name	User Name	Ext Map	Add Failover
Delete					

Note: The tserver/AES and failover names cannot contain '*'. Server name must be unique: i.e. tserver/AES names cannot be duplicated. Failover within a tserver cannot be duplicated. Failover name cannot be the same as tserver/AES.

Name: A unique name to identify this entry. The tserver and failover names cannot contain '*'.

Service Name: Identifies the service provider in the format: vendor#switch#type#server.

User Name: Username to connect to this tserver/AES.

Password: Unencrypted password to connect to this tserver/AES.

Confirm Password: Confirm password must match password.

Add TServer/AES

Note: You will need to restart the CTI Connector for changes to take affect. You will also need to modify tsapi.pro that is included with your runtimesupport files before connecting to a TServer/AES. Please read Dialog Designer documentation for correct location to place this file.

The screen shows the added entry in the CTI Collector table. Click the **map** link in the newly added entry.

Welcome, ddadmin
Last logged in Tue Jan 29 14:03:19 MST 2013

Dialog Designer 05.01.11
Logoff

License Server
Proxy Settings
Certificates
CTI
IR Channel Map
IC Common
IC VOX
IC VRUSM/HTTPVOX
Users

You are here: [Home](#) > CTI

CTI

Timeout: Time in ms to wait for TServer/AES to obtain the call.
Do not end the input with 'ms'.

Trace Verbosity: Amount of debug output: 0-off - 3 full.

Update

<input type="checkbox"/>	Type	Name	Service Name	User Name	Ext Map	Add Failover
<input type="checkbox"/>	tserver/AES	CM_10_67	AVAYA#TR18300#CSTA-S#AES6_TR1	utry	map	add failover

Delete

Note: The tserver/AES and failover names cannot contain '*'. Server name must be unique: i.e. tserver/AES names cannot be duplicated. Failover within a tserver cannot be duplicated. Failover name cannot be the same as tserver/AES.

Name: A unique name to identify this entry.
The tserver and failover names cannot contain '*'.

Service Name: Identifies the service provider in the format:
vendor#switch#type#server.

User Name: Username to connect to this tserver/AES.

Password: Unencrypted password to connect to this tserver/AES.

Confirm Password: Confirm password must match password.

Add TServer/AES

Note: You will need to restart the CTI Connector for changes to take affect
You will also need to modify tsapi.pro that is included with your runtimesupport files before connecting to a TServer/AES. Please read Dialog Designer documentation for correct location to place this file.

The **Tserver Extension Map** page is displayed. Enter an arbitrary number in the **Channel** field and a station extension configured in **Section 5.1** in the **Mapped Extension** field. Click **Add**. Repeat the steps for all the extensions configured in **Section 5.1**.

You are here: [Home](#) > [CTI](#) > Tserver Extension Map

Tserver Extension Map

Extension Map for Tserver : **CM_10_67**

Channel	Mapped Extension	Observe On Startup
<div> Delete </div>		

You can map a range of sequential channels to sequential extensions using the format "1-n" in the Channel field. You need only to enter the start extension in the Mapped Extension field.

Channel: Channel call will arrive on for IR. For VP, this value is arbitrary but should be unique to the list.

Mapped Extension: extension channel maps to for IR. For VP, this is the extension the call will arrive on.

Observe On Startup: ☒ always true.

Add

Make the following changes to the **tsapi.pro** file in the Tomcat server (for the compliance test the path to the file is /opt/apache-tomcat-6.0.35/lib):

- Replace the IP address with **10.64.10.21** which is the IP address of the Application Enablement Services server
- Add the **trustStoreLocation** and **trustStorePassword** parameters for supporting the use of secure link.

```
#Sun Nov 06 00:33:04 EST 2005
debugLevel=0
10.64.10.21=450
altTraceFile=tsapi_trace.txt
trustStoreLocation=/opt/apache-tomcat-6.0.35/webapps/cticonnector/WEB-INF/lib/avayaaprca.jks
trustStorePassword=password
```

8.3. Configure FTP Parameters

On the Tomcat Application Server, change directory to **/opt/TVRLOG**. Update the **ip**, **username**, **password**, and **rootPath** fields in the **ftpInfo.properties** file, where **ip** is the IP Address of the Utry server, **username** and **password** are for accessing the FTP server component on the Utry server, and **rootPath** is a local directory on the Tomcat Application Server for storing the files to be transferred.

```
ip=10.64.101.53
port=21
username=
password=
rootPath=/opt/Vox
```


8.4. Schedule FTP Jobs

The FTP jobs are initiated using two shell scripts: **MoveFile.sh** and **FtpClient.sh**. They are located in **/opt/IVRLOG**. They modify data files from the previous day to the format expected by IVR Optimization Analysis System and perform file transfer. Cron jobs should be scheduled once a day to run the two scripts with **MoveFile.sh** running first and **FtpClient.sh** running the next. Information regarding cron jobs are outside of the scope of this document.

8.5. Restart Tomcat

Once the above configuration steps are done, stop and start the Tomcat service by running the **shutdown.sh** and **startup.sh** scripts as follows:

```
cd /opt/apache-tomcat-6.0.35/bin
./shutdown.sh
./startup.sh
```


9. Configure Utry IVR Optimization Analysis System

This section focuses on the configuration of IVR Optimization Analysis System for receiving data files from the Tomcat Application Server and importing the data. It is assumed that the IVR Optimization Analysis System has already been installed. The following procedures are covered:

- Configure FTP Server
- Configure Import Time

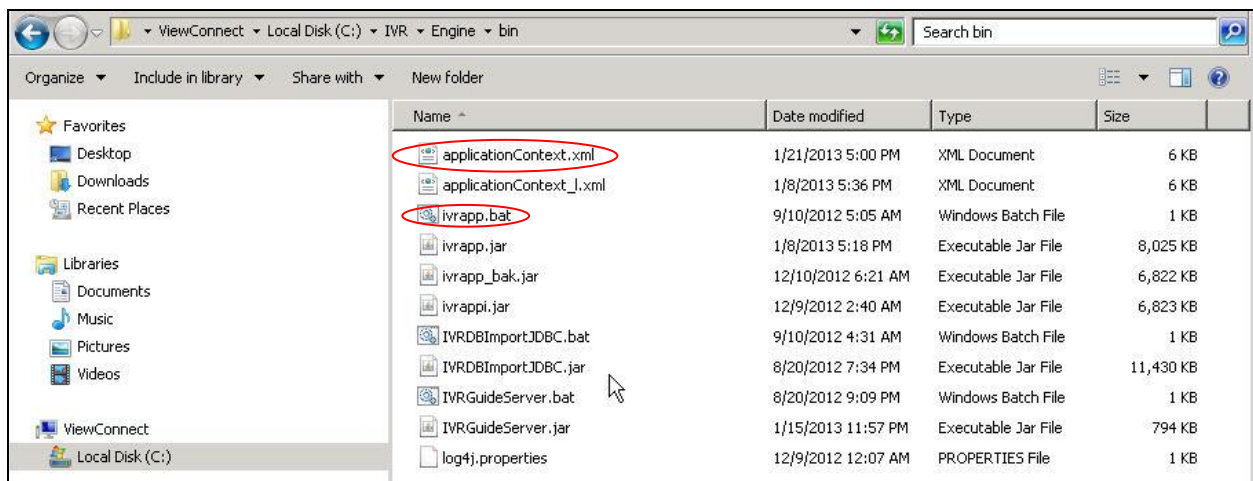
9.1. Configure FTP Server

IVR Optimization Analysis System is bundled with an FTP server. The FTP server is configured to receive data files from the Tomcat Application Server. The data files contain IVR application navigation data which will later be imported to and analyzed by IVR Optimization Analysis System.

During the FTP server configuration, proper user name, password, root location, and access permission were specified.

9.2. Configure Import Time

Once the data files are transferred over to IVR Optimization Analysis System, the system has a scheduled service to import and analyze the data. To configure the schedule, navigate to **C:/IVR/Engine/bin**. A list of files is displayed.



Right click the **applicationContext.xml** file and select **Edit**. Change the line with time specification to the desirable time. For example, “**00 00 02 ? * ***” is for 2AM everyday of the year. Save the change and exit.

```
<!-- 定义触发时间: 秒 分 小时 日期 月份 星期 年 -->
<bean id="doTime"
class="org.springframework.scheduling.quartz.CronTriggerBean">
    <property name="jobDetail"><ref bean="jobtask"/></property>
    <property name="cronExpression">
        <value>00 00 02 ? * *</value>
    </property>
```



```
</bean>
<!-- 总管理类 如果将lazy-init='false'那么容器启动就会执行调度程序 -->
<bean id="startQuertz" lazy-init="false" autowire="no"
class="org.springframework.scheduling.quartz.SchedulerFactoryBean">
    <property name="triggers"><list><ref bean="doTime"/></list></property>
</bean>
</beans>
```

In the same folder, look for the **ivrapp.bat** file. This file is invoked every time when IVR Optimization Analysis System is restarted. The execution of this file causes some DOS commands to be executed in a DOS command window (not shown). After the schedule described above is made, close the existing DOS command window and double click the **ivrapp.bat** file to run it so the time change will take effect.

10. Verification Steps

This section provides the steps to verify that Voice Portal can invoke the Utry sample application, application tree navigation data is collected and transferred to IVR Optimization Analysis System, and the IVR Optimization Analysis System's displays match the customer input.

10.1. Verify Voice Portal

From the VPMS web interface, click **System Management** → **MPP Manager** in the left pane. The **MPP Manager** page is displayed. Verify that the MPP server is **Online** and **Running**.

AVAYA Welcome, admin
Last logged in 1/28/13 at 4:41:54 PM EST

Voice Portal 5.1 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (1/31/13 4:04:02 PM EST)

[Refresh](#)

This page displays the current state of each MPP in the Voice Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: 1/31/13 4:03:53 PM EST

<input type="checkbox"/>	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input type="checkbox"/>	mpp1	Online	Running	OK	No	No	None	0	0

State Commands

[Start](#) [Stop](#) [Restart](#) [Reboot](#) [Halt](#) [Cancel](#)

Mode Commands

[Offline](#) [Test](#) [Online](#)

Restart/Reboot Options

☐ One server at a time
☒ All selected servers at the same time

[Help](#)

From the VPMS web interface, click **Real-Time Monitoring → Port Distribution** in the left pane. The **Port Distribution** page is displayed. Verify that the H.323 VoIP Connections ports configured in **Section 6.1** are in **In service** state.

Welcome, admin
Last logged in 1/28/13 at 4:41:54 PM EST

Voice Portal 5.1 (VoicePortal)
Home Help Logoff

Expand All Collapse All

▼ **User Management**
Roles
Users
Login Options

▼ **Real-Time Monitoring**
System Monitor
Active Calls
Port Distribution

▼ **System Maintenance**
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

▼ **System Management**
MPP Manager
Software Upgrade
System Backup

▼ **System Configuration**
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

▼ **Security**
Certificates
Licensing

▼ **Reports**
Standard
Custom
Scheduled

You are here: [Home](#) > Real-Time Monitoring > Port Distribution

Port Distribution (1/31/13 4:08:13 PM EST)

Refresh

This page displays information about how the telephony resources have been distributed to the MPPs. You configure the telephony resources on the VoIP Connections page.

Total Ports: 12Last Poll: 1/31/13 4:08:13 PM EST

Port	Mode	State	Port Group	Protocol	Current Allocation	Base Allocation
25508	Online	In service	utry	H323	mpp1	
25509	Online	In service	utry	H323	mpp1	
1	Online	In service	SM_10_62	SIP_Trunk	mpp1	
2	Online	In service	SM_10_62	SIP_Trunk	mpp1	
3	Online	In service	SM_10_62	SIP_Trunk	mpp1	
4	Online	In service	SM_10_62	SIP_Trunk	mpp1	
5	Online	In service	SM_10_62	SIP_Trunk	mpp1	
6	Online	In service	SM_10_62	SIP_Trunk	mpp1	
7	Online	In service	SM_10_62	SIP_Trunk	mpp1	
8	Online	In service	SM_10_62	SIP_Trunk	mpp1	
9	Online	In service	SM_10_62	SIP_Trunk	mpp1	
10	Online	In service	SM_10_62	SIP_Trunk	mpp1	

Help

From the VPMS web interface, click **System Configuration** → **Applications** in the left pane to display the **Applications** page (not shown). Click the Utry sample application link on the page. The **Change Application** page is displayed. Click the **Verify** button next to the **VoiceXML URL** field.

AVAYA Welcome, admin
Last logged in today at 8:03:09 PM EST

Voice Portal 5.1 (VoicePortal) Home ? Help Logoff

Expand All | Collapse All

▼ User Management
Roles
Users
Login Options

▼ Real-Time Monitoring
System Monitor
Active Calls
Port Distribution

▼ System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

▼ System Management
MPP Manager
Software Upgrade
System Backup

▼ System Configuration
Alarm Codes
Alarm/Log Options
Applications
MPP Servers
Report Data
SNMP
Speech Servers
VoIP Connections
VPMS Servers

▼ Security
Certificates
Licensing

▼ Reports
Standard
Custom
Scheduled

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of a VoiceXML or CCXML application.

Name: utry
Enable: ☒ Yes ☐ No
Type:

URL
☒ Single ☐ Fail Over ☐ Load Balance
VoiceXML URL: **Verify**


Mutual Certificate Authentication: ☐ Yes ☒ No
Basic Authentication: ☐ Yes ☒ No

Speech Servers
ASR: TTS:

Application Launch
☒ Inbound ☐ Inbound Default ☐ Outbound
☒ Number ☐ Number Range ☐ URI
Called Number: **Add**

Remove

Verify that the following page is displayed as an indication that the application can be accessed.



Event :error -

Handler : connection.disconnect [servlet_end](#)

Starting application : Proj_yuanchuan

Application Startup Parameters

AAI	<input type="text"/>
ANI	<input type="text"/>
DNIS	<input type="text"/>
Protocol Name	<input type="text"/>
Protocol Version	<input type="text"/>
UUI	<input type="text"/>
Call Tag	<input type="text"/>
Channel	<input type="text"/>
VP-Called Extension	<input type="text"/>
VP-Coverage Reason	<input type="text"/>
VP-Coverage Type	<input type="text"/>
VP-RDNIS	<input type="text"/>
Redirect URI	<input type="text"/>
Redirect Presentation Info	<input type="text"/>
Redirect Screening Info	<input type="text"/>
Redirect Reason	<input type="text"/>
Shared Mode	<input type="text"/>
Shared UUI ID	<input type="text"/>
Shared UUI Value	<input type="text"/>
Session Label	<input type="text"/>
SIPCallID	<input type="text"/>
Media Type	<input type="text"/>

Please note that the **Event** and **Handler** lines at the top do not affect the functions of the Utry sample application and can be ignored.

10.2. Verify IVR Optimization Analysis System

On the Utry server, enter <http://localhost:8080/ivr/main.jsp> in the URL field of an Internet Explore 8 web browser. The home page of IVR Optimization Analysis System is displayed.

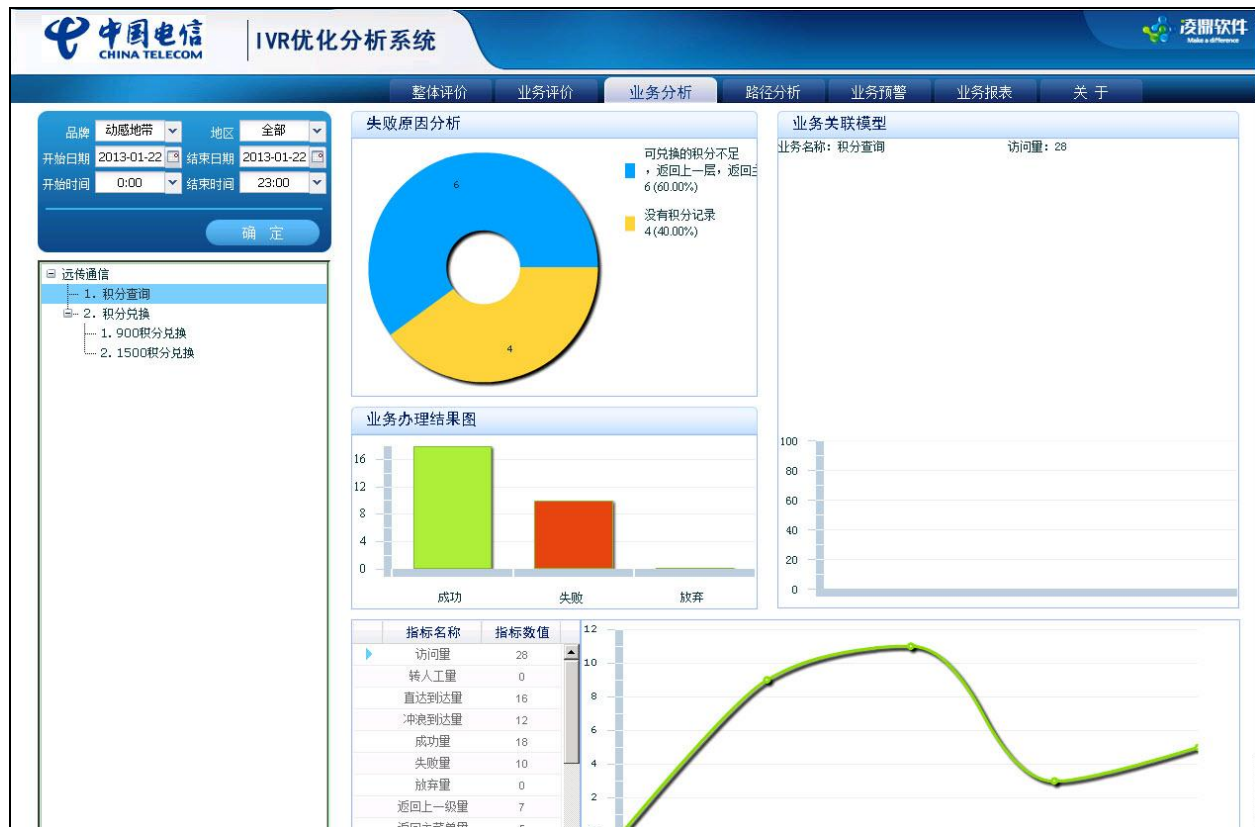
Click the **整体评价 (Overall Evaluation)** tab. Enter the start date, start time, end date, and end time in the upper left box and click **确定 (Confirm)**. The data for the specified interval is displayed. Verify that the data match the calls and key sequences made during that interval.



Click the **业务评价 (Business Evaluation)** tab. The following screen is displayed. Verify that the data match the calls and key sequences made during that interval.



Click the **业务分析 (Business Analysis)** tab. The following screen is displayed. Verify that the data match the calls and key sequences made during that interval.



11. Conclusion

These Application Notes describe the configuration steps required to integrate the Utry IVR Optimization Analysis System application with Avaya Voice Portal. All feature and serviceability test cases were completed successfully with the exception of one observation described in **Section 2.2**.

12. Additional References

This section references the product documentation that is relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.2, Issue 7.0, July 2012, Document Number 03-300509, available at <http://support.avaya.com>.
- [2] *Administering Voice Portal*, January 2011, available at <http://support.avaya.com>.
- [3] *Avaya Dialog Designer Developer's Guide Release 5.1*, June 2010, available at <http://support.avaya.com>.
- [4] *Utry IVR VOICE PORT Installation & Configuration Manual*, August 12, 2012

©2013 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.