

Avaya Solution & Interoperability Test Lab

# Application Notes for Sabio Thin Client Dialler with Avaya Proactive Contact and Avaya Aura® Application Enablement Services - Issue 1.0

#### Abstract

These Application Notes describe the configuration steps required to integrate Sabio Thin Client Dialler with Avaya Proactive Contact, Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager. The testing focused on verifying the inbound, outbound and blended agent functions of the Sabio Thin Client Dialler product.

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 tested configuration using Avaya Proactive Contact, Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Sabio Thin Client Dialler. The Sabio Thin Client Dialler solution is designed to allow contact centre agents access to Avaya Proactive Contact using only a standard web browser, this allows flexibility in terms of the physical agent location. Sabio Thin Client Dialler provides contact centre agents with access to the full range of inbound, outbound and blended agent contact capabilities by integrating with Avava Aura® Application Enablement Services using the Telephony Services API (TSAPI) and Avaya Proactive Contact. Sabio Thin Client Dialler removes the need for any applications to be installed locally on the contact centre agent PC. The TSAPI link is used with the Proactive Agent Blending feature on Avaya Proactive Contact to allow agents to handle both inbound and outbound calls. Proactive Agent Blending focuses on outbound calls and releases agents when an inbound call enters the monitored hunt group queue on Avaya Communication Manager. Sabio Thin Client Dialler used the TSAPI link to receive inbound call events and to control the inbound call (answer, hold, retrieve, hangup etc.) In the tested configuration, outbound, managed and blended jobs were supported by Sabio Thin Client Dialler. It is assumed that Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Proactive Contact Dialler have been installed and are operational. The detailed administration and basic connectivity amongst the Avaya products is not the focus of these Application Notes and will not be described.

### 2 General Test Approach and Test Results

The compliance testing focused on the ability of Sabio Thin Client Dialler to handle calls presented by Proactive Contact. All feature functionality test cases were performed manually to verify proper operation. The general test approach entailed:

- Establishing sessions from Sabio Thin Client Dialler agent to Avaya Proactive Contact and Application Enablement Services
- Verify Sabio Thin Client Dialler agents are able to view and join relevant dialler campaigns
- Verify Sabio Thin Client Dialler agents are able to handle calls directed to them from outbound, managed and blended agent dialer jobs.
- Verify Sabio Thin Client Dialler agents are able to set termination codes and schedule call backs
- Verify agents are automatically joined to another campaign when job linking is used
- Verify call handling using basic telephony operations such as answer, hold/retrieve, transfer, consult, conference, and disconnect.
- Verify Proactive Contact specific tasks such as job linking and call failures to busy or unobtainable.

The serviceability tests were performed by disconnecting and reconnecting Sabio Thin Client Dialler server from the network and restarting the server based components used in the testing.

### 2.1 Interoperability Compliance Testing

The interoperability testing focused on the ability of the Sabio solution to interoperate with the Avaya solution. The following is a summary of the feature and functionality testing that was undertaken:

- Establish sessions from Sabio Thin Client Dialler agent to Avaya Proactive Contact.
- Verify Sabio Thin Client Dialler agents are able to view and join relevant dialler campaigns.
- Verify Sabio Thin Client Dialler agents are able to handle calls directed to them.
- Verify basic telephony operations such as hold/retrieve, transfer, consult, conference, and disconnect.
- Verify Sabio Thin Client Dialler agents are able to set termination codes and schedule call backs.
- Verify agents are automatically joined to another campaign when job linking is used.

The serviceability testing focused on verifying the ability of Sabio Thin Client Dialler to recover from adverse conditions, such as reboots, network failures and restarting agent sessions.

### 2.2 Test Results

All feature and serviceability tests passed. Sabio Thin Client Dialler successfully handled inbound, outbound and blended agent calls. For serviceability testing, Sabio was able to resume call handling after restoration of connectivity to the Proactive Contact and Application Enablement Services servers, from network disconnect/re-connect, and Sabio resets.

### 2.3 Support

For technical support of Sabio products please check for the local support contact at the following web address: <u>www.sabio.co.uk</u>

# 3 Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The solution consisted of Proactive Contact, Communication Manager, Application Enablement Services and Sabio Thin Client Dialler web server. Proactive Contact has a CTI connection to Application Enablement Services and uses this connection to make calls from the Communication Manager. Sabio Thin Client Dialler uses the Proactive Contact Agent API and the Telephony Services API (TSAPI) provided by Application Enablement Services to complete agent functions.

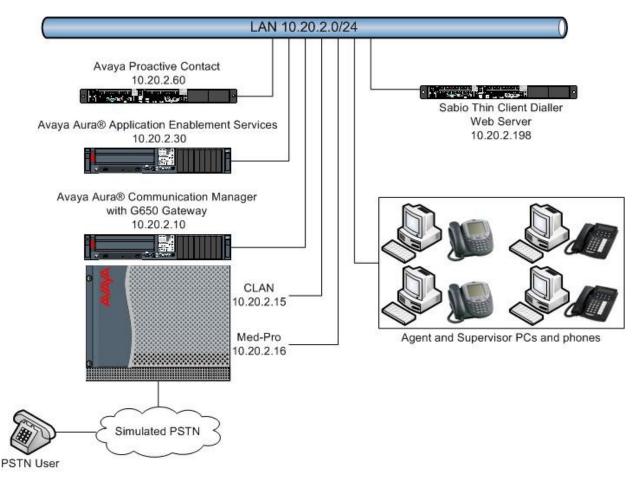


Figure 1: Network Topology Used During Testing

# 4 Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment	Software Version
Avaya S8730 Server	Avaya Aura® Communication Manager
	0.2.1
Access C(50 Mailia Catagoria	(R015x.02.1.016.4)
Avaya G650 Media Gateway	
- CLAN TN799DP	HW15, FM49
- IP Media Processor TN2602AP	HW01, FM34
Dell PowerEdge 1950 Server	Avaya Aura® Application Enablement
	Services
	4.2.2 patch 4 (r4-2-2-31-0)
HP ProLiant DL 385 G2 Server	Avaya Proactive Contact 4.1.1 Patch 137
PC Desktop Running Proactive Contact	Proactive Contact Supervisor 4.1.1
Supervisor	
Sabio Web Server	Sabio Thin Client Dialler v1.6.5.0

Table 1: Hardware and Software Version Numbers

# 5 Configuration of Avaya Aura® Communication Manager

These Application Notes assume that Communication Manager is configured and operational and the basic connectivity to Proactive Contact is in place. This section focuses only on the configuration required to enable Sabio Thin Client Dialler to integrate with Communication Manager and that of the station that will be used by the Sabio Thin Client Dialler agent. The configuration is performed via the System Access Terminal (SAT) on Communication Manager.

#### 5.1 Confirm Necessary Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Log into the Communication Manager SAT interface and use the **display system-parameters customer-options** command to determine these values. On **Page 2** verify the **Maximum Concurrently Registered IP Stations** is sufficient.

display system-parameters customer-options		Page	<b>2</b> of	10
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:	200	0		
Maximum Concurrently Registered IP Stations:	18000	5		
Maximum Administered Remote Office Trunks:	0	0		
Maximum Concurrently Registered Remote Office Stations:	0	0		

On Page 3 verify the field Computer Telephony Adjunct Links is set to y.

display system-parameters customer-opt	ions Page	3	of	11
OPTIONAL	FEATURES			
Abbreviated Dialing Enhanced List? n	Audible Message Waiting?	n		
Access Security Gateway (ASG)? n	Authorization Codes?	У		
Analog Trunk Incoming Call ID? n	CAS Branch?	n		
A/D Grp/Sys List Dialing Start at 01? n	CAS Main?	n		
Answer Supervision by Call Classifier? n	Change COR by FAC?	n		
ARS? y	Computer Telephony Adjunct Links?	У		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net?	N		

On Page 6 confirm that the call centre features highlighted below are activated.

```
display system-parameters customer-options
                                                                               6 of 11
                                                                       Page
                         CALL CENTER OPTIONAL FEATURES
                          Call Center Release: 5.0
                                ACD? v
                                                                 Reason Codes? n
                       BCMS (Basic)? y
                                          Service Level Maxımızer? n
Service Observing (Basic)? y
                                                     Service Level Maximizer? n
         BCMS/VuStats Service Level? n
 BSR Local Treatment for IP & ISDN? n Service Observing (Remote/By FAC)? n
                  Business Advocate? n
                                                   Service Observing (VDNs)? n
                                                                    Timed ACW? n
                   Call Work Codes? n
      DTMF Feedback Signals For VRU? n
                                                            Vectoring (Basic)? y
                   Dynamic Advocate? n
                                                       Vectoring (Prompting)? y
      Dynamic Advocate? n
Expert Agent Selection (EAS)? y
EXC. DUD2 a
                                                   Vectoring (G3V4 Enhanced)? y
               Forced ACD Calls? n
Least Occupied Agent? n
bead Interfol
          Lookahead Interflow (LAI)? n
                                                            Vectoring (CINFO)? n
```

#### 5.2 Define Feature Access Codes (FAC)

A FAC (feature access code) should be defined for each feature that will be used. Use **change feature-access-codes** to define the required access codes. On **Page 5** define a FAC for each of the following:

- Auto-In Access Code: When activated this feature will set the ACD agent to a state where they are available to handle calls, upon completion of a call the agent will automatically be made available again.
- Aux Work Access Code: When activated this feature will set the ACD agent to an Auxilary work state, this is the default state for an agent upon first login.
- Login Access Code: This feature allows ACD agents to log in to an extension.
- Logout Access Code: This feature allows ACD agents to log out of an extension.
- **Manual-in Access Code:** When activated this feature will set the ACD agent to a state where they are available to handle calls, upon completion of a call the agent will be unavailable until the feature is activated again.

```
      change feature-access-codes
      Page
      5 of
      8

      FEATURE ACCESS CODE (FAC)
      Automatic Call Distribution Features
      8

      After Call Work Access Code:
      Assist Access Code:
      8

      Auto-In Access Code:
      *27
      8

      Aux Work Access Code:
      *28
      10gin Access Code:
      *28

      Login Access Code:
      *25
      10gout Access Code:
      *26

      Manual-in Access Code:
      *29
      *29
```

### 5.3 Configure Sabio Thin Client Dialler Agent Station

Use the **add station n** command to add a station that will be used by Sabio Thin Client Dialler Agent. Set the **Type** field to the handset type being used. Enter a descriptive name in the **Name** field and specify a **Security Code** that will be used for the phone to log in.

add station 31020	Page	1 of 5
	STATION	
Extension: 31020	Lock Messages? n	BCC: 0
Туре: 9620	Security Code: 31020	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: IP Station	Coverage Path 2:	COS: 1
	Hunt-to Station:	

On Page 2 set Auto Answer to acd to allow acd calls to be automatically answered.

```
add station 31020
                                                            Page
                                                                  2 of
                                                                         5
                                    STATION
FEATURE OPTIONS
                                         Auto Select Any Idle Appearance? n
         LWC Reception: spe
                                                 Coverage Msg Retrieval? y
       LWC Activation? y
 LWC Log External Calls? n
                                                             Auto Answer:acd
           CDR Privacy? n
                                                        Data Restriction? n
  Redirect Notification? y
                                               Idle Appearance Preference? n
 Per Button Ring Control? n
                                             Bridged Idle Line Preference? n
```

#### 5.4 Configure ACD Agent for Blending

If call blending is to be used with Proactive Contact then an ACD agent must be added and assigned the relevant skills. To add an agent login ID, use the command **add agent-loginID n** where **n** is the agent ID to be added. Enter a descriptive name for **Name**.

```
add agent-loginID 34020
                                                                    Page
                                                                            1 of
                                                                                    2
                                AGENT LOGINID
               Login ID: 34020
                                                                AAS? n
                   Name: ACD Agent ID
                                                              AUDIX? n
                     TN: 1
                                                     LWC Reception: none
                    COR: 1
                                            LWC Log External Calls? n
                                           AUDIX Name for Messaging:
          Coverage Path:
          Security Code:
          Port Extension:
                                       LoginID for ISDN/SIP Display? n
```

On **Page 2** assign skills to the agent by entering the required inbound or outbound hunt groups for **SN** and entering a skill level of **1** for **SL**.

add agent-login]	ID 34020				Page	<b>2</b> of	2
		AGENI	LOGINID				
Direct Agent	: Skill:			Se	rvice Objective?	n	
Call Handling Pref	ference: sk	ill-level		Local	Call Preference?	n	
SN RL SL	SN	RL SL	SN	RL SL	SN RL SL		
1:2 <b>1</b>	16:		31:		46:		
2: <b>3 1</b>	17:		32:		47:		

#### 5.5 Configure Node-Names IP

Use the **change node-names ip** command. Add an entry in the node-names form for the CLAN, AES server and the default gateway used for the IP network to which the CLAN will be connected. A **Name** and **IP** Address should be added for each. The values used during the interoperability test are highlighted below.

change node-names	ip		Page	1 of	2
-	-	IP NODE NAMES	-		
Name	IP Address				
CLAN	10.20.2.15				
Gateway	10.20.2.1				
MEDPRO	10.20.2.16				
PC4.1	10.20.2.60				
RDTT	10.20.2.41				
SiteB	10.10.15.13				
VPCLAN	10.20.2.18				
aesserver	10.20.2.30				
announce	10.20.2.17				

#### 5.6 Configure CLAN for AES Connectivity

Add the CLAN to the system configuration using the **add ip-interface n** command where **n** is the CLAN board location. Enter the CLAN node name assigned in **Section 5.5** to the **Node Name** field. Enter values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, /24 and **Gateway** are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** field to **y**, and use a separate **Network Region** for the CLAN dedicated for AES connectivity. Default values may be used in the remaining fields.

```
add ip-interface 01a02
                                                                                         Page
                                                                                                   1 of
                                                                                                             3
                                           IP INTERFACES
                       Type: C-LAN

    Slot: 01A02
    Target socket load and Warning level: 400

    Code/Suffix: TN799
    D

    Receive Buffer TCP Window Size: 8320

    Allow H 323 Endpoints? v

       Enable Interface? y
                                                                Allow H.323 Endpoints? y
                                                                  Allow H.248 Gateways? y
                     VLAN: n
         Network Region: 1
                                                                    Gatekeeper Priority: 5
                                          IPV4 PARAMETERS
                Node Name: CLAN
             Subnet Mask: /24
      Gateway Node Name: Gateway
           Ethernet Link: 1
           Network uses 1's for Broadcast Addresses? y
```

#### 5.7 Configure Transport Link for AES Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- Service Type: Set to AESVCS.
- Enabled: Set to y.
- Local Node: Set to the node name assigned for the CLAN in Section 5.5.
- Local Port: Retain the default value of 8765.

change ip-	services					Page	<b>1</b> of	4
Service Type AESVCS	Enabled Y	Local Node CLAN	IP SERVICES Local Port 8765	Remote Node	Remote Port			

Go to Page 4 of the ip-services form, and enter the following values:

- AE Services Server: Name obtained from the AES server, in this case aesserver.
- **Password:** Enter a password to be administered on the AES server.
- Enabled: Set to y.

Note: The name and password entered for the AE Services Server and Password fields must match the name and password on the AES server in Section 7.2. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing uname –n at the Linux command prompt.

change ip-ser		AE Services Administr	ation	Page	4 of	4
Server ID	AE Services Server	Password	Enabled	Status		
1:	aesserver	aeserverpw123	У	in use		
2:						

#### 5.8 Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command where **n** is the link number to be added. Enter an available extension number in the **Extension** field. 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 11
      Page 1 of 3

      CTI Link: 11
      CTI LINK

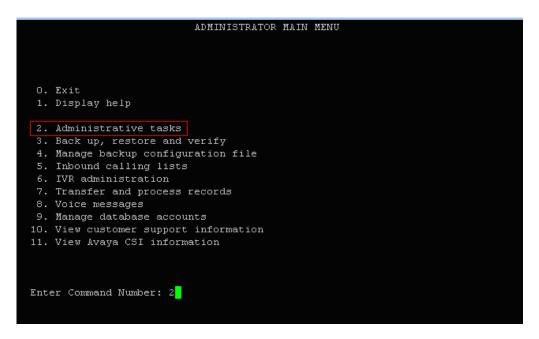
      Extension: 720
      COR: 1

      Type: ADJ-IP
      COR: 1
```

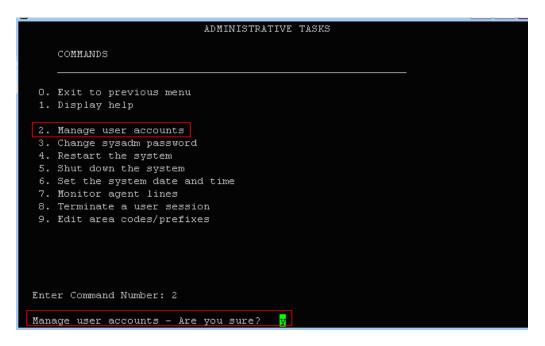
MMc; Reviewed:	Solution & Interoperability Test Lab Application Notes	11 of 26
SPOC 7/20/2011	©2011 Avaya Inc. All Rights Reserved.	SabioTCD_521

### 6 Configure Avaya Proactive Contact Agents

A user account needs to be setup for each agent that will log in to Proactive Contact via Sabio Thin Client Dialler. One of the ways to setup an agent user account is to use the Linux administration menus. Log in to Proactive Contact with system administrative privileges. To add an agent account, from the ADMINISTATOR MAIN MENU screen, select Administrative tasks by entering 2 at the Enter Command Number prompt.



In the resulting menu, select Manage user accounts by entering 2 in the Enter Command Number prompt, and enter y in the Manager use accounts – Are you sure? prompt.



MMc; Reviewed: SPOC 7/20/2011

Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved. 12 of 26 SabioTCD\_521 In the resulting screen, press **CTRL-L** to add a new agent login. Enter values in the **USER NAME**, **PASSWORD**, **GROUP FOR LOGIN** and **DESCRIPTION** fields, and press **Enter**. Repeat this for each agent that will log in to Proactive Contact via Sabio Thin Client Dialler. Press **CTRL-X** to exit the screen and enter **y** at the **Save Changes**? prompt.

		MANAGE	USE	R ACCOUNTS		
	USE.	R NAME:		Agent6		UID: 2025
	PAS	SWORD:		*******	* * *	* * * * * * * * * * * * * * * * * * * *
	GRO	UP FOR LOGIN:		agent		
	DES	CRIPTION:		Test Agent 6		
COMMAND	s:		GI	ROUPS:		
CTRL-	L	Add a user LOGIN		system	SY	STEM OPERATOR
CTRL-	С	CHANGE a field		agent	AG.	ENTS
CTRL-	D	DELETE current user		pcanal	AN.	ALYSIS OPERATOR
CTRL-	F	FIND a user		sysadm	SY	STEM ADMINISTRATOR
CTRL-	X	EXIT user editing		auditor	SY	STEM AUDITOR
				rbac	RB.	AC GROUP
				rbacadmin	RB.	AC Admin GROUP
Save ch	ange	s? – (Y/N) <mark>y</mark>				

# 7 Configure Avaya Aura® Application Enablement Services

This section covers the administration of AE Services (Application Enablement Services). AE Services is configured via an internet browser using the Administration web interface. It is assumed that AE Services software and the license file have already been installed.

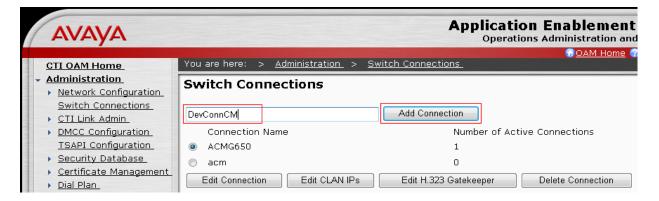
#### 7.1 Logging in to Avaya Aura® Application Enablement Services

To access the administration web interface, enter **https://<ip-addr>/MVAP** as the URL in an internet browser, where <ip-addr> is the active IP address of AE Services. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button

Please log on.	Application Enablen	nent Services	? Hel
Logon:	Pleas	e log on.	
	Logon:		
Password:	Password:		

### 7.2 Add Switch Connection

From the left pane of the Administration web interface, navigate to Administration  $\rightarrow$  Switch Connections. Enter a name for the switch connection to be added and select the Add Connection button.



In the resulting screen, enter and confirm the **Switch Password**. This must match the password configured in **Section 5.7**. When finished, select the **Apply** button.

Αναγα		Application Enabl Operations Administ
CTI OAM Home	You are here: > <u>Administration</u> > <u>Sw</u>	vitch Connections
<ul> <li>Administration</li> <li>Network Configuration</li> </ul>	Set Password - DevConnCM	
Switch Connections	Please note the following: * Changing the password affects only new	
DMCC Configuration	Changing the password anects only nev	w connections, not open connections.
TSAPI Configuration Security Database	Switch Password	
<u>Certificate Management</u> Dial Plan	Confirm Switch Password	
Enterprise Directory	SSL Apply Cancel	V
Host AA		

Back in the **Switch Connections** screen select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the CLAN that will be used for the AE Services connection and select the **Add Name or IP** button.



#### 7.3 Add TSAPI Link

From the left pane of the Administration web interface, navigate to Administration  $\rightarrow$  CTI Link Admin  $\rightarrow$  TSAPI Links. For Link, select the next available link number using the drop down menu. For the Switch Connection field, select the switch connection defined in Section 7.2. The Switch CTI Link Number must match the CTI link number configured in Section 5.8. Ensure that the ASAI Link Version field is set to 4. Set the Security field to Both to create a secure and a non-secure TSAPI link. When all the values have been set, select the Apply Changes button.

Αναγα		Application Enablemen Operations Administration a
CTI OAM Home	You are here: > <u>Administration</u> > <u>C</u>	OAM Home TI Link Admin > TSAPI Links
<ul> <li>Administration</li> <li>Network Configuration</li> </ul>	Add / Edit TSAPI Links	
Switch Connections	Link:	3 🗸
TSAPI Links	Switch Connection:	DevConnCM -
CVLAN Links DLG Links	Switch CTI Link Number:	11 -
DLG LINKS     DMCC Configuration	ASAI Link Version	4 -
TSAPI Configuration	Security	Both 👻
Security Database	Apply Changes Cancel Changes	
<u>Certificate Management</u> Dial Plan		_

Once the TSAPI link has been added navigate to Administration  $\rightarrow$  Security Database  $\rightarrow$  Tlinks to view the Tlink Name.

Αναγα	Application Enablement Ser Operations Administration and Maint
CTI OAM Home. Administration. Network Configuration. Switch Connections. CTI Link Admin. DMCC Configuration. TSAPI Configuration. Security Database. SDB Control. CTI Users. Worktops. Devices. Device Groups. Tlinks.	You are here: > Administration > Security Database > Tlinks         Tlinks         Tlink Name         AVAYA#DEVCONNCM#CSTA#AESSERVER         AVAYA#DEVCONNCM#CSTA-S#AESSERVER         Edit Tlink         Delete Tlink

#### 7.4 Add TSAPI User

From the left pane of the Administration web interface, navigate to User Management  $\rightarrow$  Add User. From the Add User screen, enter values for all of the compulsory fields marked with \*. The User ID and User Password are used in the configuration of Sabio Thin Client Dialler. In addition to the compulsory fields, the CT User field should be set to Yes. When complete, select the Apply button (not shown).

Αναγα				Enablement S
User Management Home	You are here: > <u>U</u>	ser Management > <u>Ac</u>	<u>id User</u>	<mark>⊚OAM Home</mark> ⊘H
✓ <u>User Management</u> List All Users	Add User			
Add User Search Users	Fields marked with *	can not be empty.		
Modify Default User Change User Password	* User Id	sabio		
Service Management	* Common Name	L		
▶ <u>Help</u>	* Surname	sabio		
	* User Password	•••••		
	* Confirm Password	•••••		
	Admin Note			
	Avaya Role	None -		
	Business Category			
	Car License			
	CM Home			
	Css Home			
	CT User	Yes 🕶		
	Department Number	•		

# 8 Configure Sabio Thin Client Dialler

For Sabio Thin Client Dialler to interoperate properly with the Avaya solution, two files on the Sabio Thin Client Dialler server require information about the Avaya solution. The **tsapi.pro** file and the **setting.xml** file.

### 8.1 Administer tsapi.pro file

From the Sabio Thin Client Dialler server browse to  $C: \rightarrow Program Files \rightarrow apache-tomcat 5.5.28 \rightarrow common \rightarrow classes and open the file tsapi.pro with an editor. Add in the IP address of$ the Application Enablement Server and the port number used for TSAPI communication,highlighted in the screen below is the entry used during testing.

```
# tsapi.pro
#
tsapi.pro
#
the transful to the servers offering Telephony Services via TCP/IP.
# This is a list of the servers offering Telephony Services via TCP/IP.
# Either domain name or IP address may be used; default port number is 450
# The form is: host_name=port_number For example:
#
tserver.mydomain.com=450
# 127.0.0.1=450
#
# (Remove the '#' when creating actual server entries.)
[Telephony Servers]
10.20.2.30=450
tsDevicePerformanceOptimization=true
```

#### 8.2 Administer setting.xml file

From the Sabio Thin Client Dialler server browse to C:  $\rightarrow$  Program Files  $\rightarrow$  apache-tomcat-5.5.28  $\rightarrow$  webapps  $\rightarrow$  ThinClientCTI\_1.6.5.0  $\rightarrow$  conf and open the file setting.xml with an editor. In the softphone section set properties for Proactive Contact Agent API and for AE services connections. Highlighted below are the values used in the example configuration.

- Proactive Contact Agent API connection: provider id="DIALLER" type="pc4" server="localhost" port="22700
- AE Services TSAPI connection: provider id="AES" type="jtapi" tlink="AVAYA#DEVCONNCM#CSTA#AESSERVER" username="sabio"password="\*\*\*\*\*\*"

For more information on the **setting.xml** file, please contact Sabio support using the detail in **Section 2.3.** 

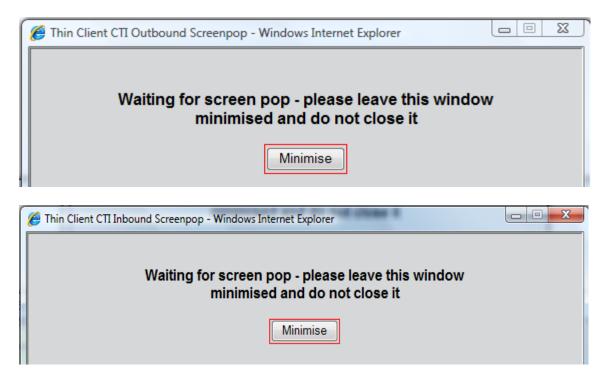
<Text removed for brevity> <softphone class="uk.co.sabio.softphone.pc4api.blended.Pc4ApiBlendedSoftphone" lbclass="uk.co.sabio.softphone.pc4api.blended.Pc4ApiBlendedProviderLoadBalancer" mode="Dialler" multiStage="true" userModes="Blend,Outbound"> <provider id="BLENDER" type="pc4blended" server="" port="" formfile="" /> <provider id="DIALLER" type="pc4" server="localhost" port="22700" formfile="" diallerListConfig="true" /> <provider id="AES" type="jtapi" tlink="AVAYA#DEVCONNCM#CSTA#AESSERVER" username="sabio" password="\*\*\*\*\*\*" /> </softphone> <Text removed for brevity>

# 9 Logging into Sabio Thin Client Dialler

To access the Sabio Thin Client Dialler agent application, enter the URLs provided by Sabio into an internet browser. The following URLs were used during testing and are provided to illustrate the type of URLs that may be provided.

- http://l3c7637.sabio.co.uk:8083/softphone/jsp/softphonestandalone.jsp?targetPage=/softp hone/jsp/integrated.jsp&thickClient=true&screenpopURL=/softphone/custom/dasinboun dscreenpop.jsp&readonly=false&directCall=true&profile=clasup
- http://l3c7637.sabio.co.uk:8083/softphone/jsp/softphonestandalone.jsp?targetPage=/softp hone/jsp/integrated.jsp&thickClient=false&screenpopURLInbound=/softphone/custom/d asinboundscreenpop.jsp&screenpopURLOutbound=/softphone/custom/dasoutboundscree npop.jsp&readonly=false&directCall=true&profile=recbed

Three windows will appear, two screenpop windows and the Thin Client Agent interface window. The windows entitled **Thin Client CTI Inbound Screenpop** and **Thin Client CTI Outbound Screenpop** can be minimized by clicking the **Minimise** button.



In the Sabio Thin Client Agent window, enter the Proactive Contact agent username in the **agent** field, and password in the **password** field. Enter the station number used by the agent in the **station** field. Click the **next** button.

Sabio Thin Client Agent Version 1.6.5.0 - Windows Internet Explorer		
Status: Not Registered.	Please enter Dialler login details:     X       agent     agent1       station     31003       password     next	Logou AS: NOT REGISTERED

In the resulting window, use the drop down menu to select the **mode** that the Sabio Thin Client Agent application will login in with. If call blending is to be used, enter an ACD agent login ID and password in the **acm login** and **acm pass** fields respectively. If no call blending is to be used, then these fields may remain blank. Click the **register** button to continue.

🏉 Sabio Thin Client Agent Version 1.6.5.0 - Wir	ndows Internet Explorer		
Status: Not Registered.	1 2 3 acm lo acm p	Outbound  ACW ACW ACW ACW ACW ACW ACW ACW ACW	AUX AVL Login Logov

In the resulting window, use the drop down menu to select one of the available Proactive Contact dialler jobs in the **campaign** field and click the **join** button to join the job.

8	Sabio Thin Client Agent Version 1.6.5.0 - Windows Internet Explore		
	Status: Logged On (St.:31003, Ag.:         1         2         3	Please select the campaign to join:     X       campaign     outbnd       refresh     join	ACW AUX AVL Login Logou 1.Break AS: NOT REGISTERED

Once the Sabio Thin Client Agent is logged in, the softphone functional buttons will appear to the left of the window as highlighted below.

Ø Sabio Thin Client Agent Version 1.6.5.0 - Windows Internet Explorer	
Status: Logged On (Ca.:outbnd, St.:31003, Ag.:	ACW AUX AVL Login Logov
Click here to display the dialer pane.	HI IP II I I III IIII IIIII IIIIIIIIIII

When an inbound or outbound call is delivered to the Sabio Thin Client Dialler a screen pop is given to the agent displaying the available customer details. To end and complete the call a completion code is selected at the bottom of the screen pop window.

Screen Pop: Session 7B13A	EA8CBDDE9FDD83A7399FB551A83 77940cc6-d729-4 💷 💷 💻
notifyFieldData:	<empty></empty>
waitMsg:	<empty></empty>
ZIPCODE:	9221
callType:	OUTBOUND
PHONE2:	000000000
PHONE1:	2032768732
opMesg:	Home phone - 2032768732
notifyFieldName:	<empty></empty>
NAME2:	JOHN DOE
NAME1:	JOHN DOE
BALANCE:	0
ACCTNUM:	5300292221349177
Acc mom.	5500292221349177
Completions	Code 24   Set Code 24
	Code 23
	Code 22 Recall release
	Recall release Code 21

### **10 Verification Steps**

The status of the Sabio Thin Client Dialler server can be checked by logging in to Sabio Softphone Manager. To login into Sabio Softphone Manager, enter the URL: http://servername:8083/softphone/jsp/softphone-manage.jsp into an internet browser and login with the appropriate credentials.

<u>sabio</u>		none Manager 1.6.5.0 tion required HOME EMAIL US
Softphone Authentication Re	equired	
Username:		
Password:		
Log In Reset		

The resulting page will give a summary of the Sabio Thin Client Dialler configuration.

Softphone Manager 1.6.5.0 Periodically updated with live statistical information	
Softphone Configuration	Web App Configuration
Version: 1.6.5.0	App Context: HPR AES CTI Softphone Application
Softphone Implementation Class: uk.co.sabio.softphone.pc4api.blended.Pc4ApiBlendedSoftphone	Total License Count: 5
Softphone Implementation Load Balancer Class: uk.co.sabio.softphone.pc4api.blended.Pc4ApiBlendedProviderLoadBalancer	Available License Count: 3
Client Poll Frequency - Client AJAX Request Poll(Browser reads this setting after page load event).	Inactive Session Expires: 7200 secs
Client Poll Frequency: 0 secs	Active Session Count: 2
Agent Login Over-ride - agent will not be prompted when over-riding an existing agent associated with station	JVM Details
Agent Login Auto Over-ride: false	VM Version: 16.3-b01 Vendor: Sun Microsystems Inc.
Agent Greeting - performs db insertion/removal queries on agent login/logout.	Used Memory (bytes): 29970432
Agent Greeting Enabled: false	Free Memory (bytes): 14615152
Screen Pop - conf details	Max Memory (bytes): 259522560
Screen Pop URL: http://10.80.138.143:9190/G2/UX/M/HomeserveAID/SearchResultsCP/	JVM Start Time: Jul 07 2010 13:19:50.195
Screen Pop Enabled: true	JVM Up Time: 0:11:50.613
Screen Pop Agent Call Enabled: false	Live Softphone Data
UUI Bean: uk.co.sabio.softphone.uui.UUIBean	Active Softphone Count: awaiting live data
UUI Parser Delimiter: ,	Inactive Softphone Count: awaiting live data
Auto Answer - finite thread that fires on alerting event.	Full Softphone Count: 2
Auto Answer Delay: -1ms	Provider Details
Auto Answer Enabled: true	Provider ID: BLENDER
Auto Answer Agent Calls Enabled: false	Allocation Count: 2

Scroll to the bottom of the page and the active connections can be viewed. Verify the expected station numbers and agent login ids can be seen towards the left and that expected activity state is seen towards the right.

1	1.	Station: 31002	Agent ID: agent2,34002	IP: 10.20.2.198	Created: Jul 07 2010 13:30:51.365	Last Poll: Jul 07 2010 13:33:07.642	Poll Count: 55	key: 20A90168A3B4264F31C06AD04C223841	Actively Receiving Events: true	TLink: BLENDER	ASC: READY
2	2.	Station: 31003	Agent ID: agent1,34003	IP: 10.20.2.199	Created: Jul 07 2010 13:27:25.028	Last Poll: Jul 07 2010 13:33:06.340	Poll Count: 138	key: 7B13AEA8CBDDE9FDD83A7399FB551A83	Actively Receiving Events: true	TLink: BLENDER	ASC: BUSY

# 11 Conclusion

These Application Notes describe the required configuration steps for Sabio Thin Client Dialler to successfully interoperate with Avaya Proactive Contact, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature functionality and serviceability test cases were completed successfully.

# 12 Additional References

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

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

- 1. Administering Avaya Proactive Contact (Linux-based Interface); Mar 2009
- 2. Administering Avaya Proactive Contact 4.; April-2009
- 3. Administering Avaya Aura® Communication Manager, Document No. 03-300509, May 2009
- 4. Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent Selection (EAS) Reference, Document No. 07-600780, April 2009
- 5. Application Enablement Services Administration and Maintenance Guide Document No. 02-300357, May 2008

Documentation for Sabio products may be requested from Sabio at http://www.sabio.co.uk

#### ©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and <sup>TM</sup> 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*.