



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Computer Instruments Screen Pop Premium (SPP), with Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Computer Instruments Screen Pop Premium to integrate with Avaya Aura® Application Enablement Services to monitor and control Avaya 9600 series telephones.

Computer Instruments Screen Pop Premium is a client/server system that allows users to manage and track information related to a particular caller (ANI). SPP can keep track of callers contact information, document history, emails, and appointments.

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 procedure for configuring Computer Instruments Screen Pop Premium to interoperate with Avaya Aura® Application Enablement Services. Screen Pop Premium is a client/server system that allows users to manage and track information related to a particular caller (ANI). When a call comes to a user via the SPP screen pop, a collection of data is made available for that caller. The data is sent to the client PC as part of the call notification. Information collected and stored includes document and call history. All documents that have been associated with the caller are made readily available to the user the moment the call is received. In addition, the Outlook integration organizes emails and appointments associated with the caller so that the user can easily find information. The client program communicates with the SPP server via a socket connection, and the server interacts with the TSAPI client to both receive events and initiate call functions.

These Application Notes assume that the pre-requisites in **Section 5** have been met prior to configuring the Avaya Application Enablement Services. Only steps relevant to this compliance test are described in this document.

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

The general test approach included verification of a successful integration of the SPP server application with Application Enablement Services and Avaya 9600 Telephones. Modifications were made using the SPP client GUI and verified by placing calls to the configured extensions associated with the SPP application.

The following scenarios were used to verify SPP functionality:

- Inbound calls
- Hold / Resume
- Call termination (origination/destination)
- Buddy Transfer
- Contact Information
- Document History
- Emails
- Appointments

2.2. Test Results

Computer Instruments SPP successfully passed the compliance testing.

2.3. Support

Technical support for the SPP solution can be obtained by contacting Computer Instruments:

- URL – support@instruments.com
- Phone – (888) 451-0851 and option 2

3. Reference Configuration

Figure 1 illustrates the reference configuration used during testing. In the reference configuration, the SPP application was integrated with Avaya Aura® Application Enablement Services and Avaya 9600 IP Telephones. Configuration for the SPP application was performed using the SPP client GUI and verification was done by placing calls to the associated extensions. Calls were placed both internally and externally, along with email, contact, and document verification.

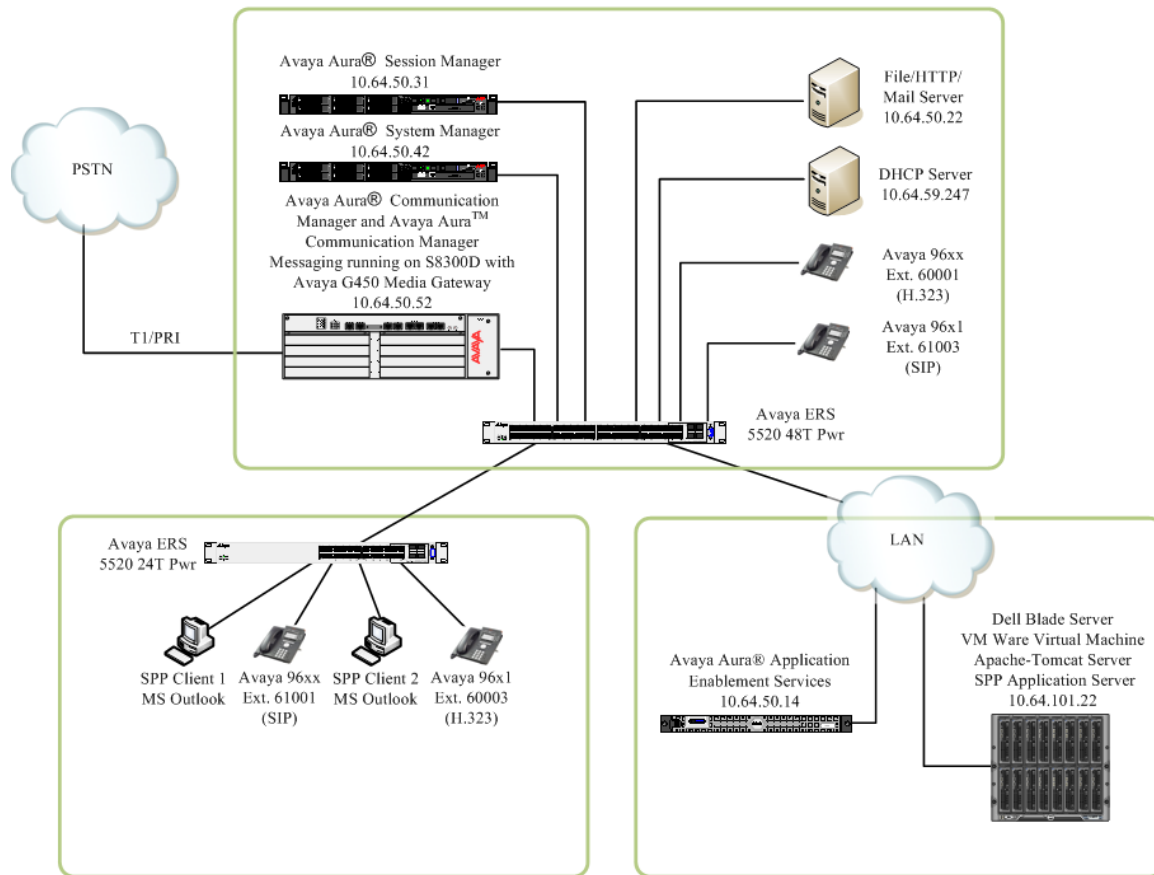


Figure 1: Test Configuration of SPP

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0.1 with SP5.0.1(Patch 19303)
Avaya G450 Media Gateway MGP MM710 T1 Module MM711 Analog Module MM712 DCP Media Module MP80 VoIP-DSP	HW 2 FW 31.20.0 HW 5 FW 22 HW 23 FW 73 HW 7 FW 14 HW 6 FW 67
<i>Avaya Aura® Session Manager</i>	
Avaya Aura® Session Manager HP Proliant DL360 G7	6.1 with SP5
Avaya Aura® System Manager HP Proliant DL360 G7	6.1 with SP5
<i>Avaya Aura® Application Enablement Services</i>	
Avaya Application Enablement Services Dell Power Edge R610	r6-1-2-32-0
<i>Avaya Telephony Sets</i>	
Avaya 96xx Series IP Telephones	(H.323 3.1SP2), (SIP 2.6.6.0)
Avaya 96x1 Series IP Telephones	(H.323 S6.010f), (SIP 6.0.3)
<i>CII Screen Pop Premium (SPP)</i>	
Windows Server 2008 R2 Enterprise SP1 VM Ware Virtual Machine	
SPP Server	eCI Server
SPP Client GUI	2.1.15.0
TSAPI Client	6.1.1.469

5. Pre-requisite Configuration

The following components must be installed and running in order for the SPP application to function properly. This configuration should be done by the CII support team.

- eCI Server must be installed and enabled as a Windows service on the server machine. deployed

6. Configure Avaya Aura® Application Enablement Services

This section describes the Application Enablement Services configuration to support the network shown in **Figure 1**.

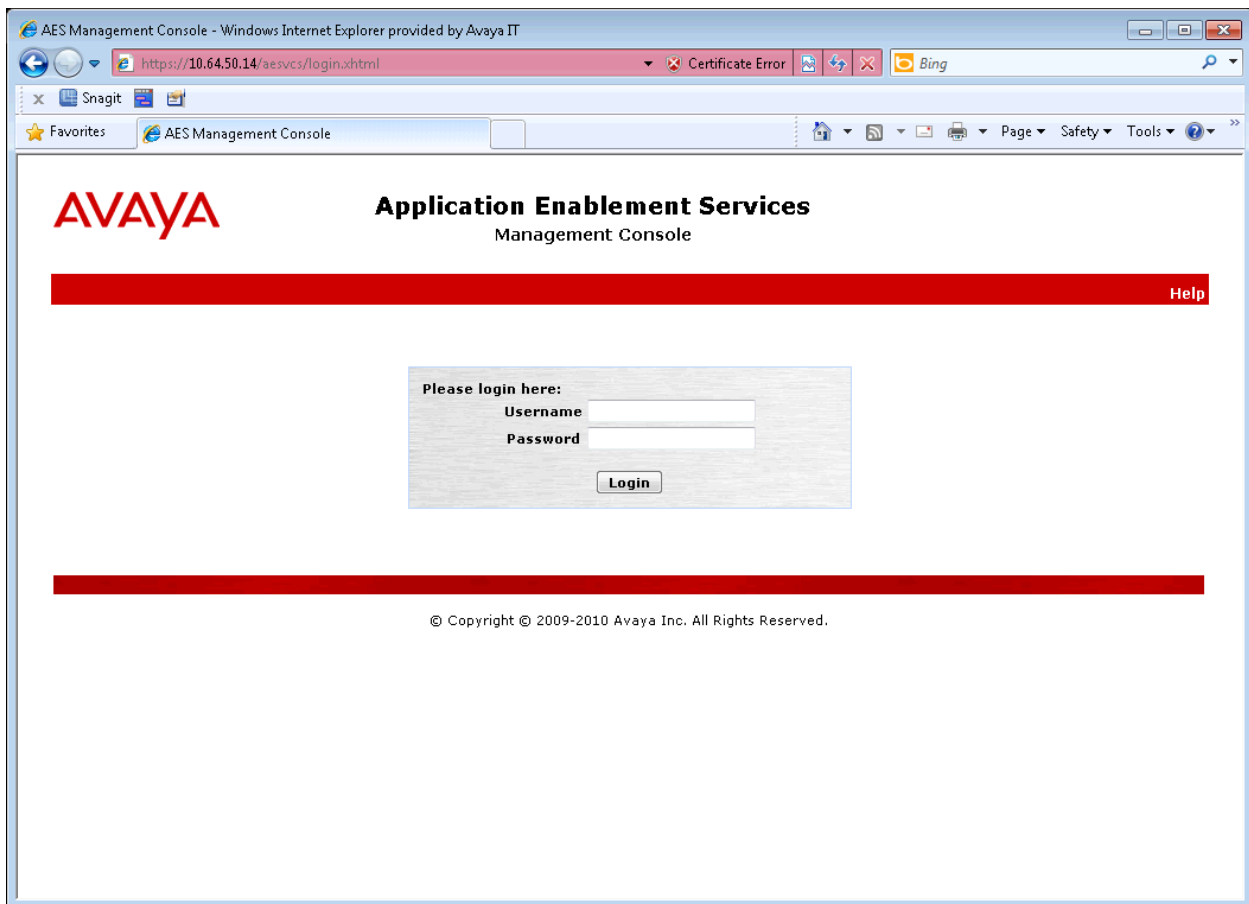
Configuration of Application Enablement Services was performed using a web browser.

Application Enablement Services configuration includes the following:

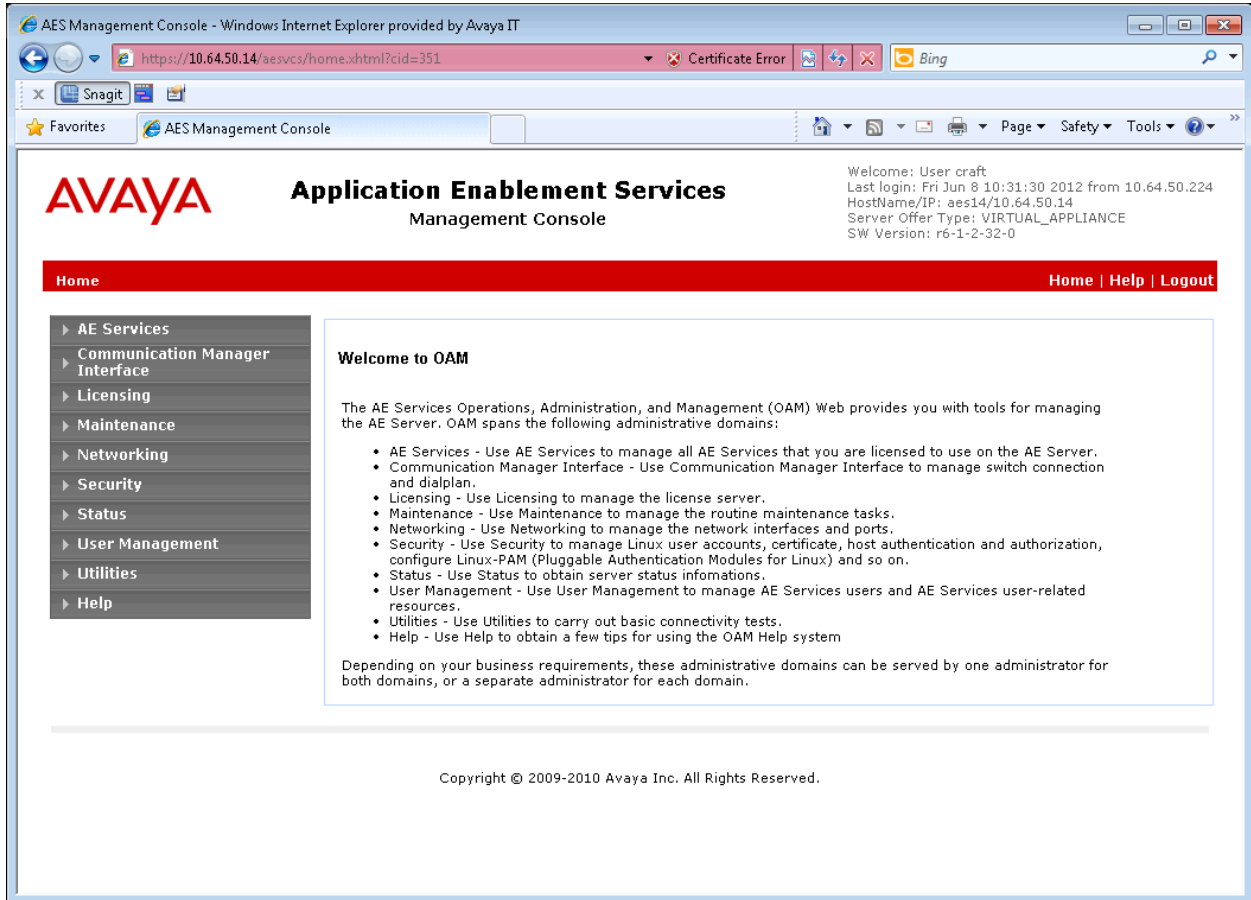
- Communication Manager Interface
- AE Services
- User Management
- Security

6.1. Communication Manager Interface

From a PC open a web browser and enter the URL for Application Enablement Services and login with the proper credentials.



Upon successful login, the following page should be displayed. From the left pane select **Communication Manager Interface** → **Switch Connections**.



Add a name for the connection and click the **Add Connection** button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Fri Jun 8 10:31:30 2012 from 10.64.50.224
HostName/IP: aes14/10.64.50.14
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
cm5052	Yes	30	1

cmSPP Add Connection

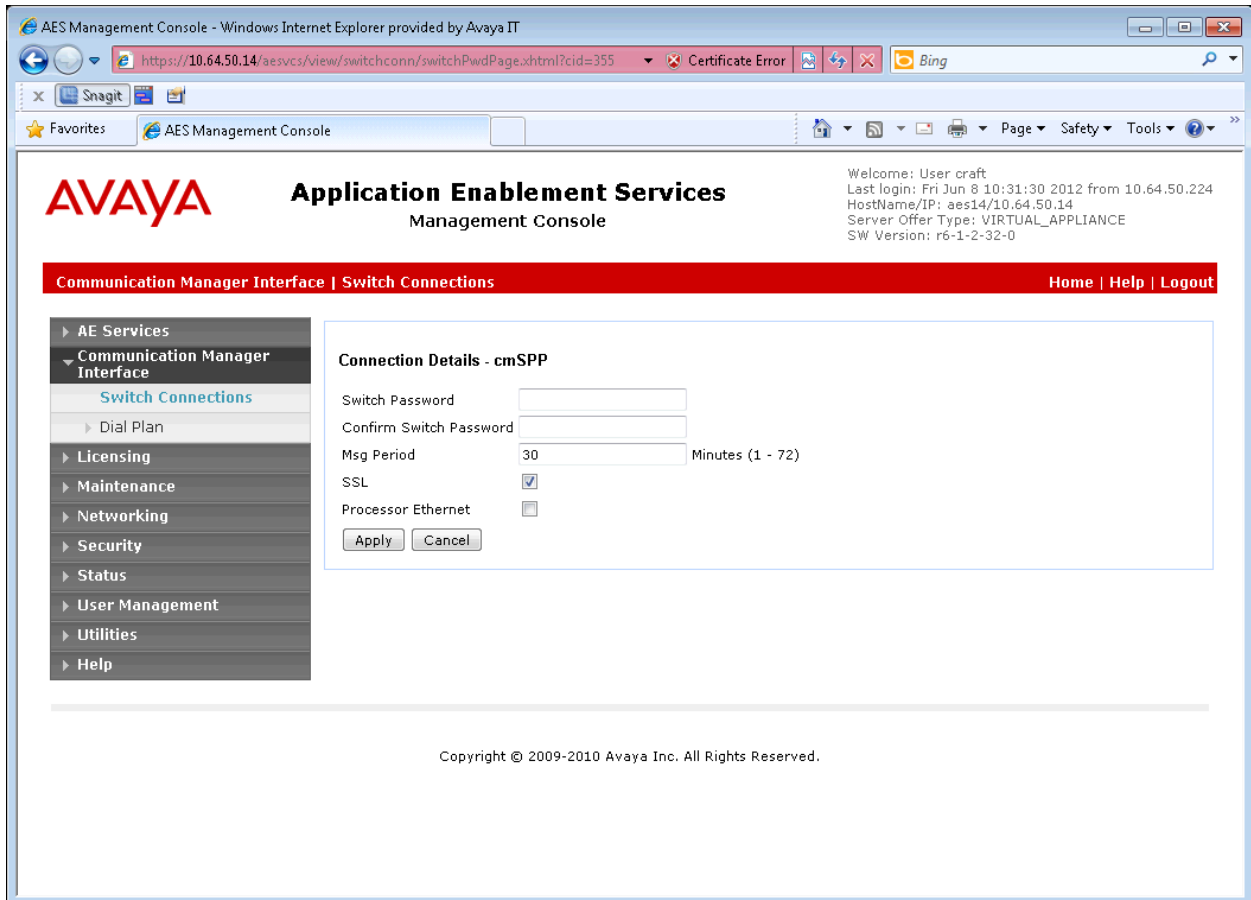
Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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

Enter the password for connecting to the Communication Manager.

Note: This password is configured on the *ip-services* form in Communication Manager.

Click **Apply**.



You should now see your new entry in the list.

From the list select your new connection and click the **Edit PE/CLAN IPs** button.

The screenshot shows the Avaya AES Management Console interface. The page title is "Application Enablement Services Management Console". The user is logged in as "User craft". The page displays the "Switch Connections" section, which includes a table of connections and several action buttons.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm5052	Yes	30	1
<input type="radio"/> cmSPP	No	30	0

Buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, Delete Connection, Survivability Hierarchy

Enter the IP Address or FQDN of the Communication Manager and click the **Add Name or IP** button.

The screenshot shows the Avaya AES Management Console interface in a Windows Internet Explorer browser. The browser address bar shows the URL: `https://10.64.50.14/aesvcs/view/switchconn/switchClansPage.xhtml?cid=359`. The page title is "AES Management Console - Windows Internet Explorer provided by Avaya IT".

The main content area displays the "Application Enablement Services Management Console" logo and navigation menu. The left sidebar contains a tree view with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help.

The main content area is titled "Communication Manager Interface | Switch Connections" and includes a "Home | Help | Logout" link. Below this, there is a section titled "Edit CLAN IPs - cmSPP". This section contains a text input field, an "Add Name or IP" button, and a table with the following data:

Name or IP Address	Status
<input checked="" type="radio"/> 10.64.50.50	Idle

Below the table are "Delete IP" and "Back" buttons.

At the bottom of the page, the copyright notice reads: "Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

6.2. AE Services TSAPI Links

From the left pane select **AE Services** → **TSAPI** → **TSAPI Links**.

Click the **Add Link** button.

The screenshot shows the Avaya AES Management Console interface. The browser address bar indicates the URL: `https://10.64.50.14/aesvcs/view/tsapi/TSAPILinksPage.xhtml?cid=359`. The page title is "Application Enablement Services Management Console". A navigation bar at the top contains "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout".

The left sidebar shows a tree view with "AE Services" expanded, and "TSAPI" and "TSAPI Links" selected. The main content area displays a table of "TSAPI Links" with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm5052	1	4	Unencrypted

Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link".

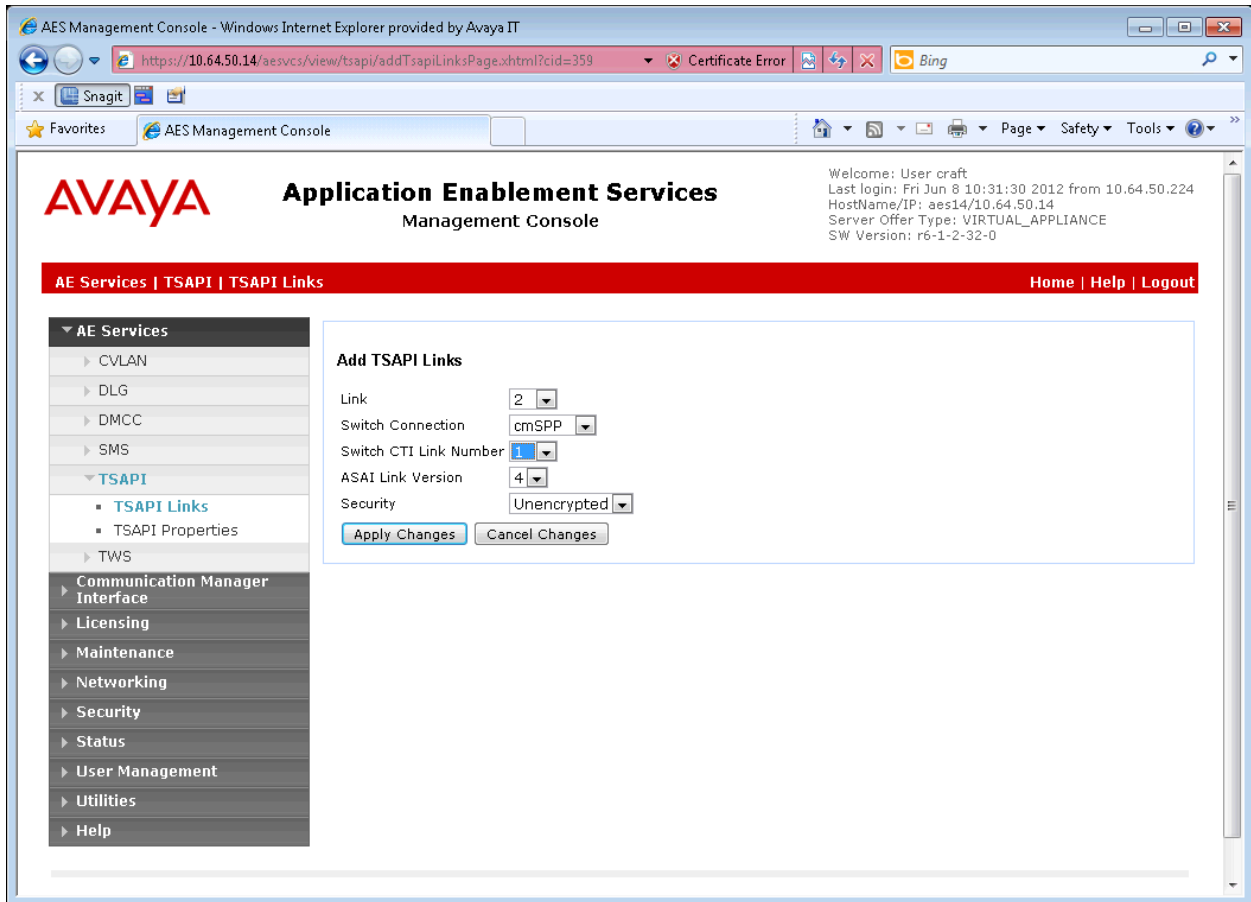
Select a number from the **Link** pull-down box to identify this link.

Select the connection configured in **Section 6.1** from the **Switch Connection** pull-down box.

Select the **Switch CTI Link Number** that corresponds to the CTI link number on the Communication Manager.

Remaining fields can use the default settings.

Click **Apply Changes**.

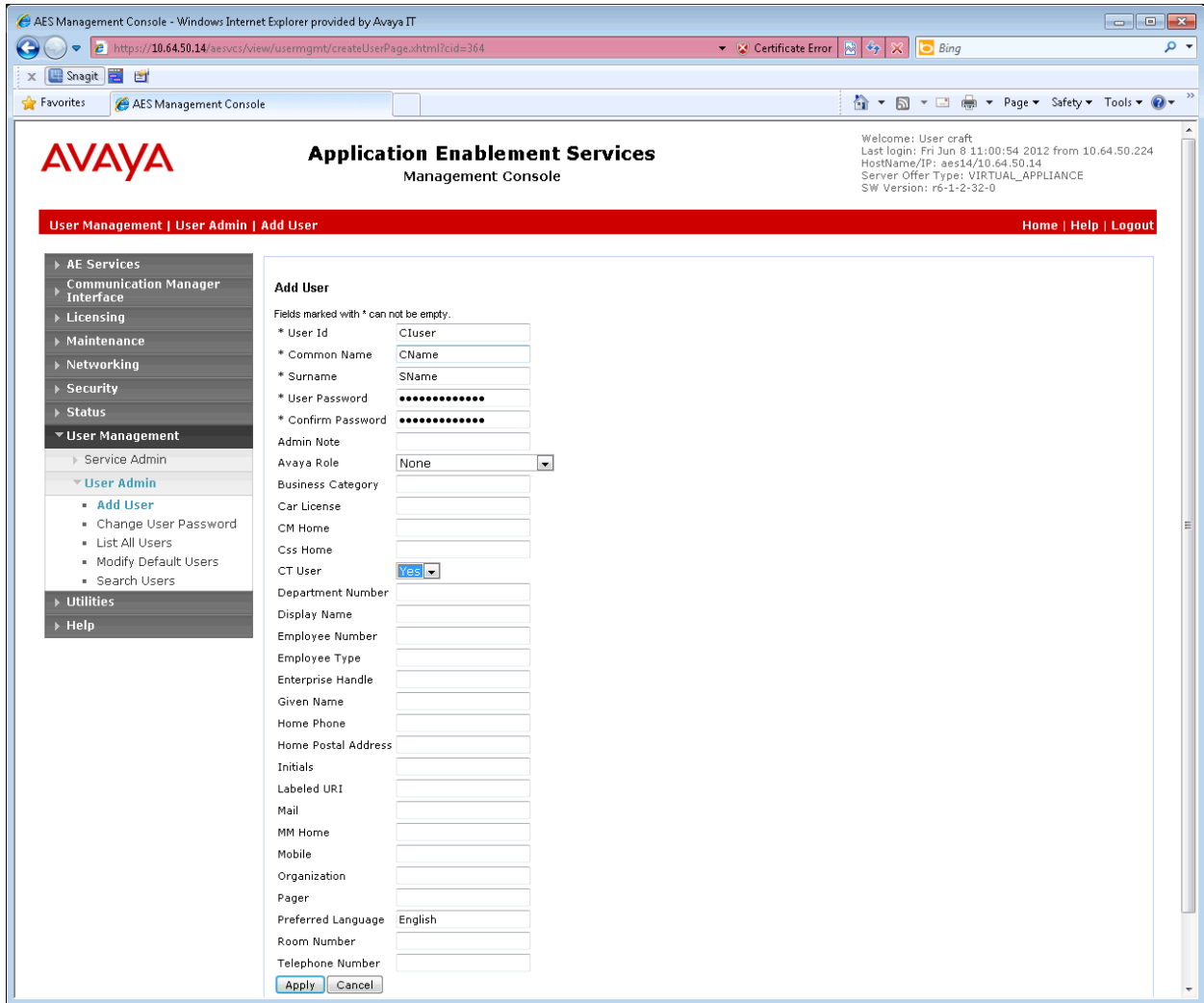


Note: Addition of a TSAPI link requires a restart of the TSAPI server. Follow on-screen instructions after applying changes to restart. (Not Shown)

6.3. User Management

From the left pane select **User Management** → **User Admin** → **Add User**.

Enter data for the required fields marked with an asterisk and select **Yes** for **CT User**. The **User Id** field will be used by the SPP Application server when connecting to Application Enablement Services.



6.4. Security

During the compliance test Unrestricted Access was allowed for the CTI User. Actual deployments may have a more detailed security policy.

From the left pane select **Security Database** → **CTI Users** → **List All Users**→.

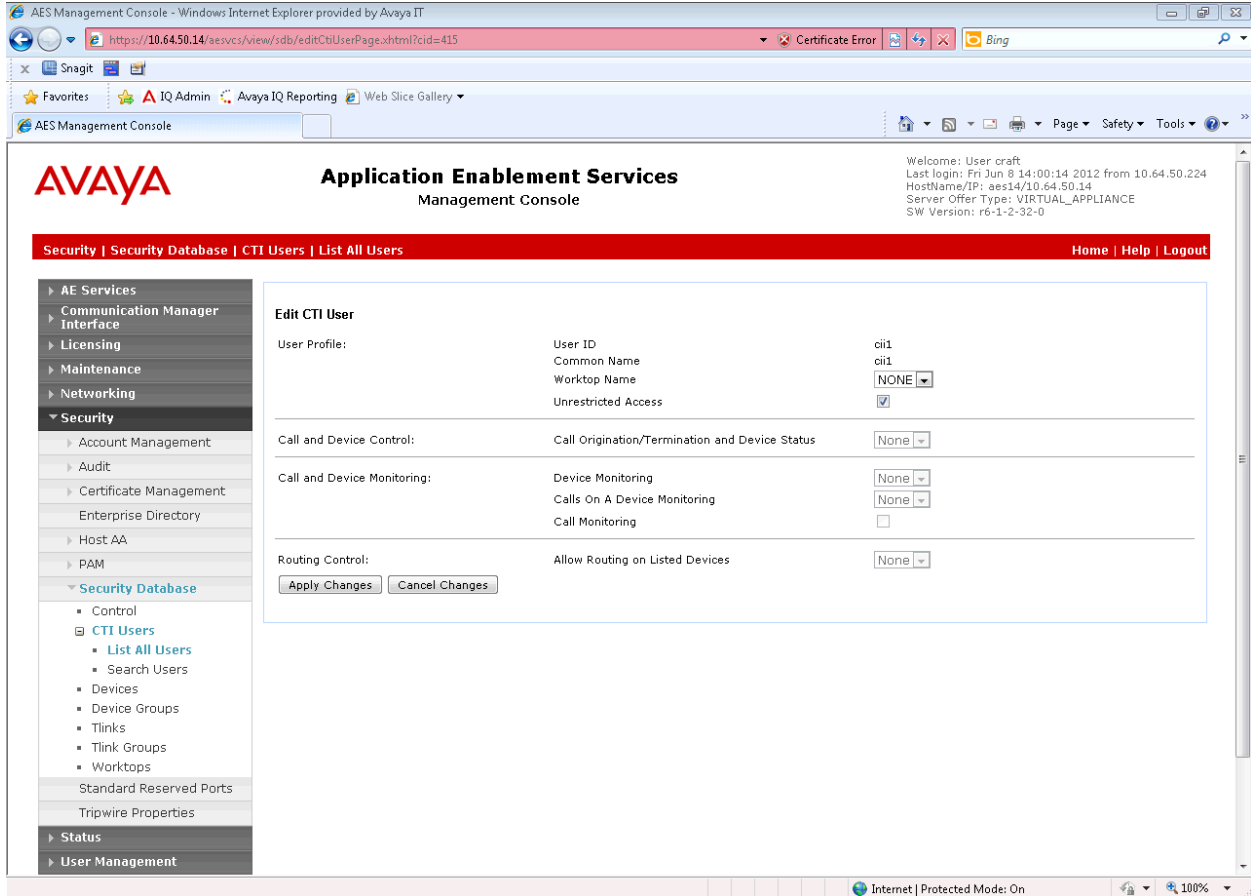
Select the desired user and click the **Edit** button.

The screenshot shows the Avaya Application Enablement Services Management Console. The browser address bar indicates the URL: <https://10.64.50.14/aesvcs/view/sdb/listCtiUsersPage.xhtml?cid=374>. The page title is "AVAYA Application Enablement Services Management Console". A welcome message is displayed: "Welcome: User craft, Last login: Fri Jun 8 11:00:54 2012 from 10.64.50.224, HostName/IP: aes14/10.64.50.14, Server Offer Type: VIRTUAL_APPLIANCE, SW Version: r6-1-2-32-0". The breadcrumb navigation is "Security | Security Database | CTI Users | List All Users". The left navigation pane shows the "Security Database" expanded to "CTI Users" and "List All Users" selected. The main content area displays a table of CTI Users:

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> cii1	cii1	NONE	NONE
<input type="radio"/> CUser	CName	NONE	NONE

Below the table are "Edit" and "List All" buttons. The footer of the page reads "Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

In the **User Profile:** section check the **Unrestricted Access** box.



Click **Apply Changes**.

7. Configure Screen Pop Premium

This section describes the Screen Pop Premium configuration to support the network shown in **Figure 1**.

7.1. Configure Server

Configuration of the Screen Pop Premium server was performed CII support personnel.

7.2. Configure Client

SPP Client GUI configuration includes the following:

- Start Client
- Configure Server Information
 - Server IP Address
 - My Extension
 - User ID
 - Minimum digits needed for pop-up

- Connect to Server

7.2.1. Start Client

On the Windows SPP Client PC double-click the NACT Client desktop shortcut (Not Shown) to start the client application. This action loads the SPP client into the Windows system tray (Not Shown).

7.2.2. Configure Server Information

From the Windows system tray, right-click the NACT Client icon and select **Configuration** (Not Shown) The following configuration window should be displayed:

Enter the **Server IP Address** of the SPP Server, a valid extension for the SPP Client to monitor in the **My Extension** field, and a **User ID**.

Default values for the remaining fields are acceptable.

Click **Save**.

Note: If *Minimum digits needed for pop-up* is left blank it will default to 5 after saving.

Configuration

Server Connection

Server IP Address: 10.64.101.22 Auto Connect

My Extension: 60003

User ID: User3

Outlook Configuration

User ID: Password:

Load appointments on call notification

Default Contact Manager

Microsoft Outlook ACT!
 Gold Mine

Desktop Options

Open Documents automatically upon call notification
 Open Call Form on Answer (default is ON Ring)

Phone Pad Options

Display Phonepad on Ring Do not display Phonepad
 Display Phonepad on Answer

Backup Extension:

Transfer to backup if on a call

Transfer Message:

Minimum digits needed for pop-up: 5

Save Cancel

Note: After clicking the Save button click OK when you see the following warning.

NACTInterface

Could not save configuration to server. Check connection status

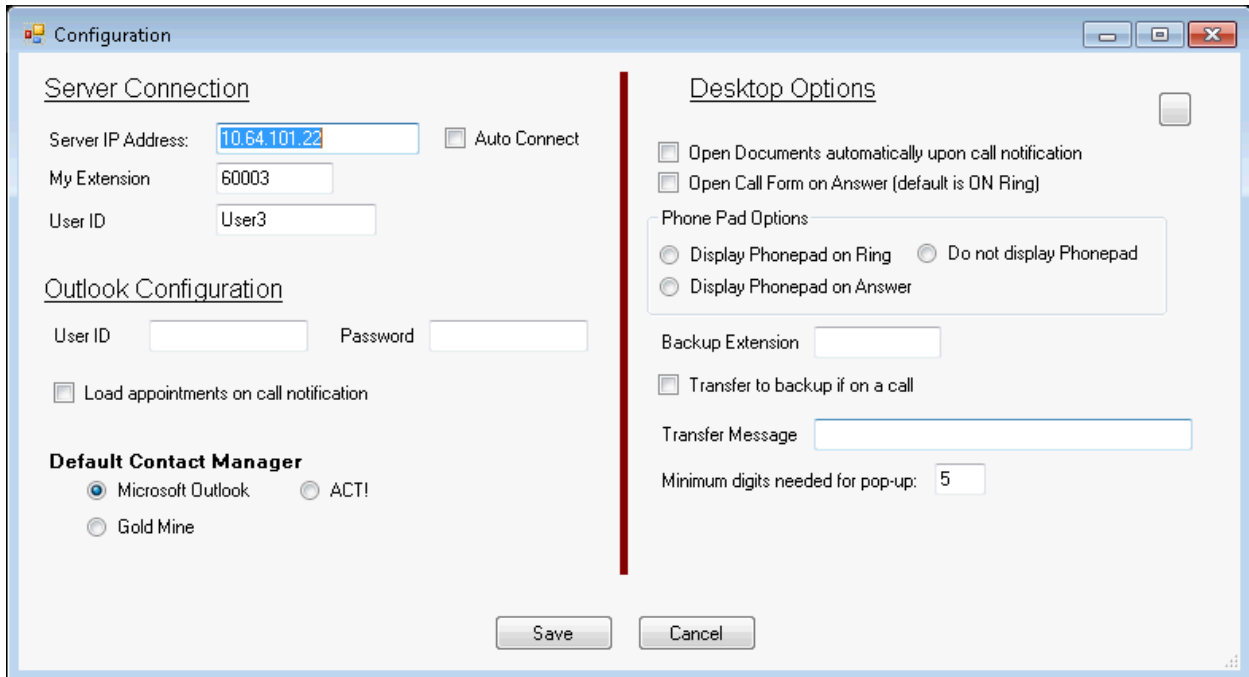
OK

7.2.3. Connect to Server

From the Windows system tray right-click the NACT Client icon and select **Connect** (Not Shown)

From the Windows system tray right-click the NACT Client icon and select **Configuration** (Not Shown) The following configuration window should be displayed:

Verify the information in the **Configuration** window and click **Save**. Now that the client is connected to the server the configuration will be saved without a warning.



8. Verification Steps

The following steps may be used to verify proper configuration between Avaya Application Enablement Services and SPP.

8.1. Verify Avaya Aura® Application Enablement Services

From the Application Enablement Services Management Console select **Status** → **Status and Control** → **TSAPI Service Summary**. Verify that the **Status** is **Talking**, **State** is **Online**, and the number of **Associations** corresponds to the devices being monitored.

The screenshot shows the Avaya Application Enablement Services Management Console interface. The page title is "Application Enablement Services Management Console". The navigation menu on the left includes "Status and Control" with "TSAPI Service Summary" selected. The main content area displays "TSAPI Link Details" with a table of link information.

Welcome: User craft
Last login: Fri Jun 8 12:49:24 2012 from 10.64.50.224
HostName/IP: aes14/10.64.50.14
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-2-32-0

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

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	
<input checked="" type="radio"/>	1	cm5052	1	Talking	Wed May 16 09:20:56 2012	Online	16	7	31	59	30

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

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

8.2. Verify Screen Pop Premium

8.2.1. SPP Client Connection

From the Windows system tray right-click the NACT Client icon and select **Status** (Not Shown). The following Status window should be displayed:



8.2.2. SPP Functionality

Place calls to the monitored extension and verify the screen-pop.



9. Conclusion

Computer Instruments Screen Pop Premium passed compliance testing. These Application Notes describe the procedures required to configure Computer Instruments SPP to interoperate with Avaya Aura® Application Enablement Services to support the reference configuration shown in **Figure 1**.

10. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>

[1] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1 Issue 2 February 2011.

CII product documentation can be found at <http://www.instruments.com/support/index.html>

©2012 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.