



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

---

# **Application Notes for Bold Technologies Manitou with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Bold Technologies Manitou to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Bold Technologies Manitou is an alarm automation solution for central stations.

In the compliance testing, Bold Technologies Manitou used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to support the Auto Dialer feature for central station operators.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for Bold Technologies Manitou to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Bold Technologies Manitou is an alarm automation solution for central stations.

In the compliance testing, Bold Technologies Manitou used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to provide the Auto Dialer feature for central station operators.

The central station operators have desktop computers running the Bold Technologies ManitouCS Operator Workstation to handle alarms. The Auto Dialer feature allows an operator to select a customer contact phone number, and have the system place the outbound call on behalf of the operator. Bold Technologies Manitou accomplishes this by using the DMCC interface and the Multiple Registration feature from Avaya Aura® Application Enablement Services to register a virtual IP softphone for the operator, and initiate the outbound call from the virtual IP softphone. The Bold Technologies ManitouCS Operator Workstation can also be used to hang up the outbound call.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Initiation and termination of outbound calls were performed using the ManitouCS Operator Workstation. Additional call controls such as hold, resume, transfer, and conference were performed from the operator telephone.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to Manitou and to the ManitouCS Operator Workstation.

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 test included feature and serviceability testing.

The feature testing focused on verifying the following on Manitou:

- Use of DMCC registration and monitoring services to register and monitor the virtual IP softphones.
- Use of DMCC call control services to initiate and drop outbound calls via the virtual IP softphones.
- Proper passing of replacement calling party number in the User-to-User Information parameter.
- Proper handling of outbound call for scenarios involving invalid number, internal destination, external destination, drop, hold, resume, transfer, conference, multiple operators, and multiple calls.

The serviceability testing focused on verifying the ability of Manitou to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to Manitou and to the ManitouCS Operator Workstation.

## 2.2. Test Results

All test cases were executed and verified. The following were observations on Manitou from the compliance testing.

- When the operator uses ManitouCS Operator Workstation to drop from an active conference, by design the conference call is cleared and therefore all remaining parties are dropped.
- The ManitouCS Operator Workstation displays the generic “Unknown error in connecting” for any failures from the outbound call, including a busy destination.
- The ManitouCS Operator Workstation may generate multiple instances upon server and/or client Ethernet disruptions. The multiple instances do not have downside impact as any can continue to be used, and the operator can manually close the extra instances as desired.

## 2.3. Support

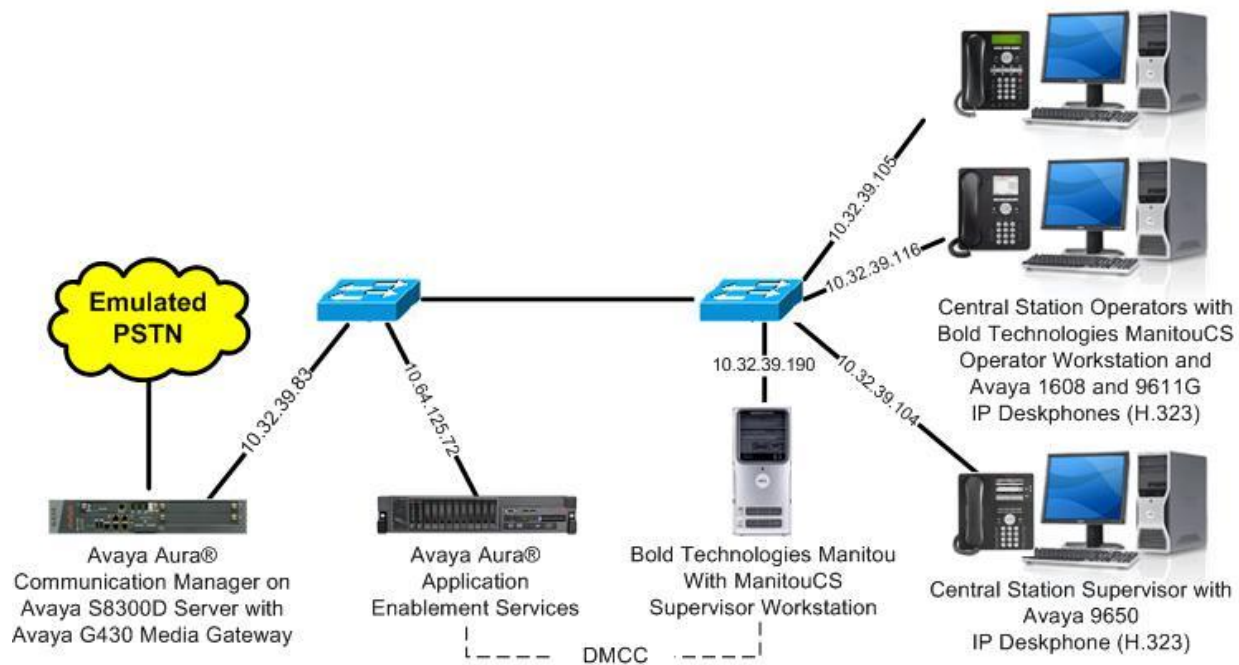
Technical support on Manitou can be obtained through the following:

- **Phone:** (719) 593-2829
- **Email:** [support@boldgroup.com](mailto:support@boldgroup.com)

### 3. Reference Configuration

Manitou can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration, which also hosted the ManitouCS Supervisor Workstation application, as shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of telephony devices are not the focus of these Application Notes and will not be described.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G450 Media Gateway	6.2 SP5 (R016x.02.0.823.0-20396)
Avaya Aura® Application Enablement Services	6.2 (r6-2-0-18-0 Patch 1)
Avaya 1608 IP Deskphone (H.323)	1.302S
Avaya 9611G IP Deskphone (H.323)	6.2209
Avaya 9650 IP Deskphone (H.323)	3.105S
Bold Technologies Manitou on Microsoft Windows 2008 R2 Standard <ul style="list-style-type: none"><li>• PBXServer</li><li>• ManitouCS Supervisor Workstation</li><li>• Avaya DMCC .NET (ServiceProvider.dll)</li></ul>	1.61.0.885 SP1 1.61.4827.650 1.61.0.682 6.2.0.29
Bold Technologies ManitouCS Operator Workstation on Microsoft Windows XP Professional <ul style="list-style-type: none"><li>• BoldPBX.tsp</li></ul>	1.61.0.885 2002 SP3 1.61.4827.381

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer special applications
- Administer operator stations

### 5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	y	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>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			

### 5.2. Administer CTI Link

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

add cti-link 1		Page	1 of	3
CTI LINK				
CTI Link:	1			
<b>Extension:</b>	40001			
<b>Type:</b>	ADJ-IP			
<b>Name:</b>	TSAPI Link			
		COR:	1	

### 5.3. Administer Special Applications

Use the “change system-parameters special-applications” command, and navigate to **Page 4**. Enable the **(SA8481) – Replace Calling Party Number with ASAI ANI** special application, as shown below.

This feature allows Manitou to supply calling party number information as part of the third party make call request for outgoing ISDN calls.

```
change system-parameters special-applications                               Page 4 of 10
                                SPECIAL APPLICATIONS

    (SA8481) - Replace Calling Party Number with ASAI ANI? y
        (SA8500) - Expanded UII Display Information? n
        (SA8506) - Altura Interoperability (FIPN)? n
        (SA8507) - H245 Support With Other Vendors? n
        (SA8508) - Multiple Emergency Access Codes? n
    (SA8510) - NTT Mapping of ISDN Called-Party Subaddress IE? n
        (SA8517) - Authorization Code By COR? n

        (SA8520) - Hoteling Application for IP Terminals? n
    (SA8558) - Increase Automatic MWI & VuStats (S8700 only)? n
        (SA8567) - PHS X-Station Mobility over IP? n
    (SA8569) - No Service Observing Tone Heard by Agent? n
        (SA8573) - Call xfer via ASAI on CAS Main? n
    (SA8582) - PSA Location and Display Enhancements? n
        (SA8587) - Networked PSA via QSIG Diversion? n
            (SA8589) - Background BSR Polling? n
        (SA8608) - Increase Crisis Alert Buttons? n
            (SA8621) - SCH Feature Enhancements? n
```

## 5.4. Administer Operator Stations

Use the “change station n” command, where “n” is the first operator station extension, in this case “45001”.

Enable **IP SoftPhone**, to allow for a virtual IP softphone to be registered against the station. Note the value of **Security Code**, which will be used later to configure Manitou.

change station 45001		Page	1 of	4
STATION				
Extension: 45001	Lock Messages? n	BCC: 0		
Type: 1608	<b>Security Code: 12345</b>	TN: 1		
Port: S00000	Coverage Path 1: 1	COR: 1		
Name: Bold Operator #1	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 45001			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>			
	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			

Repeat this section to administer all operator stations. In the compliance testing, two stations were administered as shown below.

list station 45001 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
<b>45001</b>	<b>S00000</b>	<b>Bold Operator #1</b>			<b>1</b>	<b>1</b>			
	<b>1608</b>		<b>no</b>			<b>1</b>	<b>1</b>		
<b>45002</b>	<b>S00045</b>	<b>Bold Operator #2</b>			<b>1</b>	<b>1</b>			
	<b>9611</b>		<b>no</b>			<b>1</b>	<b>1</b>		



## 6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Obtain Tlink name
- Administer Bold user
- Enable ports

### 6.1. Launch OAM Interface

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

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form includes the text "Please login here:" followed by "Username" and "Password" labels, each next to a text input field. Below the input fields is a blue "Login" button. At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot shows 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 the user. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining that the OAM Web provides tools for managing the AE Server and listing the administrative domains it covers: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be managed by a single administrator or separate administrators.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 18 07:43:33 MDT 2013

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 all domains, or a separate administrator for each domain.

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in with the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" title and provides instructions for setting up and maintaining the WebLM, including the need to use the WebLM Server Address and WebLM Server Access. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the Reserved Licenses option.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 18 07:43:33 MDT 2013

Home | Help | Logout

Licensing

▸ AE Services  
▸ Communication Manager Interface  
▾ Licensing  
    WebLM Server Address  
    WebLM Server Access  
    Reserved Licenses  
▸ Maintenance  
▸ Networking  
▸ Security

**Licensing**

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

- WebLM Server Address

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


- WebLM Server Access

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

- Reserved Licenses

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

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for monitoring and call control via DMCC, and the DMCC license is used for the virtual IP softphones.



Web License Manager (WebLM v6.2)

Help | About | Change Password | Log off

WebLM Home

Install license

Licensed products

APPL\_ENAB

▼ Application\_Enablement

View license capacity

View peak usage

Uninstall license

Server properties

Manage users

Shortcuts

Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

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

License installed on: May 11, 2012 6:07:47 PM -05:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_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_AES_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;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0

### 6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" table with one link listed. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	4	Both

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 "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area contains a form with the following fields: "Link" (set to 2), "Switch Connection" (set to S8300D), "Switch CTI Link Number" (set to 1), "ASAI Link Version" (set to 4), and "Security" (set to Unencrypted). At the bottom of the form are buttons for "Apply Changes" and "Cancel Changes".



## 6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “S8300D”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. Two connections are listed: S8300D and S8800. The S8300D connection is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	1
<input type="radio"/> S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as the H.323 gatekeeper, in this case “10.32.39.83” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - S8300D' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.32.39.83' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons.

## 6.5. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services', both of which are unchecked. An 'Apply Changes' button is located below the checkboxes. The top right corner displays user information: 'Welcome: User', 'Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes\_125\_72/10.64.125.72', 'Server Offer Type: VIRTUAL\_APPLIANCE', 'SW Version: r6-2-0-18-0 Patch 1', and 'Server Date and Time: Mon Mar 18 07:43:33 MDT 2013'. The top navigation bar includes 'Security | Security Database | Control' and links for 'Home | Help | Logout'.

## 6.6. Restart Services

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'DMCC Service' and 'TSAPI Service' checked. Below the table, there is a link 'For status on actual services, please use [Status and Control](#)'. At the bottom, there are buttons for 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right corner displays user information: 'Welcome: User', 'Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes\_125\_72/10.64.125.72', 'Server Offer Type: VIRTUAL\_APPLIANCE', 'SW Version: r6-2-0-18-0 Patch 1', and 'Server Date and Time: Mon Mar 18 07:43:33 MDT 2013'. The top navigation bar includes 'Maintenance | Service Controller' and links for 'Home | Help | Logout'.

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

## 6.7. 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, to be used later for configuring Manitou.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES2-S8800”. Note the use of the switch connection “S8300D” from **Section 6.3** as part of the Tlink name.

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 the user. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. The Security Database is expanded, showing sub-items like Control, CTI Users, Devices, Device Groups, and Tlinks. The main content area shows the Tlinks page with a list of three Tlink names: AVAYA#S8300D#CSTA#AES\_125\_72 (selected), AVAYA#S8800#CSTA#AES\_125\_72, and AVAYA#S8800#CSTA-S#AES\_125\_72. A "Delete Tlink" button is visible below the list.

Welcome: User  
Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 18 07:43:33 MDT 2013

Security | Security Database | Tlinks

Home | Help | Logout

**Tlinks**

Tlink Name

- ☒ AVAYA#S8300D#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA#AES\_125\_72
- ☐ AVAYA#S8800#CSTA-S#AES\_125\_72

Delete Tlink

## 6.8. Administer Bold User

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

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

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 the user. The left navigation pane shows a tree structure with 'User Management' expanded, leading to 'User Admin' and then 'Add User'. The main content area is titled 'Add User' and contains a form with various fields. Fields marked with an asterisk (\*) are required. The 'CT User' field is a dropdown menu set to 'Yes'. The 'Avaya Role' field is a dropdown menu set to 'None'. The 'User Password' and 'Confirm Password' fields are masked with dots. The 'Admin Note' field is a text area. The 'Business Category', 'Car License', 'CM Home', 'Css Home', 'Department Number', 'Display Name', 'Employee Number', 'Employee Type', and 'Enterprise Handle' fields are text boxes.

Welcome: User  
Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 18 07:43:33 MDT 2013

User Management | User Admin | Add User Home | Help | Logout

**Add User**

Fields marked with \* can not be empty.

\* User Id   
\* Common Name   
\* Surname   
\* User Password   
\* Confirm Password   
Admin Note   
Avaya Role   
Business Category   
Car License   
CM Home   
Css Home   
CT User   
Department Number   
Display Name   
Employee Number   
Employee Type   
Enterprise Handle



## 6.9. Enable Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Mar 18 07:29:20 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 18 07:43:33 MDT 2013

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

## 7. Configure Bold Technologies Manitou

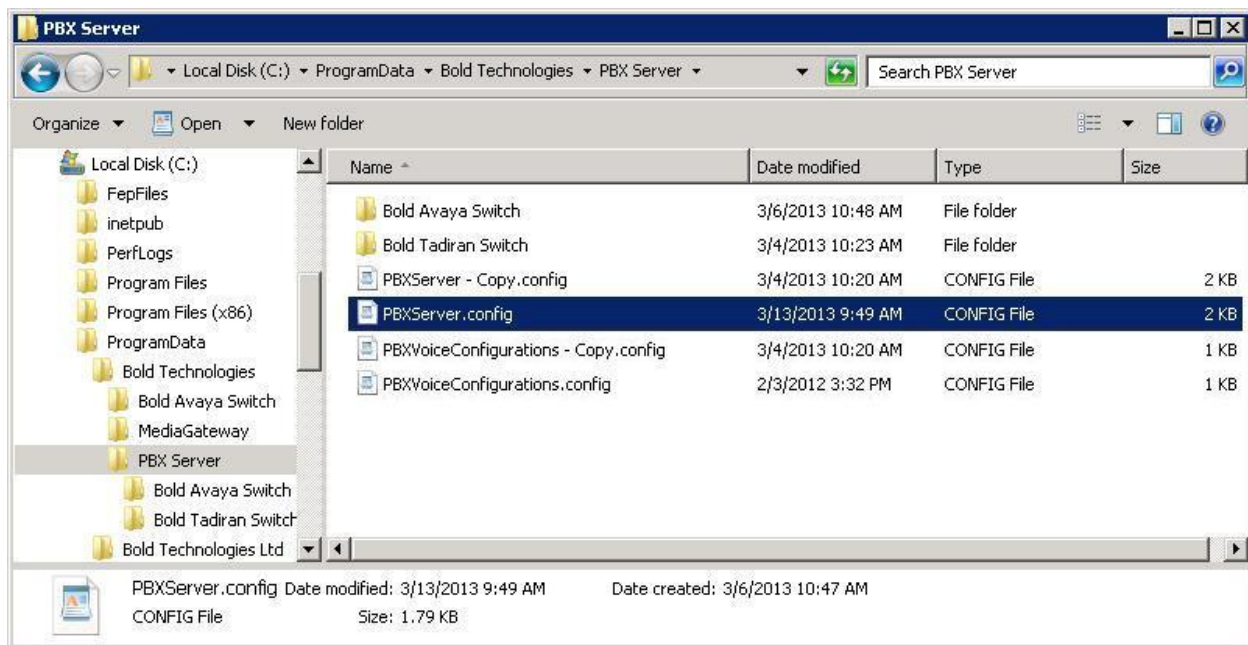
This section provides the procedures for configuring Manitou. The procedures include the following areas:

- Administer PBX server
- Administer Avaya switch
- Administer extensions

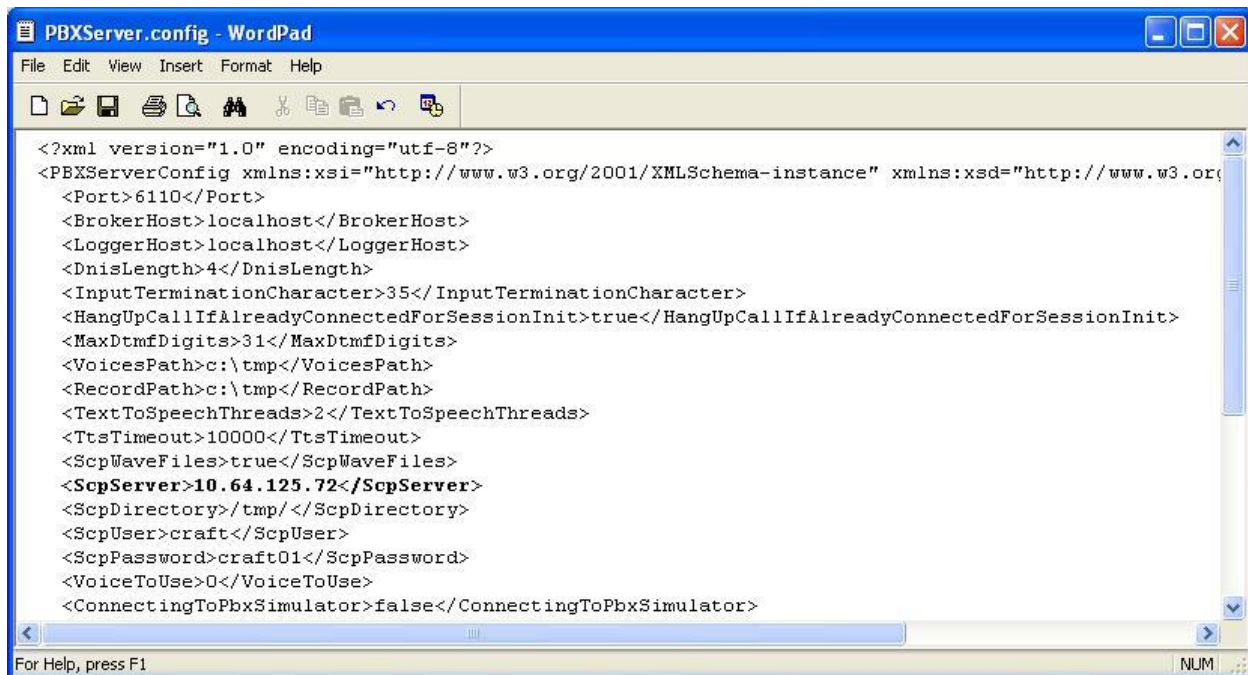
The configuration of Manitou is performed by Bold Technologies technicians. The procedural steps are presented in these Application Notes for informational purposes.

### 7.1. Administer PBX Server

From the Manitou server running the PBXServer component, navigate to the **C:\ProgramData\Bold Technologies\PBX Server** directory to locate the **PBXServer.config** file shown below.

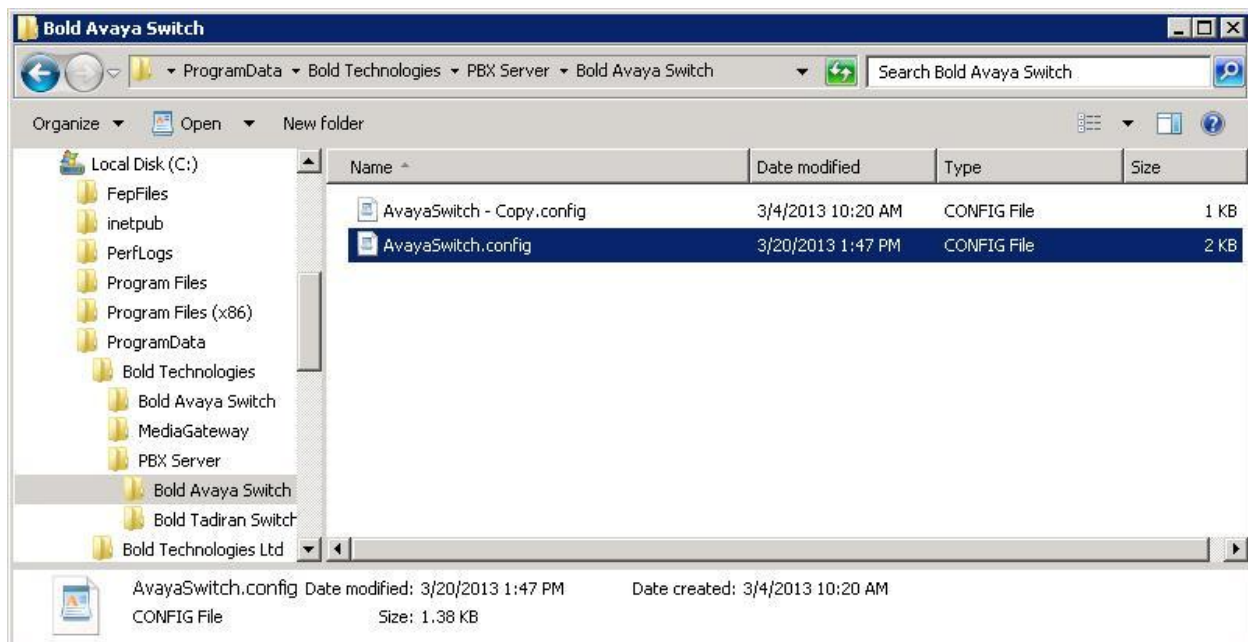


Open the **PBXServer.config** file with the WordPad application. Navigate to the **ScpServer** parameter, and set the value to the IP address of Application Enablement Services, as shown below. Retain the default values in the remaining fields.



## 7.2. Administer Avaya Switch

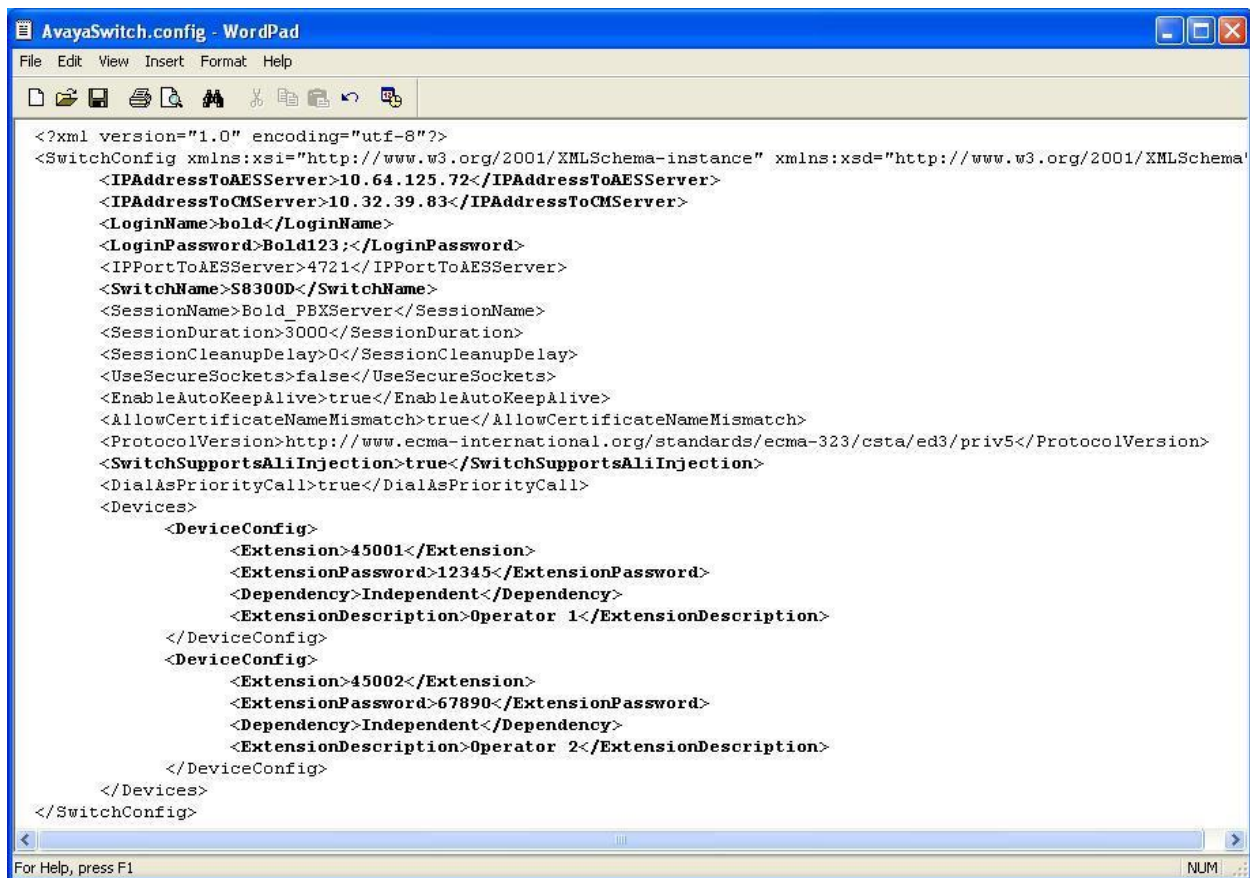
From the Manitou server running the PBXServer component, navigate to the **C:\ProgramData\Bold Technologies\PBX Server\Bold Avaya Switch** directory to locate the **AvayaSwitch.config** file shown below.



Open the **AvayaSwitch.config** file with the WordPad application. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **IPAddressToAESServer:** IP address of Application Enablement Services.
- **IPAddressToCMServer:** IP address of H.323 gatekeeper from **Section 6.4**.
- **LoginName:** The Bold user credential from **Section 6.8**.
- **LoginPassword:** The Bold user credential from **Section 6.8**.
- **SwitchName:** Switch connection name from **Section 6.3**.
- **SwitchSupportsAliInjection:** "true"

For each operator station from **Section 5.4**, create a virtual IP softphone device in the **DeviceConfig** subsection as shown below. For **Extension** and **ExtensionPassword**, use the operator station extension and security code from **Section 5.4**. Use "Independent" for **Dependency**, and enter a desired description for **ExtensionDescription**.



```
<?xml version="1.0" encoding="utf-8"?>
<SwitchConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <IPAddressToAESServer>10.64.125.72</IPAddressToAESServer>
  <IPAddressToCMServer>10.32.39.83</IPAddressToCMServer>
  <LoginName>bold</LoginName>
  <LoginPassword>Bold123</LoginPassword>
  <IPPortToAESServer>4721</IPPortToAESServer>
  <SwitchName>S8300D</SwitchName>
  <SessionName>Bold_PBXServer</SessionName>
  <SessionDuration>3000</SessionDuration>
  <SessionCleanupDelay>0</SessionCleanupDelay>
  <UseSecureSockets>>false</UseSecureSockets>
  <EnableAutoKeepAlive>true</EnableAutoKeepAlive>
  <AllowCertificateNameMismatch>true</AllowCertificateNameMismatch>
  <ProtocolVersion>http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5</ProtocolVersion>
  <SwitchSupportsAliInjection>true</SwitchSupportsAliInjection>
  <DialAsPriorityCall>true</DialAsPriorityCall>
  <Devices>
    <DeviceConfig>
      <Extension>45001</Extension>
      <ExtensionPassword>12345</ExtensionPassword>
      <Dependency>Independent</Dependency>
      <ExtensionDescription>Operator 1</ExtensionDescription>
    </DeviceConfig>
    <DeviceConfig>
      <Extension>45002</Extension>
      <ExtensionPassword>67890</ExtensionPassword>
      <Dependency>Independent</Dependency>
      <ExtensionDescription>Operator 2</ExtensionDescription>
    </DeviceConfig>
  </Devices>
</SwitchConfig>
```

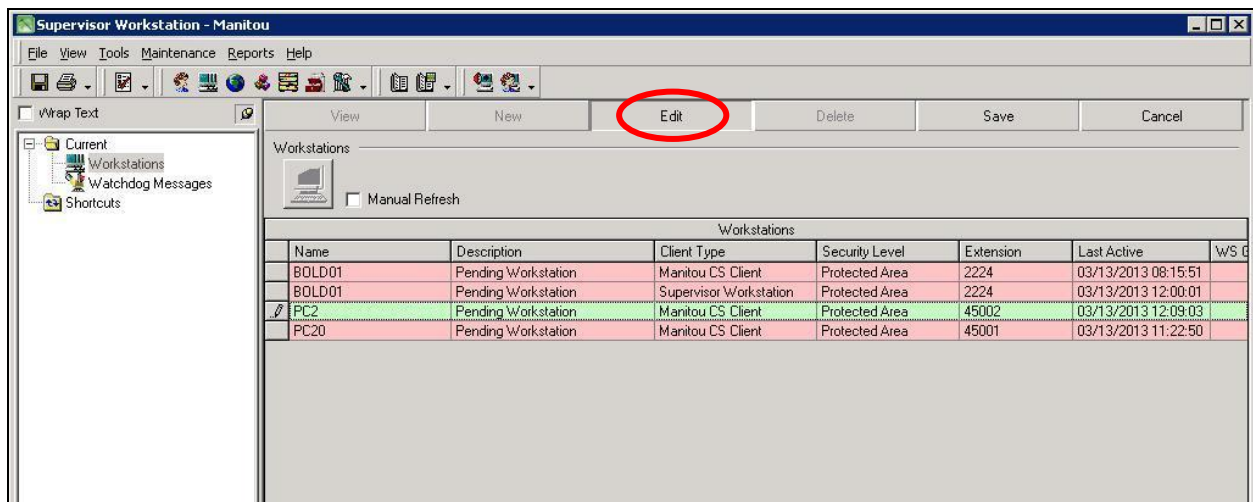
### 7.3. Administer Extensions

From the Manitou server running the ManitouCS Supervisor Application, select **Start → All Programs → Bold Technologies → Supervisor Workstation** to launch the application, and log in using the appropriate credentials.

The **Supervisor Workstation – Manitou** screen is displayed. Select **Maintenance → Workstations** from the top menu, to display the updated screen below.

Select a workstation entry that corresponds to an operator, in this case **PC2**. Click **Edit** toward the top of the screen.

In the workstation entry, click on the **Extension** field and enter the corresponding operator station extension from **Section 5.4**, in this case “45002”. Repeat this section for all operator workstations.





## 8. Verification Steps

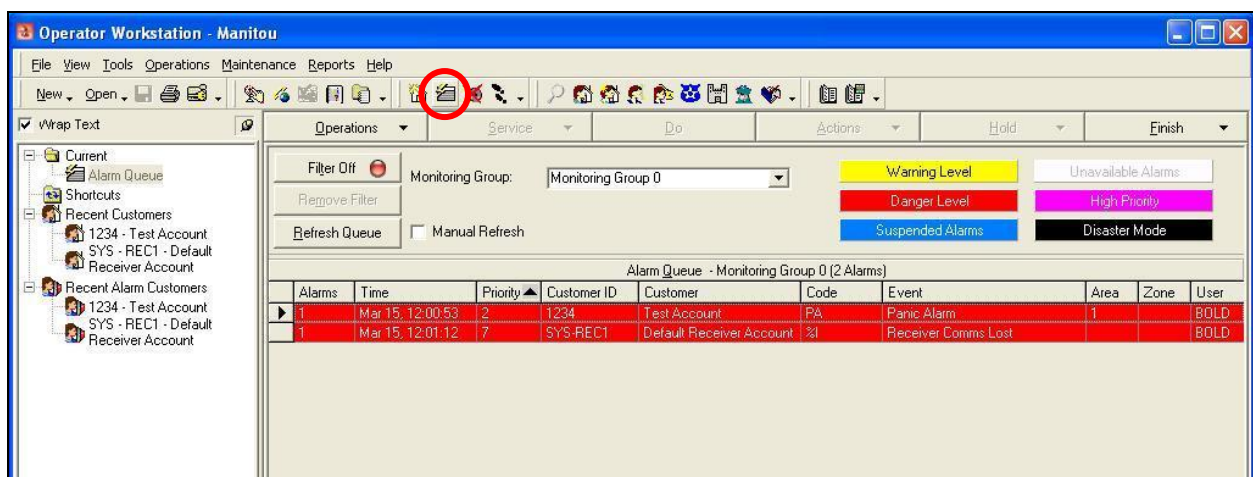
This section provides the tests that can be performed to verify proper configuration of Manitou, Communication Manager, and Application Enablement Services.

### 8.1. Verify Bold Technologies Manitou

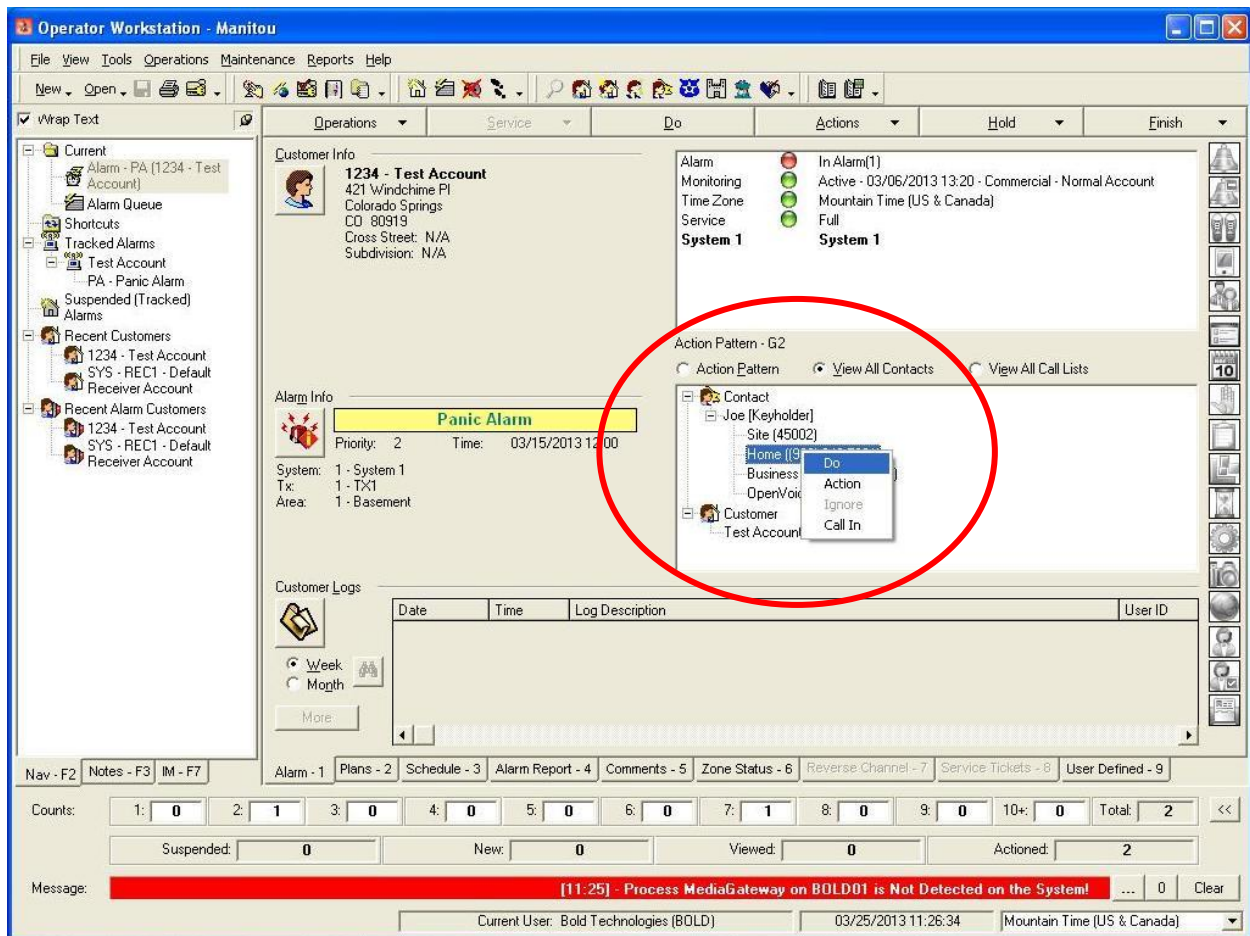
From the operator PC running the ManitouCS Operator Workstation application, select **Start → All Programs → Bold Technologies → Manitou Workstation** to launch the application, and log in using the appropriate credentials.



The **Operator Workstation - Manitou** screen is displayed. Select the **Alarm Queue** icon from the top menu to display a list of outstanding alarms, as shown below. Double click on an alarm entry.



The screen is updated with the details of the alarm and associated customer information. Select **View All Contacts**, and expand the **Contact** listing. Right click on a contact entry and select **Do**, as shown below.



Verify that the **Auto-Dialer** screen is displayed, and that the **Status** is “Dialing”, as shown below. Also verify that the call is ringing at the PSTN destination.



Answer the call at the PSTN. Verify that the **Auto-Dialer** screen is updated with **Status** of “Connected”, and that the operator station is connected to the PSTN user with two-way talk paths.





From the **Operator Workstation – Manitou** screen, select the **Monitoring Company Maintenance** icon from the top menu, to display the details of the monitoring company.

Verify that the display of the connected PSTN telephone shows the calling number shown below in the **ALI Injection** field.

The screenshot shows the 'Operator Workstation - Manitou' application window. The top menu bar includes 'File', 'View', 'Tools', 'Operations', 'Maintenance', 'Reports', and 'Help'. The 'Maintenance' menu is open, and the 'Monitoring Company Maintenance' icon is circled in red. The main window displays the details for a monitoring company. The 'Name' section shows 'Company ID: 1' and 'Name: Central Station'. The 'Address' section includes fields for 'Street 1', 'Street 2', 'City', 'State', 'Zip Code', 'Country' (United States of America), 'Language' (English (United States)), and 'Time Zone' (Mountain Time (US & Canada)). The 'Contact' section has a dropdown for 'ALI Injection' set to '(719) 555-4444', which is circled in red. Other contact fields include 'Site', 'Home', and 'Business'. The 'E-mail' section has an 'E-Mail' dropdown and a 'PDF' button. The 'Web' section has a 'Web Address' field. On the right, a 'Jump To:' list includes 'Monitoring Compar', 'Contact List', 'Call Lists', 'Comments', 'Action Patterns', 'General Schedule', 'Reverse Command', 'TX ID Ranges', 'Billing Charges', 'Billing Rates', 'Reports', 'Maintenance Issur', and 'Statistics'. At the bottom, there are 'Counts' for various statuses (1: 0, 2: 1, 3: 0, 4: 0, 5: 0, 6: 0, 7: 1, 8: 0, 9: 0, 10: 0, Total: 2), 'Suspended: 0', 'New: 0', 'Viewed: 0', 'Actioned: 2', and a 'Message:' field. The status bar at the bottom shows 'Current User: Bold Technologies (BOLD)', '03/18/2013 07:36:46', and 'Mountain Time (US & Canada)'.

## 8.2. Verify Avaya Aura® Communication Manager

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 CTI link administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
<b>1</b>	<b>4</b>	<b>no</b>	<b>aes_125_72</b>	<b>established</b>	<b>23</b>	<b>21</b>

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that there is a virtual IP softphone entry for each operator station that is active on an outbound call, as shown below.

```
list registered-ip-stations
```

Page 1

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
45000	9650	IP_Phone	y	10.32.39.104	
	1	3.105S		10.32.39.83	
45001	1608	IP_Phone	y	10.32.39.105	
	1	1.302S		10.32.39.83	
<b>45001</b>	<b>1608</b>	<b>IP_API_A</b>	<b>y</b>	<b>10.64.125.72</b>	
	<b>1</b>	<b>3.2040</b>		<b>10.32.39.83</b>	
45002	9611	IP_Phone	y	10.32.39.106	
	1	6.2209		10.32.39.83	

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

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 that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, as shown below. Also verify that the corresponding **Associations** column reflects the number of active virtual IP softphones from **Section 8.2**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Mon Mar 25 11:35:48 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0 Patch 1  
Server Date and Time: Mon Mar 25 11:52:34 MDT 2013

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

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
○	1	S8800	2	Talking	Wed Mar 13 07:21:28 2013	Online	16	0	15	15	30
●	2	S8300D	1	Talking	Mon Mar 25 11:04:18 2013	Online	16	1	21	23	30


OnlineOffline

For service-wide information, choose one of the following:

TSAPI Service StatusTLink StatusUser Status

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

In the lower portion of the screen, verify that the **User** column shows an active session with the Bold user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of active virtual IP softphones from **Section 8.2**.



## Application Enablement Services

### Management Console

Welcome: User

Last login: Mon Mar 25 11:35:48 2013 from 10.32.39.20

Number of prior failed login attempts: 0

HostName/IP: aes\_125\_72/10.64.125.72

Server Offer Type: VIRTUAL\_APPLIANCE

SW Version: r6-2-0-18-0 Patch 1

Server Date and Time: Mon Mar 25 11:51:40 MDT 2013

Status | Status and Control | **DMCC Service Summary**
Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ **Status**

Alarm Viewer

▶ Logs

▼ **Status and Control**

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ **DMCC Service Summary**

▪ Switch Conn Summary

▪ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

### DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Mon Mar 25 11:51:40 MDT 2013

Service Uptime: 12 days, 4 hours 29 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 22

Number of Existing Devices: 1

Number of Devices Created Since Service Boot: 242

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	DBF3233129A1622A6 CF7575237D60058-21	bold	Bold_PBXServer	20.32.39.190	XML Unencrypted	1

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1

## 9. Conclusion

These Application Notes describe the configuration steps required for Bold Technologies Manitou to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 1, July 2012, available at <http://support.avaya.com>.
3. *Bold Technologies Manitou CS Operator Workstation*, Manitou CS 1.6.0, February 2013, available at <http://support.boldgroup.com>.

---

**©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](mailto:devconnect@avaya.com).