



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

---

# **Application Notes for Komutel Kontakt with Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services - Issue 1.0**

### **Abstract**

These Application Notes describe the steps required to integrate the Komutel Kontakt (Call Center Solution) with Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. Komutel Kontakt is a call queue and call center (ACD) management tool for managing virtual agents, generating statistics for the proper management of resources, and intelligently distributing calls. In the compliance test, Komutel Kontakt successfully registered with Session Manager via SIP, distributed calls to available agents in the appropriate queue, and transferred calls to agents. In addition, Kontakt used TSAPI link on Application Enablement Services to obtain status information of monitored stations on Avaya Aura® Communication Manager.

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 steps required to integrate the Komutel Kontakt with Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. Kontakt is a call queue and call center (ACD) management tool for managing virtual agents, generating statistics for the proper management of resources, and intelligently distributing calls. In the compliance test, Komutel Kontakt successfully registered with Avaya Aura® Session Manager via SIP, distributed calls to available agents in the appropriate queue, and transferred calls to agents. In addition, Kontakt used TSAPI to track agent status.

Komutel Kontakt consists of two components: BLF Configuration and DAK Configuration. BLF Agent Configuration is used to track the agent status and DAK is basically a SIP phone that is responsible for handling incoming calls and transferring calls.

Komutel Kloud is a virtual next-generation telecom solution available in a cloud-based mode. It provides stability, performance, and extensibility. Kloud is available in either self-hosted local mode or provider-hosted configurations.

## 2. General Test Approach and Test Results

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

Interoperability compliance testing covered the following features and functionality:

- Successful SIP registration of Kontakt with Session Manager.
- Calls routed from Kontakt to an available agent.
- Manually transferring calls in a queue by Kontakt to a specified agent who is local to Communication Manager or on the PSTN.
- Tracking agent states with TSAPI.
- Playing music on hold by Kontakt.
- Playing announcement to queued calls periodically by Kontakt.
- Tracking statistics such as abandoned calls and incoming/outgoing calls in the call log.
- Caller ID display on Kontakt.
- Proper system recovery after restart of the Kontakt server and loss of IP connectivity.

## 2.2. Test Results

All test cases passed with the following observations noted:

- If a user places a call that is answered by an available agent and then the PC with Komutel Kcloud installed is restarted, the agent's status will be set to Not Ready Kontakt PC.
- If a user places a call that is answered by an available agent, and then the agent's PC is restarted, after the agent logs in to Kontakt again the agent's status will be set to logged out. The user has to manually change to the proper status.

## 2.3. Support

For technical support on Kontakt, contact Komutel Support via phone, email, or website.

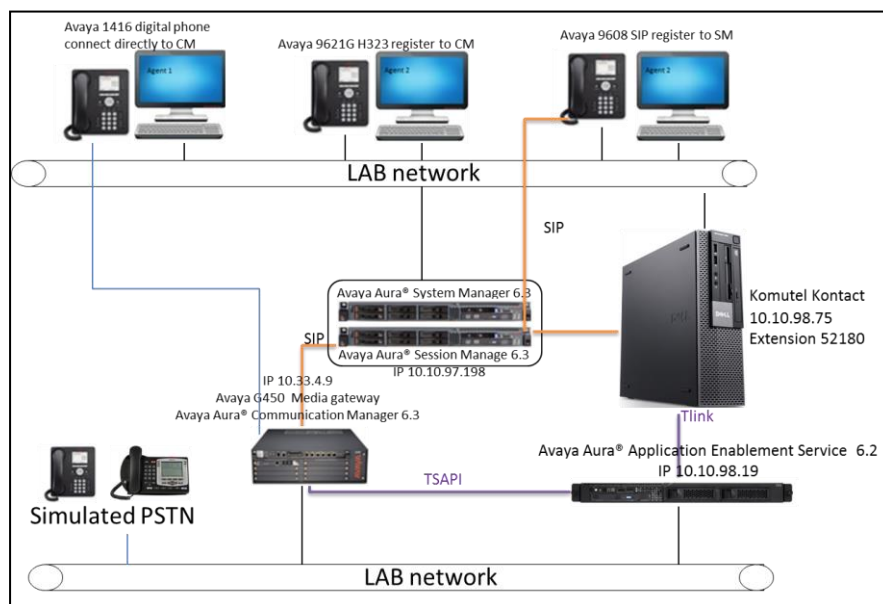
- **Phone:** (877) 225-9988
- **Email:** [service@komutel.com](mailto:service@komutel.com)
- **Web:** <http://www.gotoassist.com/ph/komutel>

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration with an Avaya SIP-based network that includes the following Avaya products:

- Communication Manager running on an Avaya S8300 Server with a G450 Media Gateway.
- Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones.
- System Manager used to configure Session Manager.
- Application Enablement Services used to monitor the availability of stations via a TSAPI link.

In addition, a Komutel Kontakt registered with Session Manager and was configured SIP user. The Komutel BLF Agent was also installed and configured to support the BLF feature on the console.



**Figure 1: Avaya SIP Network with Komutel Kontakt**

## 4. Equipment and Software Validated

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

Hardware Component	Version
Avaya S8300D Media Server with Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.3 SP3
Avaya Aura® System Manager running on S8800 Server	Avaya Aura® System Manager 6.3.4
Avaya Aura® Session Manager running on S8800 Server	Avaya Aura® Session Manager 6.3SP4
Avaya Aura® Application Enablement Services VM on Avaya S8800 Server	6.2
Avaya 9600 Series IP Telephones	6.2.3 (H.323) 6.2.2 (SIP)
Avaya Digital Telephones 1416	NA
Komutel Kloud	1.3.9.15677
Komutel BLF Agent	2.0.7.22990
Komutel DAK	2.0.0.11107

## 5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager license
- Administer CTI link between Communication Manager and Application Enablement Services for use with the BLF feature on the Contact

A SIP trunk is created between Communication Manager and Session Manager. It is assumed the general installation of Communication Manager on Avaya G450 Media Gateway and Session Manager has been previously completed such as ip-network-regions, SIP signaling groups, SIP trunk, etc.

The Communication Manager configuration was performed using Communication Manager System Access Terminal (SAT) interface. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

Please note that in the sample screenshots listed below the “display” command was used instead of the “change” or “add” commands, this is because all necessary changes were already in place when the screenshots were taken.

### 5.1. Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS), SIP Trunks, and the Computer Telephony Adjunct Links options are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                                Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                         Module ID (MID): 1

                                                USED
Platform Maximum Ports: 65000 170
Maximum Stations: 41000 77
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 36000 0
Maximum Off-PBX Telephones - OPS: 41000 6
Maximum Off-PBX Telephones - PBFMC: 36000 0
Maximum Off-PBX Telephones - PVFMC: 36000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0
(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** of the **system-parameters customer-options** form, verify that the number of SIP trunks supported by the system is sufficient.

display system-parameters customer-options	Page	2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	40
Maximum Concurrently Registered IP Stations:	18000	17
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	18000	0
Maximum Video Capable IP Softphones:	18000	0
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>30</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	1
Maximum Media Gateway VAL Sources:	250	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 3**, verify that the **Computer Telephony Adjunct Links** option is enabled.

display system-parameters customer-options	Page	3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	<b>Computer Telephony Adjunct Links? y</b>	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? n	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? n		
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

## 5.2. Configuring AE Services

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services.

Enter command **change ip-services**. Complete Page 1 of the **ip-services** form as follows:

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled**, enter **y**.
- In the **Local Node** field, type **procr**.
- In the **Local Port** field, accept the default (**8765**).

change ip-services			Page 1 of 3		
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

Complete Page 3 of the **ip-services** form as follows:

- In the **AE Services Server** field, type the name of the AES Server, for example: **DevAES62**.
- Enter **Password**, see example in screenshot below.
- Set the **Enabled** field to **y**.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	DevAES62	DevConnect123	y	in use		

## 5.3. Configure 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.

display cti-link 7		Page 1 of 3	
CTI LINK			
CTI Link: 2			
Extension: 52102			
Type: ADJ-IP			
COR: 1			
Name: DevAES62			

## 6. Configure Avaya Aura® Session Manager

It is assumed that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms. All the configuration items required as part of the initial Session Manager installation have already been defined. This includes items such as certain SIP domains, locations, SIP entities and Session Manager itself.

This section provides the procedures for configuring SIP User on Session Manager.

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

## 6.1. Add SIP Users

Add a SIP user for the Kontact and use the option to automatically generate the SIP stations on Communication Manager when adding a new SIP user for Session Manager.

To add new SIP users, expand **Users Management** and select **Manage Users** from left and select the **New** button (not shown) on the right. Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.
- **Login Name:** Enter *<extension>@<sip domain>* of the user (e.g., 52180@bvwddev.com).
- **Authentication Type:** Select *Basic*.
- **SMGR Login Password:** Enter the password which will be used to log into System Manager
- **Confirm Password:** Re-enter the password from above.
- **Shared Communication Profile Password:** Enter the password which will let the SIP phone log into Session Manager.
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information of a SIP user created for the compliance test:

The screenshot displays the 'User Profile Edit' interface for the user '52180@bvwddev.com'. The left sidebar shows the navigation menu with 'User Management' expanded and 'Manage Users' selected. The main content area has a breadcrumb trail 'Home / Users / User Management / Manage Users' and a 'Help' link. Below the breadcrumb, there are buttons for 'Commit & Continue', 'Commit', and 'Cancel'. The 'Identity' tab is active, showing fields for 'Last Name' (filled with 'Tam'), 'First Name' (filled with 'Muoi'), 'Middle Name' (empty), 'Description' (empty), 'Update Time' (displayed as 'October 23, 2013 4:33'), 'Login Name' (filled with '52180@bvwddev.com'), and 'Authentication Type' (set to 'Basic'). A red box highlights the 'Last Name' and 'First Name' fields.

Click on the **Communication Profile** tab, in the **Communication Profile** section, enter:

- **Communication Profile password:** Enter the password used to login SIP device.

Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** (not shown) and enter values for the following required:

- **Name:** Enter **Primary**.
- **Default:** Enter ☒

Click **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** select *Avaya SIP*.
- **Handle:** SIP extension.
- **Domain:** select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add** (not shown).

**User Profile Edit: 52180@bvwdev.com** Comm

Identity \*

**Communication Profile \***

Membership

Contacts

Communication Profile ▾


Communication Profile Password:  Edit

New

Delete

Done

Cancel

Name
 Primary

Select : None

\* Name:

Default : ☒

Communication Address ▾

New

Edit

Delete

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	52180	bvwdev.com

Select : All, None

In the **Session Manager Profile** section, specify the Session Manager entity for **Primary Session Manager** and assign the **Application Sequence** to the new SIP user. The same Application Sequence can be used for both the originating and terminating sequence. Set the **Home Location** field. Below is an example used during the compliance test:

☒ **Session Manager Profile** ▼

**SIP Registration**

\* **Primary Session Manager**

DevSM ▼

Primary	Secondary	Maximum
38	0	38

**Secondary Session Manager** (None) ▼

**Survivability Server** (None) ▼

**Max. Simultaneous Devices** 1 ▼

**Block New Registration When Maximum Registrations Active?** ☐

**Application Sequences**

**Origination Sequence** DevCM3\_Seq ▼

**Termination Sequence** DevCM3\_Seq ▼

**Call Routing Settings**

\* **Home Location** Belleville ▼

**Conference Factory Set** (None) ▼

In the **CM Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Profile Type:** Select **Endpoint**.
- **Extension:** Enter extension number of SIP user.
- **Set Type:** The value of this read only field depends on the selected template. In the example as shown below, the type is **9608SIP** (when this user was created, the template **9608SIP\_DEFAULT\_CM\_6\_3** was selected).

Leave other fields with default value. The screen below shows the information when adding a new SIP user to the sample configuration.

The screenshot shows the 'CM Endpoint Profile' configuration form. The form is titled 'CM Endpoint Profile' with a dropdown arrow. It contains several fields and checkboxes. The fields are: 'System' (dropdown menu with 'DevCM3\_62' selected), 'Profile Type' (dropdown menu with 'Endpoint' selected), 'Extension' (text input with '52180'), 'Template' (dropdown menu with 'Select/Reset' selected), 'Set Type' (text input with '9608SIP'), 'Security Code' (text input), 'Port' (text input with 'S00064'), 'Voice Mail Number' (text input), and 'Preferred Handle' (dropdown menu with '(None)' selected). There are three checkboxes: 'Use Existing Endpoints' (unchecked), 'Enhanced Callr-Info display for 1-line phones' (unchecked), and 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' (checked). There is also a checkbox for 'Override Endpoint Name' which is checked. A red box highlights the 'System', 'Profile Type', 'Extension', and 'Set Type' fields. A blue box highlights the 'Endpoint Editor' button next to the 'Extension' field.

CM Endpoint Profile

\* System DevCM3\_62

\* Profile Type Endpoint

Use Existing Endpoints ☐

\* Extension 52180 Endpoint Editor

Template Select/Reset

Set Type 9608SIP

Security Code

Port S00064

Voice Mail Number

Preferred Handle (None)

Enhanced Callr-Info display for 1-line phones ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User ☒

Override Endpoint Name ☒

Click the **Endpoint Editor** button beside **Extension** field (shown above) to modify endpoint details. In the **General Options** tab, make sure **Type of 3PCC Enable** is set to **Avaya**.

Done

Cancel

[ Save As Template]

System

DevCM3\_62

Extension

52180

Template

Select

Set Type

9608SIP

Port

S00064

Security Code

Name

Tam, Muoi

General Options (G) \*

Feature Options (F)

Site Data (S)

Abbreviated Call Dialing (A)

Enhanced Call Fwd (E)

Button Assignment (B)

Group Membership (M)

\* Class of Restriction (COR)

1

\* Emergency Location Ext

52180

\* Tenant Number

1

\* SIP Trunk

5

Coverage Path 1

Lock Message

☐

Multibyte Language

Not Applicable

\* Class Of Service (COS)

1

\* Message Lamp Ext.

52180

Type of 3PCC Enabled

Avaya

Coverage Path 2

Localized Display Name

Tam, Muoi

In the **Feature Options** tab, make sure **IP Softphone** option is checked (not shown). In the **Button Assignment** tab, maximize the allowed of **call-appr** are 10 lines (8 lines in **Button Assignment** tab:

General Options (G) \*

Feature Options (F)

Site Data (S)

Abbreviated Call Dialing (A)

Button Assignment (B)

Group Membership (M)

Main Buttons

Feature Buttons

Button Modules

1

call-appr

2

call-appr

3

call-appr

4

call-appr

5

call-appr

6

call-appr

7

call-appr

8

call-appr

Button assignment for **call-appr** continue if needed on the **Feature Buttons** tab:

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Button Assignment (B)		Group Membership (M)					
Main Buttons		Feature Buttons		Button Modules			
9	call-appr ▼						
10	call-appr ▼						
11	None ▼						

## 7. Configure Avaya Aura® Application Enablement Services

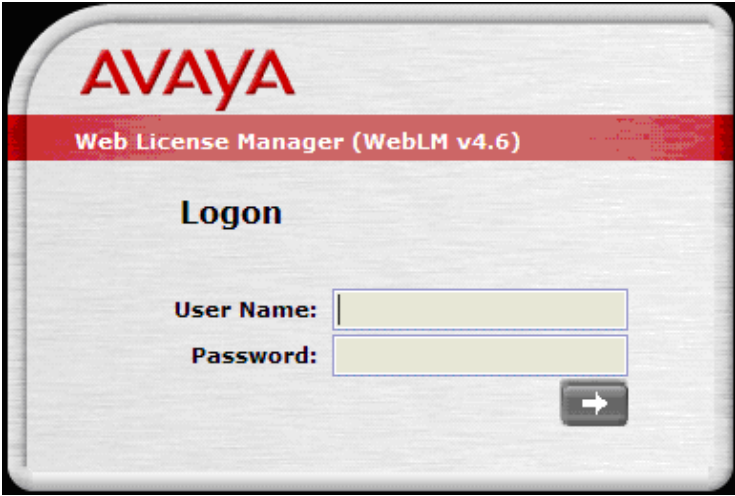
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

- Verify TSAPI license
- Launch OAM interface
- Administer TSAPI link
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer user for Komutel BLF Agent

### 7.1. Verify TSAPI License

Access the Web License Manager interface by using the URL “https://<ip-addr>/WebLM/” in an Internet browser window, where <ip-addr> is the IP address of the Application Enablement Services server.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.



The **Web License Manager** screen is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown below. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED MEDIUM SWITCH** for the Avaya S8800 Server.

Licensed products	License installed on: August 16, 2013 10:12:09 AM -04:00		
APPL_ENAB	License File Host IDs: CC-F9-54-AC-AA-0D		
Application_Enablement	Licensed Features		
View license capacity			
View peak usage			
COMMUNICATION_MANAGER			
Communication_Manager			
Uninstall license			
Server properties			
Manage users			
Portcuts			
Help for Installed Product			
	Feature (Keyword)	Expiration date	Acquired
	CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16
	Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000
	AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3
	CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16
	Product Notes (VALUE_NOTES)	permanent	Not counted
	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; IXP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; IXM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;		
	AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3
	TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000
	DLG (VALUE_AES_DLG)	permanent	16
	Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000
	AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3
	Acquired licenses		
	Feature	Acquired by	Count
	VALUE_AES_TSAPI_USERS	TSAPI (DevAES62)	2

## 7.2. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://<ip-addr>” in an Internet browser window, where <ip-addr> is the IP address of the Application Enablement Services server. Log in using the appropriate credentials. (not shown)

## 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**.

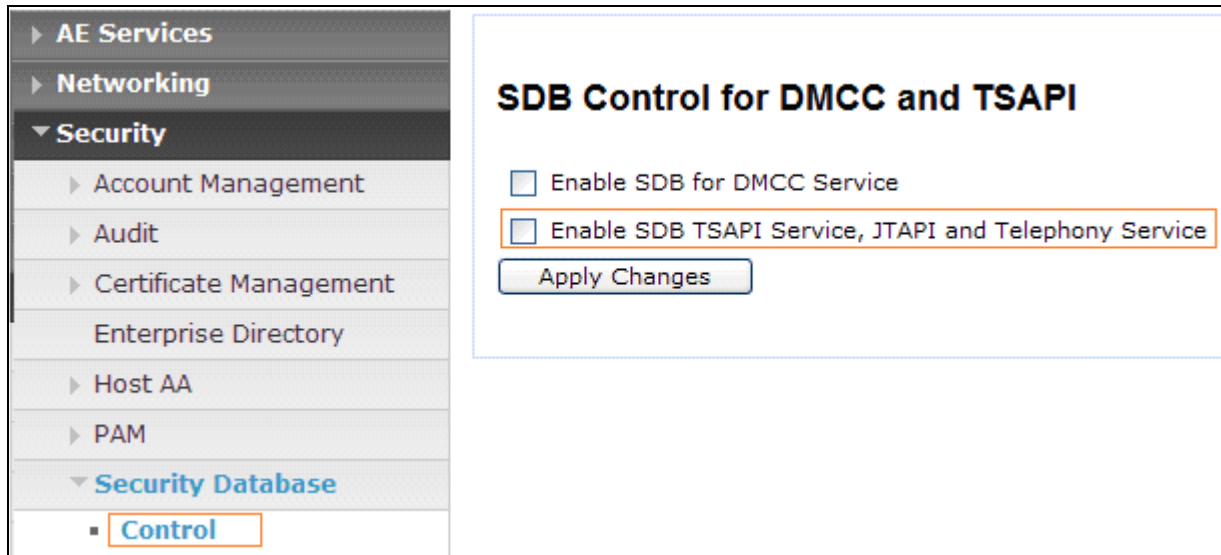
The screenshot shows the 'TSAPI Links' screen. On the left is a navigation pane with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', and 'TSAPI'. Under 'TSAPI', 'TSAPI Links' is selected. The main area is titled 'TSAPI Links' and contains a table with columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete 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 **DevCM63** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Retain the default values in the remaining fields and click **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' screen. On the left is the same navigation pane as before. The main area is titled 'Edit TSAPI Links' and contains form fields for 'Link', 'Switch Connection', 'Switch CTI Link Number', 'ASAI Link Version', and 'Security'. The 'Link' field contains the value '7'. The 'Switch Connection' dropdown is set to 'DevCM63'. The 'Switch CTI Link Number' dropdown is set to '7'. The 'ASAI Link Version' dropdown is set to '5'. The 'Security' dropdown is set to 'Unencrypted'. At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

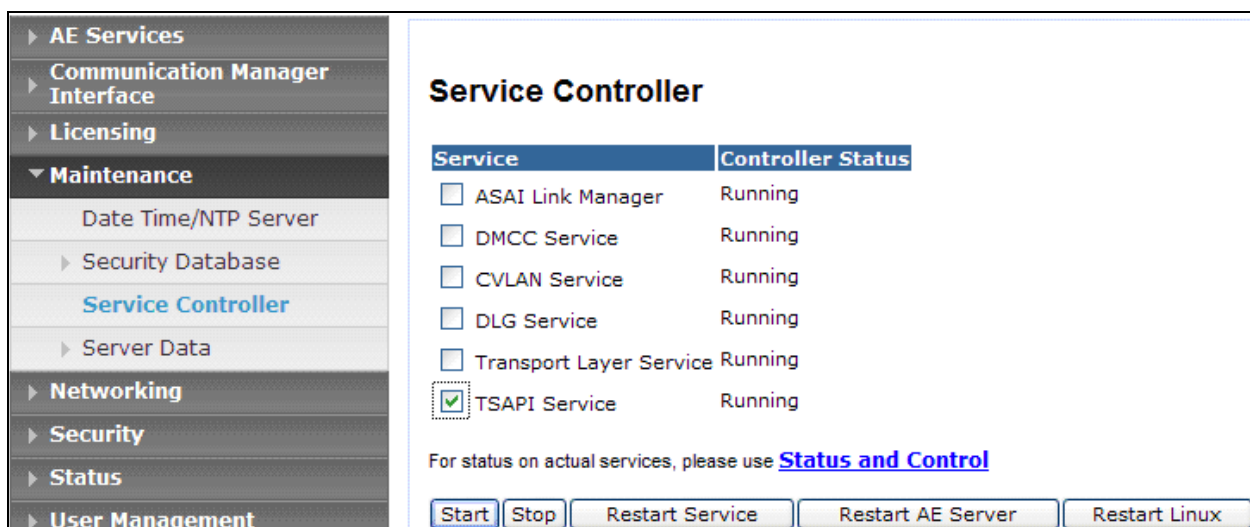
## 7.4. Disable Security Database

Select **Security**→**Security Database**→**Control** from the left pane to display the **SDB Control for DMCC and TSAPI** screen. Uncheck **Enable SDB TSAPI Service, JTAPI and Telephony Service** and click **Apply Changes**.



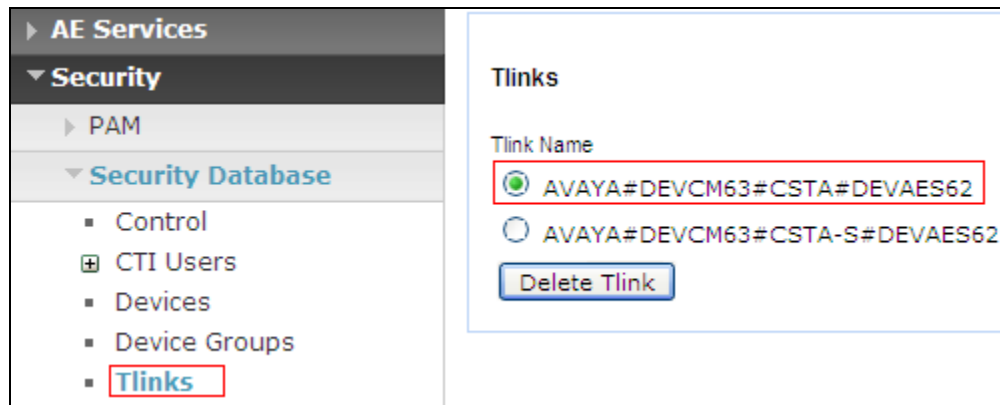
## 7.5. Restart TSAPI Service

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



## 7.6. Obtain Tlink Name

Select **Security**→**Security Database**→**Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, which will be used later for configuring the Komutel BLF Agent. See the screen below for an example of tlink name:



## 7.7. Administer User for Komutel Kontakt

Select **User Management**→**User Admin**→**Add User** from the left pane to display the **Add User** screen.

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. Click **Apply** at the bottom of the screen:

The screenshot displays the 'Edit User' interface. On the left, a navigation pane shows a tree structure under 'User Management', with 'User Admin' expanded and 'Add User' selected. The main content area is titled 'Edit User' and contains the following fields:

- \* User Id: komutel
- \* Common Name: Komutel
- \* Surname: SIT
- User Password: [masked]
- Confirm Password: [masked]
- Admin Note: [empty text box]
- Avaya Role: None (dropdown)
- Business Category: [empty text box]
- Car License: [empty text box]
- CM Home: [empty text box]
- Cms Home: [empty text box]
- CT User: Yes (dropdown)
- Department Number: [empty text box]
- Display Name: [empty text box]
- Telephone Number: [empty text box]

At the bottom of the form, there are two buttons: 'Apply Changes' (highlighted with a red box) and 'Cancel Changes'.

## 8. Configure Komutel Kontakt

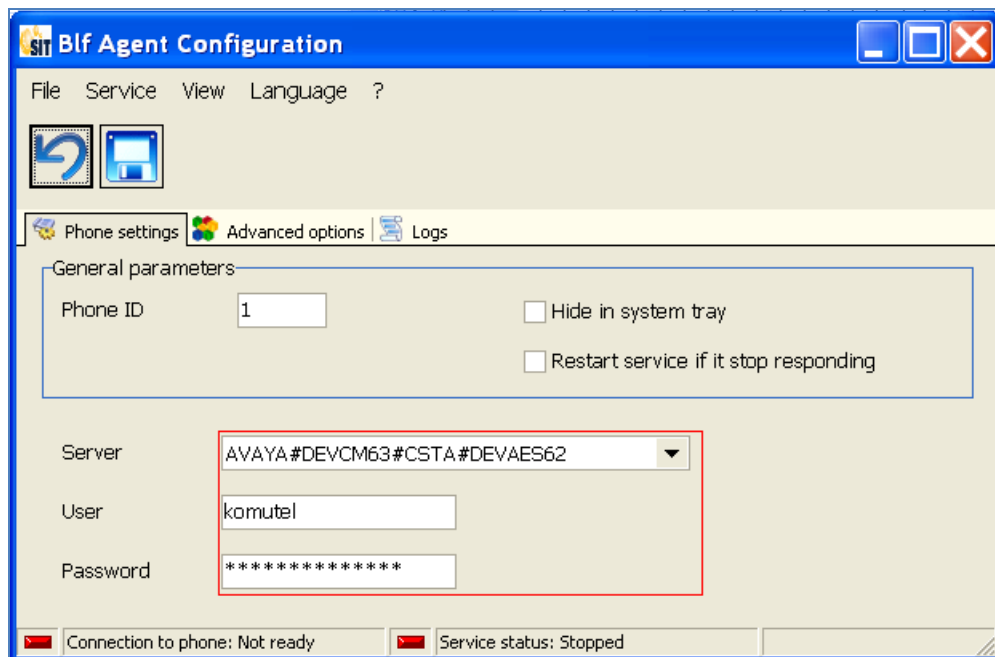
This section provides the procedures for configuring Komutel Kontakt. The procedures include the following areas:

- Configure Kontakt through **BLF Agent** and **DAK Configuration** applications
- Verify Phone System
- Configure Queues
- Configure Agents

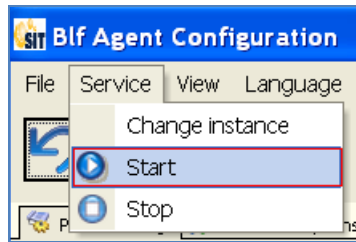
Komutel Kontakt consists of two components: BLF Agent Configuration and DAK Configuration. BLF Agent Configuration is used to track agent status and DAK is a SIP phone responsible for handling incoming calls and transferring calls.

### 8.1. Configure BLF Agent

The BLF Agent is used to track the line status of monitored stations on Communication Manager using a TSAPI link configured on Application Enablement Services. In the **BLF Agent Configuration** application, set the **Server** field to the Tlink name of the TSAPI link obtained in **Section 7.6**. The **Server** field should automatically discover the Tlink name. Set the **User** and **Password** fields according to the CT User configured in **Section 7.77.7**. Set the **Phone ID** field, which will group stations from a particular Communication Manager system. This Phone ID will be used for all users when configuring BLF buttons.



To start the BLF Agent service, select **Service→Start** from the menu of the **BLF Agent Configuration** application as shown below.



## 8.2. Configure DAK Configuration

Use the **DAK Configuration** application to configure the console's lines. In the **DAK configurations** tab, depending on the number of lines that are available, choose *Automatic Line* in the **Functions** column and enter the extension number in the **Description** column. As shown below, the console was configured with 24 line appearances with extension 52180.

DAK configurations
 Settings
 Debug

User: 
☒ Reset call number

	Enabled	Functions	Description	Display group	Overflow disp	Overflow nu	Use overflow only when
1	<input checked="" type="checkbox"/>	Automatic line	52180				Always
2	<input checked="" type="checkbox"/>	Automatic line	52180				Always
3	<input checked="" type="checkbox"/>	Automatic line	52180				Always
4	<input checked="" type="checkbox"/>	Automatic line	52180				Always
5	<input checked="" type="checkbox"/>	Automatic line	52180				Always
6	<input checked="" type="checkbox"/>	Automatic line	52180				Always
7	<input checked="" type="checkbox"/>	Automatic line	52180				Always
8	<input checked="" type="checkbox"/>	Automatic line	52180				Always
9	<input checked="" type="checkbox"/>	Automatic line	52180				Always
10	<input checked="" type="checkbox"/>	Automatic line	52180				Always
11	<input checked="" type="checkbox"/>	Automatic line	52180				Always
12	<input checked="" type="checkbox"/>	Automatic line	52180				Always
13	<input checked="" type="checkbox"/>	Automatic line	52180				Always
14	<input checked="" type="checkbox"/>	Automatic line	52180				Always
15	<input checked="" type="checkbox"/>	Automatic line	52180				Always
16	<input checked="" type="checkbox"/>	Automatic line	52180				Always
17	<input checked="" type="checkbox"/>	Automatic line	52180				Always
18	<input checked="" type="checkbox"/>	Automatic line	52180				Always
19	<input checked="" type="checkbox"/>	Automatic line	52180				Always
20	<input checked="" type="checkbox"/>	Automatic line	52180				Always
21	<input checked="" type="checkbox"/>	Automatic line	52180				Always
22	<input checked="" type="checkbox"/>	Automatic line	52180				Always
23	<input checked="" type="checkbox"/>	Automatic line	52180				Always
24	<input checked="" type="checkbox"/>	Automatic line	52180				Always

In the **Setting** tab, enter the following information:

In the **General parameter** section:

- **Delay after answer call (ms)**: select **500**.
- **Call distribution mode**: select **Direct transfer**.

In the **SIP phone connection** section, enter:

- A descriptive **Display name** (e.g., *52180*).
- The **Username** and **Password** used to register with Session Manager specified in **Section 6.1**.
- The **SIP Domain** (e.g., *bvwdev.com*).
- The **Proxy**, which specifies the IP address of the SIP interface of Session Manager.

In the **Audio devices** section, specify the audio device or headset that will be used with the console. And select **History-info** option for **Additional caller id information for incoming calls**. Click the **Save** button at the top of screen.

The screenshot shows the 'Settings' tab of the 'DAK configurations' window. The 'General parameters' section includes checkboxes for 'Hide in system tray' (checked) and 'Restart service if it stop responding' (unchecked). It also has input fields for 'Delay before answer call (ms)' (0), 'Delay after answer call (ms)' (500), 'Call distribution mode' (Direct transfer), and 'Cancel call after (ms)' (6000). The 'SIP phone connection' section includes fields for 'Display name' (52180), 'Display number (Nortel)' (empty), 'Username' (52180), 'Password' (\*\*\*\*), 'Domain' (bvwdev.com), 'Proxy' (10.10.97.198), 'Blf type' (Dialog), and 'Group name' (empty). The 'Audio devices' section includes dropdowns for 'Speaker', 'Microphone', and 'Ring', all set to 'VXI UC ProSet USB v1.0<'. The 'Additional caller id information for incoming calls' dropdown is set to 'History-info'. A note at the top right states 'Phone settings need a service restart to take effect'.

Section	Parameter	Value
General parameters	Hide in system tray	Checked
	Restart service if it stop responding	Unchecked
	Delay before answer call (ms)	0
	Delay after answer call (ms)	500
	Call distribution mode	Direct transfer
SIP phone connection	Display name	52180
	Display number (Nortel)	
	Username	52180
	Password	****
	Domain	bvwdev.com
	Proxy	10.10.97.198
	Blf type	Dialog
Audio devices	Speaker	VXI UC ProSet USB v1.0<
	Microphone	VXI UC ProSet USB v1.0<
	Ring	VXI UC ProSet USB v1.0<
Additional caller id information for incoming calls		History-info

### 8.3. Verify Kontakt Phone system

From a web browser access the page 127.0.0.0 with the appropriate login credentials. This will launch the Komutel Kloud admin web interface. Select the **Configuration** tab then click on the **Configurations** link. In the configuration page, select **Kontakt** → **Phone System**. It shows detail of SIP extension that was configured in **DAK** application.

The screenshot shows the 'Phone system' configuration page for 'SIP\_AVAYA\_CM - Komutel'. The 'Phone connection' section is highlighted with a red box. It contains the following fields:

- Save statistics as: KOMUTEL (dropdown)
- Username: 52180 (text input)
- Password: .... (password input)
- Domain: bvwdev.com (text input)
- DN: 52180 (text input, with a red 'X' icon)
- Max number of calls: 24 (spinner)
- DN configuration: (empty text input)
- 0 (spinner)

Click on **Recorded announcements** and **Music on hold** tab to manager the audio file for annoucement and music on hold so that music would be played while a caller is in queue with a message played periodically. This configuration is not shown in these Application Notes.

Select **Kontakt** → **General** to manager general information for Kontakt, below is the setup used for the compliance test:

The screenshot shows the 'General' configuration page for 'Kontakt'. The 'General' tab is selected. The following fields are visible:

- Default quick transfer number: (empty text input)
- Number of seconds to ring before changing agent status to Not Ready: 15 (spinner)
- Minimum number of seconds before marking call as Dropped: 5 (spinner)
- Recordings default number of days to display: 7 (spinner)
- Max number of days to display dropped calls: 2 (spinner)
- Number of minute after resetting call park state from abandoned to empty: 15 (spinner)
- Join on attendant answer: ☐
- Save button

## 8.4. Configure queues

Select **Kontakt** → **Queues**. This tab shows the current list of queues in the system. Click on the “+” plus sign to add new queue.

Users

General

Komand

Kontakt

Schedule Management

Server logs

Queues

General

Phone system

Recorded announcements

Music on hold

IVR Ports

Statistics

Call

Email

<

Here is the example of a queue named **pstn** used during compliance testing. When the caller with extension start with 54 dial 52180, Kontakt will route the call to an available agent logged into this queue or queue the call if there is no available agent.



**Edit queue - (PSTN)**

**General config** | Interactive voice response | Recorded announcements | Music on hold

**Queue informations**

Queue name: pstn

Queue type: Normal queue

**Rules to handle calls from phone display content**

Caller name: No rules

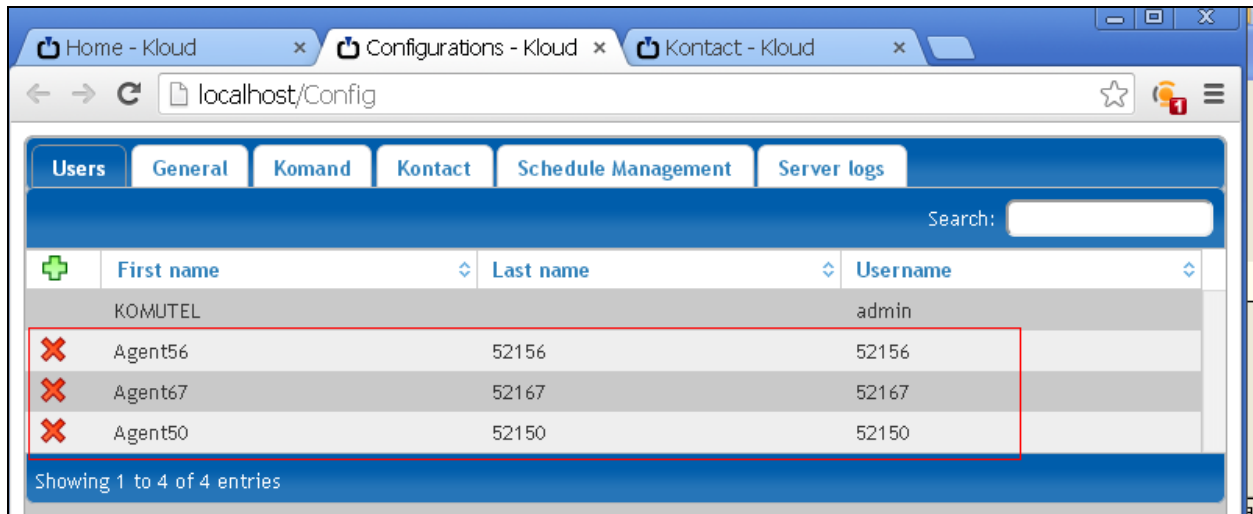
Caller id: 54\d\d\d

Forwarded from: No rules

## 8.5. Configure agents

Next, configure agent and its extension that will be monitored by the Komutel Kontakt. Repeat these steps for each agent and extension to be monitored.

In the **Configurations** page, select **User** tab. It shows the current list of agents in the system.



Click on the “+” plus sign to add new agent. The following screen shows the **User information** fields populated for an agent previously configured.

**Edit user - (Agent56 52156)**

Details | Phone | Komand | Permissions | Schedule Management | Kontakt

**User information**

Security level: [Dropdown]

First name: Agent56

Last name: 52156

Department: + [Dropdown]

Title: + [Dropdown]

Email: 52156@52156.com

Presence ID: 52156

Presence app. ID: 1

Language: English

Username: 52156

New password: [Masked]

New password confirmation: [Masked]

Select the **Phone** tab to add phone number for this agent:

	phone	extention	note	default
Phone 1	52156			<input type="radio"/>

In the **Kontakt** tab, assign queue to this agent, in the example below this **52156** agent is assigned to 3 available queues in the sytem:

**Assigned queues**

Check All / Uncheck All

- ☒ 67fwd
- ☒ General Queue
- ☒ pstn

Log into **Komutel Kloud**, then select the **Kontakt** link. In the **Queues** tab, all of the assigned queues will be displayed for the logged in agent. In this figure, the 3 queues **pstn**, **General** and **67fwd** are displayed, this 52156 agent is not ready, and all of the queues are in the **Not Ready** state as indicated by the Red circle by the queue name.

Agent56 52156 Ready / Not ready: Status

Queue: pstn

Transfer to: 52156

**Queues**

Queue	Qty.	Logged In	Ready
pstn	0	1	0
General Queue	0	1	0
67fwd	0	1	0

Click on the **Agent** tab, all of the configured agents that will be monitored are displayed as shown below. In order for an agent to become available to handle an incoming call, the agent's state must be set to *Ready*. In this example, all of the agents are in the *Not Ready* state and only 52156 is logged in.

Agent56  
52156

Ready / Not ready: Status

Queue: pstn

Not ready

Transfer to: 52156

Abd. calls: 0

Configuration

Manual transfer

Log Out

Queues Agents

Search:

Log.	Firstname	Lastname	Queue	Transfer to	TeL.	Display L1	Display L2	Ready / Not ready	Length
	KOMUTEL		pstn	5555				Logged out	00:06:36
	KOMUTEL		General Queue	5555				Logged out	00:06:36
	Agent56	52156	pstn	52156				Not ready	00:06:25
	Agent56	52156	General Queue	52156				Not ready	00:06:25
	Agent56	52156	67fwd	52156				Not ready	00:06:25
	Agent67	52167	pstn	52167				Logged out	68:02:23
	Agent67	52167	General Queue	52167				Logged out	68:02:23
	Agent67	52167	67fwd	52167				Logged out	68:02:23
	Agent50	52150	pstn	52150				Logged out	24:40:59
	Agent50	52150	General Queue	52150				Logged out	24:40:59
	Agent50	52150	67fwd	52150				Logged out	24:40:59

Showing 1 to 11 of 11 entries

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Komutel Kontakt with Communication Manager, Session Manager, and Application Enablement Services.

1. On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the configured CTI link.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
7	5	no	DevAES62	established	15	15

- On Application Enablement Services, verify the status of the TSAPI link by selecting **Status→Status and Control→TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is “Talking” for the TSAPI link.

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
7	DevCM63	7	Talking	Mon Mar 24 06:52:50 2014	Online	16	3	15	15	30

Online Offline

For service-wide information, choose one of the following:  
[TSAPI Service Status](#) [TLink Status](#) [User Status](#)

- Verify that the Kontact has successfully registered with Session Manager. The System Manager screen below shows the successful registration of Kontact SIP user.

Home / Elements / Session Manager / System Status / User Registrations

**User Registrations**

Select rows to send notifications to devices. Click on Details column for complete registration status.

View: Default Force Unregister AST Device Notifications: Reboot Reload Fallback As of 4:41 PM

38 Items Refresh Show 15 Filter: Enable

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered
Show	52180@bvvdev.com	Mot	Sau	---	10.98.75.5060			0/1		Prim Sec Surv
Hide	52180@bvvdev.com	Muoi	Tam	---	10.98.75.5060			1/1		(AC)

Users Registration Device Simultaneous History

Registration Address: 52180@bvvdev.com

IP Address: 10.98.75.5060

Actual Location: ---

Active Controller: DevSM

PPM Subscription Time (AC): ---

Event Subscriptions: ---

Instance Id: ---

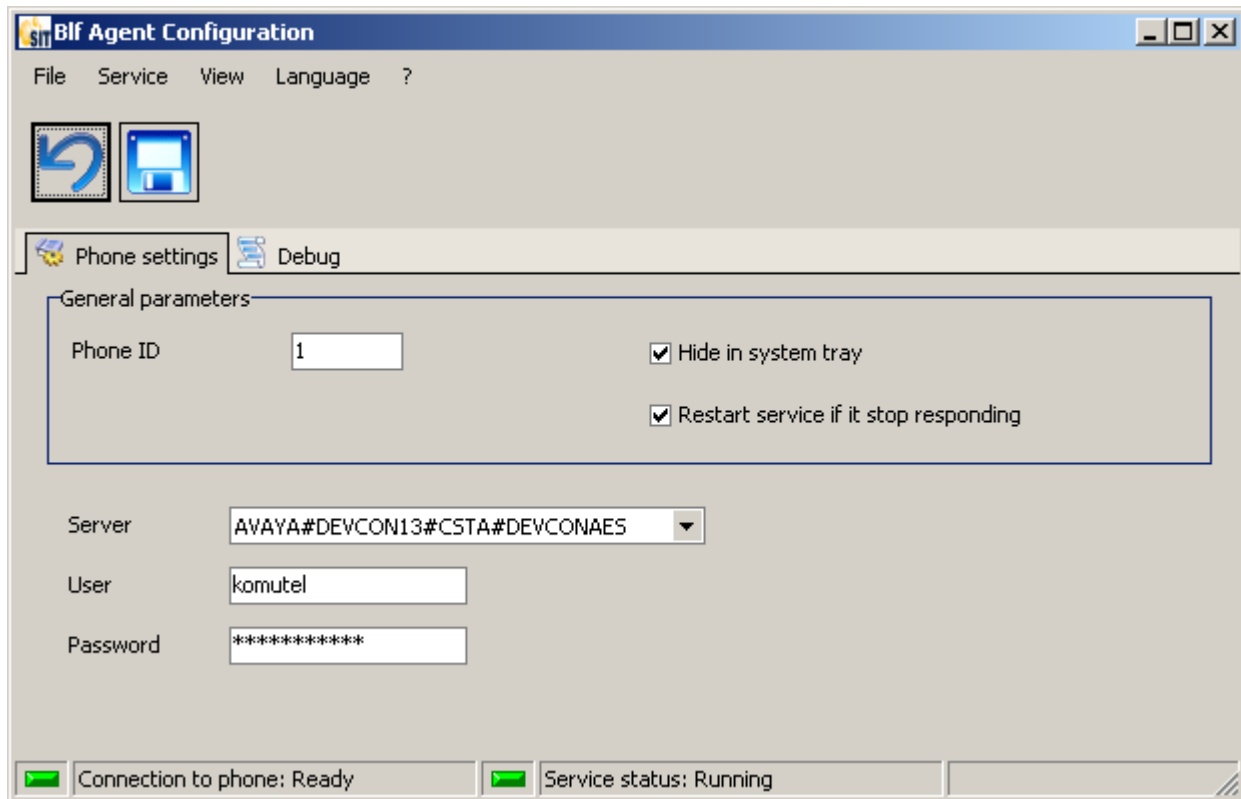
Primary Registration Time: Mon Apr 21 11:43:23 EDT 2014

Primary Registration Interrupted Time: Mon Apr 21 16:01:24 EDT 2014

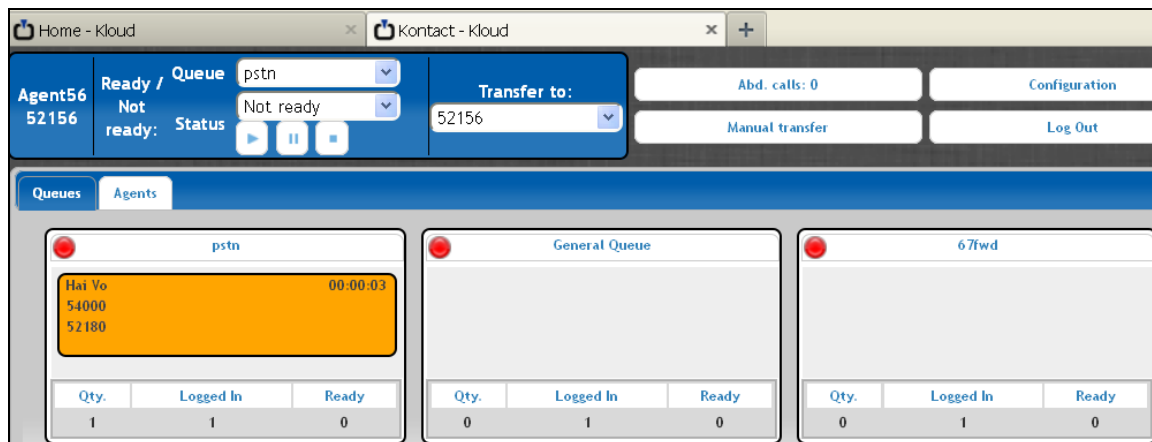
Primary Registration Interrupted: 14 d 7 hr 41 min

Secondary Registration Time: ---

- Verify that the BLF Agent service is running. Open the **Komutel BLF Agent Configuration** application and check the status bar at the bottom of the window. The **Connection to phone** status should display *Ready* and the **Service status** should display *Running* as shown below.



5. Place a call to a queue that has no available agents and verify that the call is successfully queued as shown below in the **Queues** tab in **Komutel Kloud**. In this example, a call is queued for the **pstn** queue and the caller ID is also displayed. The queued call can also be transferred to an agent by specifying the agent's number in the **Transfer to** field and clicking on the queued call in orange.



6. Place a call to a queue with an available agent and verify that when the call is answered by the agent, the agent's status is updated as shown below in the **Agents** tab in **Komutel Kloud**. In this example, the call was answered by *Agent56* and the green highlight indicates that the agent is on a call. In addition, the caller ID is also displayed.

Agent56  
52156

Ready / Not ready:

Queue: pstn

Status: Ready

Transfer to:

52156

Abd. calls: 1

Configuration

Manual transfer

Log Out

Queues Agents

Search:

Log.	Firstname	Lastname	Queue	Transfer to	Tel.	Display L1	Display L2	Ready / Not ready	Length
	KOMUTEL		pstn	5555				Logged out	00:36:44
	KOMUTEL		General Queue	5555				Logged out	00:36:44
	Agent56	52156	pstn	52156				Ready	00:00:06
	Agent56	52156	General Queue	52156				Not ready	00:36:33
	Agent56	52156	67fwd	52156				Not ready	00:36:33

## 10. Conclusion

These Application Notes have described the administration steps required to integrate the Komutel Kontakt with Avaya Aura® system. Kontakt was able to successfully register as SIP User on Session Manager and incoming calls were routed to an available agent, queued, or transferred to an agent as expected. All test cases passed with observations noted in **Section Error!** Reference source not found..

## 11. References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, May 2013, Release 6.3, Document Number 03-300509.
- [2] *Administering Avaya Aura® Session Manager*, June 2013, Release 6.3
- [3] *Administering Avaya Aura® System Manager*, May 2013, Release 6.3.
- [4] *Implementing Avaya Aura® Application Enablement Services for a Bundled Server Upgrade*, August 2010, Issue 9, Release 5.2, Document Number 02-300356.

---

**©2014 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).