



Application Notes for Riverbed UCExpert with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Riverbed UCExpert to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Riverbed UCExpert is a centralized enterprise voice administration and provisioning solution.

In the compliance testing, Riverbed UCExpert used three interfaces from Avaya Aura® Application Enablement Services to support configuration management and analysis, automated proactive testing, and remote troubleshooting.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Riverbed UCExpert to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Riverbed UCExpert is a centralized enterprise voice administration and provisioning solution.

In the compliance testing, Riverbed UCExpert used three interfaces from Avaya Aura® Application Enablement Services to support configuration management and analysis, automated proactive testing, and remote troubleshooting.

The System Management Services (SMS) interface was used by Riverbed UCExpert to support configuration management and analysis, and for remote troubleshooting. SMS syncs can be configured to run on an ad-hoc or regular basis, with sync data obtainable in CSV-format reports. The registered stations from the SMS sync data as well as the busyout and release station objects were also used for remote troubleshooting.

The Java Telephony Application Programming Interface (JTAPI) was used by Riverbed UCExpert to support automated proactive testing. Automated proactive testing can be configured to run on an ad-hoc or regular basis, with configuration for desired devices and call scenarios. The query, monitor, and call control services from JTAPI were used in the automated proactive testing.

The Device, Media, and Call Control (DMCC) XML interface was used by Riverbed UCExpert to support remote troubleshooting. UCExpert used the Multiple Registration method to register virtual IP softphones against the stations under test, for initiation of call control actions.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Avaya Aura® Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

2. General Test Approach and Test Results

The feature test cases were performed automatically and manually. The SMS sync and automated proactive testing were run automatically by scheduled tasks and manually on an ad-hoc basis. The remote troubleshooting was run manually.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the UCExpert server.

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 UCExpert:

- Use of SMS service to download and generate reports for specific managed objects including AAR analysis, ARS analysis, dial plan analysis, route pattern, trunk group, signaling group, VDN, vector, variables, VRT, station, registered IP station, COR, capacity, network region, network map, system parameters customer options, system parameters special applications, and system parameters features. Use of busyout and release station objects to support phone reset as part of remote troubleshooting.
- Use of JTAPI/TSAPI query, monitor, and call control services to support automated proactive testing for call scenarios involving inbound, outbound, answer, drop, and bypassing stations with call forwarding or do not disturb activated.
- Use of DMCC registration, monitoring, physical device, and call control services to support remote troubleshooting for call scenarios involving inbound, outbound, hold, resume, drop, MWI, transfer, and conference.

The serviceability testing focused on verifying the ability of UCExpert to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to UCExpert.

2.2. Test Results

All test cases were executed, and the following were observations on UCExpert:

- The DMCC verify test obtains a list of registered IP stations via SMS in real-time, and performs a Multiple Registration against the first registered station from the received list. As such, the success of the test is dependent upon having proper SMS connectivity, and that the applicable station must use the default password, has IP SoftPhone enabled, and not configured in off-pbx station-mappings.
- Patch 1 of UCExpert removed the creation of the Agent report. After applying the patch, any existing report groups that included the Agent report needs to be manually modified to remove the inclusion.
- List VDN parameters Service Objective, Destination, Conference Controller, Conference Access Code, Conference Type, and Route-to Number may not appear on Communication Manager, but are passed via SMS to UCExpert and included in the Vector report.
- The reported values for Maximum Off-PBX Telephones – EC500/OPS/SCCAN on the Capacity report did not match the values on Communication Manager.
- After a network link is severed, any call in progress as part of the disrupted automated test will continue by design, and will need to be manually terminated since it is not possible to conclusively verify that an existing call is associated with an automated test after network recovery.

2.3. Support

Technical support on UCExpert can be obtained through the following:

- **Phone:** (888) 782-3822 from US and Canada, +1 (415) 247-7381 from elsewhere
- **Email:** support@riverbed.com
- **Web :** <http://support.riverbed.com>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

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

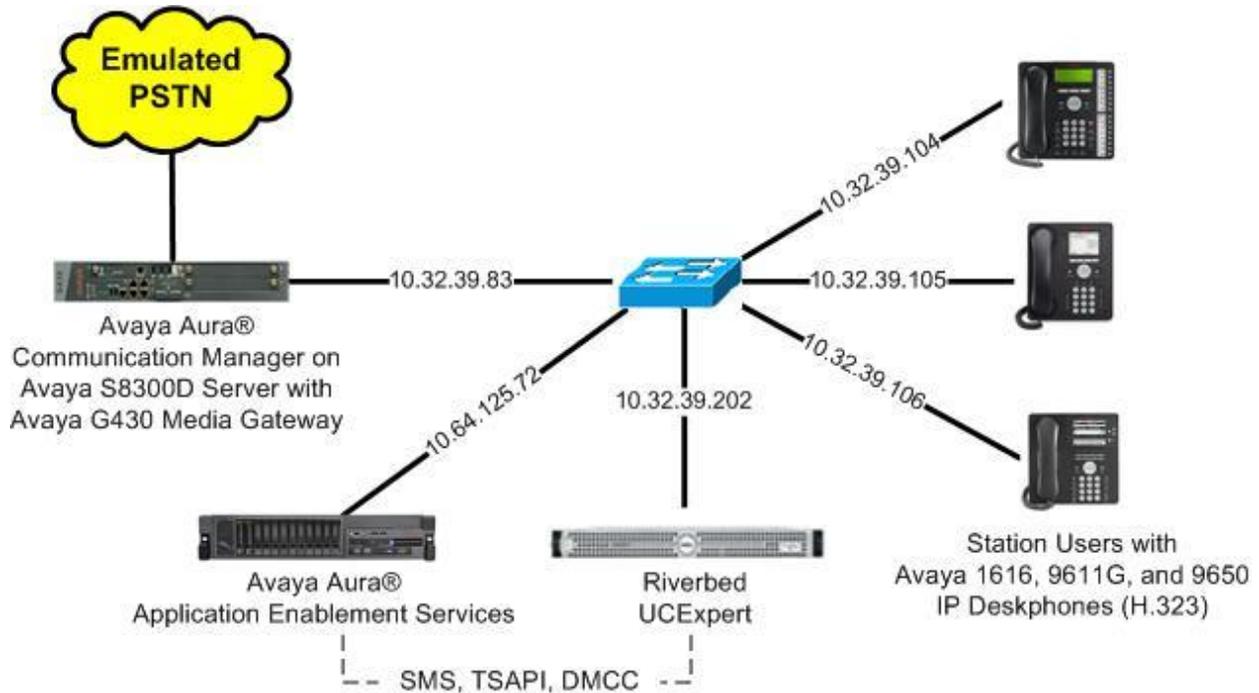


Figure 1: Compliance Testing Configuration

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	6.3.6 (R016x.03.0.124.0-21591)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
Riverbed UCExpert on Linux Red Hat <ul style="list-style-type: none">• Avaya JTAPI Client• Avaya DMCC Java	5.0 Patch 1 (dev_build.5.0.0) 2.6.32-431.11.2.el6.x86_64 6.3.0.121 6.3.0.0.327

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 stations
- Administer off PBX telephone
- Administer accounts

5.1. Verify License

Log in to the System Access Terminal 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)? n                                    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 Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                                           Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n                                     DCS (Basic)? y
ASAI Link Core Capabilities? n                                     DCS Call Coverage? y
ASAI Link Plus Capabilities? n                                     DCS with Rerouting? y
```

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
Extension: 40001
Type: ADJ-IP
                                COR: 1

Name: AES CTI Link
```

5.3. Administer Stations

Use the “change station n” command, where “n” is the first station extension that will be used by UCExpert for remote troubleshooting. Enable **IP SoftPhone**, to allow UCExpert to register a virtual IP softphone against the station. Note the value of **Security Code**, which will be used by UCExpert for remote troubleshooting.

```
change station 45001                                     Page 1 of 4
                                                    STATION
Extension: 45001           Lock Messages? n           BCC: 0
  Type: 9611              Security Code: 45001           TN: 1
  Port: S00000           Coverage Path 1: 1       COR: 1
  Name: G430 Station 1    Coverage Path 2:       COS: 1
                        Hunt-to Station:           Tests? y

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      Button Modules: 0
Survivable GK Node Name:
  Survivable COR: internal      Media Complex Ext:
  Survivable Trunk Dest? y      IP SoftPhone? y

                        IP Video Softphone? n
                        Short/Prefixed Registration Allowed: default
```

Repeat this section to administer all stations to be used in remote troubleshooting. In the compliance testing, three stations were administered as shown below.

```
list station 45001 count 3
                                                    STATIONS
Ext/      Port/      Name/      Room/      Cv1/  COR/      Cable/
 Hunt-to  Type        Surv GK NN  Move      Data Ext  Cv2  COS TN Jack
45000    S00034    G430 Station 0    no          1      1
          9650
45001    S00003    G430 Station 1    no          1      1
          1616
45002    S00040    G430 Station 2    no          1      1
          9611
```

5.4. Administer Off PBX Telephone

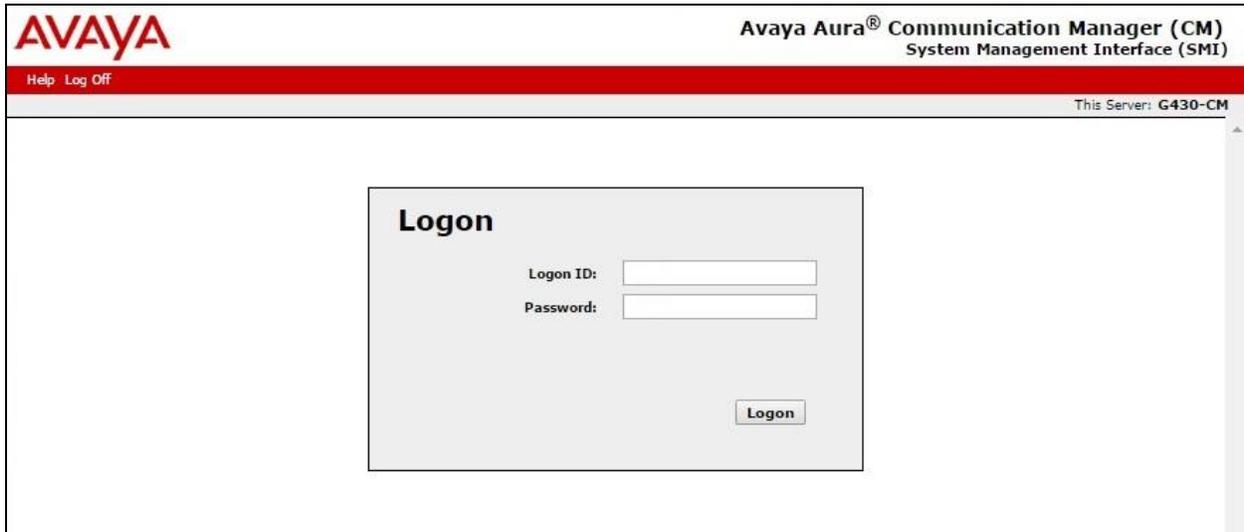
Use the “list off-pbx-telephone station-mapping” command, and make certain that an entry does not exist for each station extension from **Section 5.3**, as stations with off PBX settings are not available for remote control.

```
list off-pbx-telephone station-mapping
```

STATION TO OFF-PBX TELEPHONE MAPPING							
Station Extension	Appl	CC	Phone Number	Config Set	Trunk Select	Mapping Mode	Calls Allowed
44001	OPS		44001	1 /	aar	both	all
46001	OPS		46001	1 /	aar	both	all
46002	OPS		46002	1 /	aar	both	all
46003	OPS		46003	1 /	aar	both	all
46004	OPS		46004	1 /	aar	both	all
46005	OPS		46005	1 /	aar	both	all
46009	OPS		46009	1 /	aar	both	all
46101	OPS		46101	1 /	aar	both	all
46102	OPS		46102	1 /	aar	both	all
46201	OPS		46201	1 /	aar	both	all
46202	OPS		46202	1 /	aar	both	all
614-5001	EC500		3035383578	1 /	aar	both	all
614-6003	OPS		6146003	1 /	aar	both	all

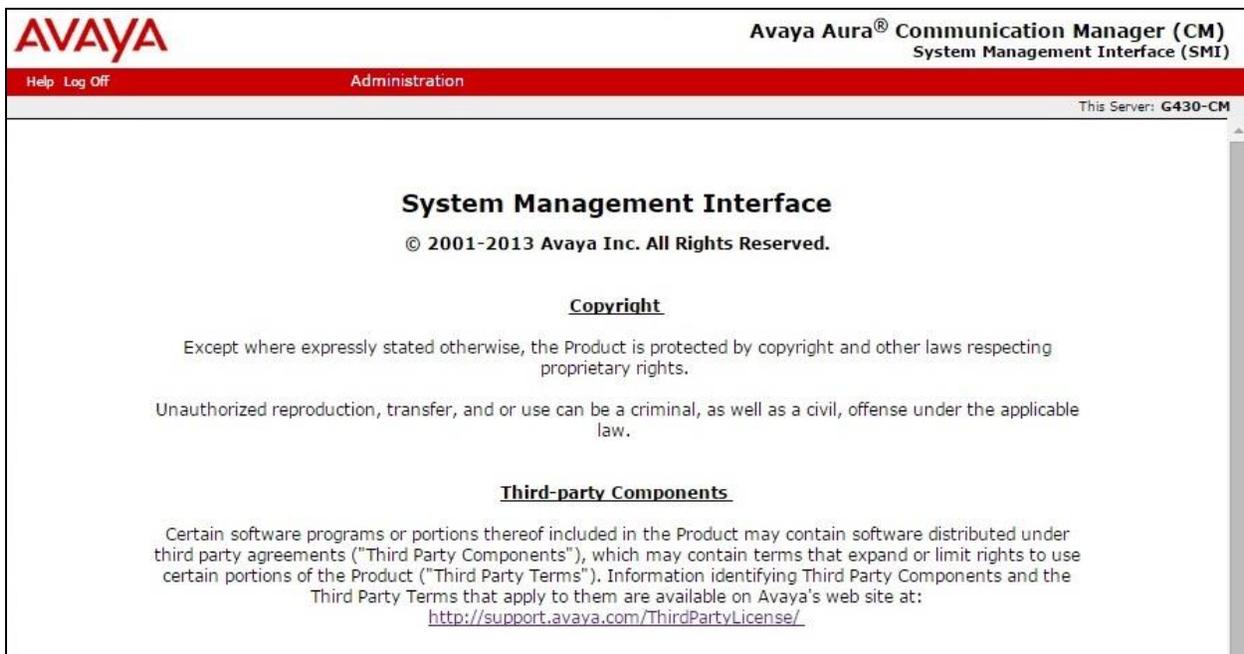
5.5. Administer Accounts

Access the web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of Communication Manager. Log in using the appropriate credentials.



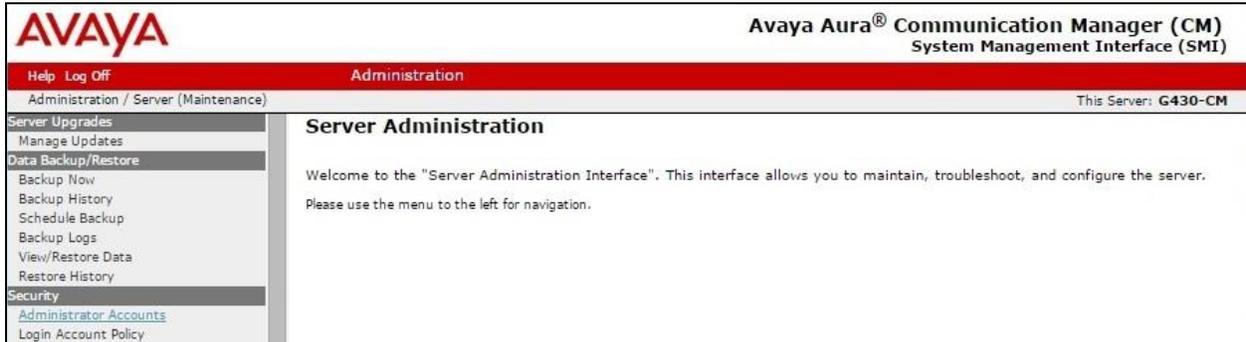
The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) login screen. The page features the Avaya logo in the top left corner and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" in the top right. Below the logo, there are links for "Help" and "Log Off". The server name "This Server: G430-CM" is displayed in the top right corner. The main content area contains a "Logon" form with two input fields: "Logon ID:" and "Password:". A "Logon" button is positioned below the password field.

The **System Management Interface** screen is displayed next. Select **Administration → Server (Maintenance)** from the top menu.

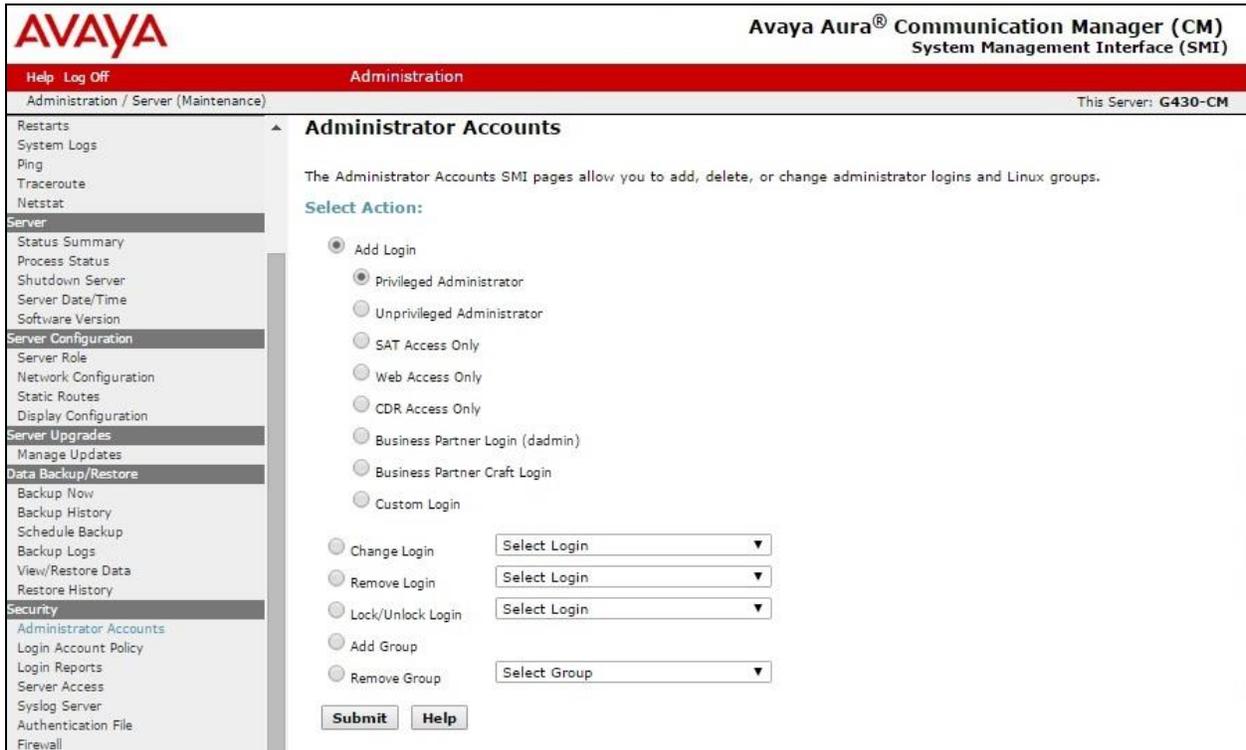


The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administration screen. The page features the Avaya logo in the top left corner and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)" in the top right. Below the logo, there are links for "Help" and "Log Off". The server name "This Server: G430-CM" is displayed in the top right corner. The main content area contains the text "System Management Interface" and "© 2001-2013 Avaya Inc. All Rights Reserved." Below this, there is a section titled "Copyright" with the text: "Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law." Below this, there is a section titled "Third-party Components" with the text: "Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>

The **Server Administration** screen is displayed. Scroll the left pane as necessary and select **Security** → **Administrator Accounts**.



The **Administrator Accounts** screen is displayed next. Select **Add Login** and **Privileged Administrator**, as shown below.



The **Administrator Accounts** screen is updated. Enter the desired credentials for **Login name**, **Enter password or key**, and **Re-enter password or key**. Retain the default values in the remaining fields.

Make a note of the account credentials, which will be used later to configure UCExpert.

AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration Administration / Server (Maintenance) This Server: G430-CM

Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	<input type="text" value="ucxs8300d"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/>
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/ucxs8300d"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Select type of authentication	<input checked="" type="radio"/> Password <input type="radio"/> ASG: enter key <input type="radio"/> ASG: Auto-generate key
Enter password or key	<input type="password" value="*****"/>
Re-enter password or key	<input type="password" value="*****"/>
Force password/key change on next login	<input type="radio"/> Yes <input checked="" type="radio"/> No

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 CT user
- Administer 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 screen. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with the word "Help" in red text on the right side. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 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 left features the Avaya logo. The main header reads "Application Enablement Services Management Console". On the right, a user information box displays: "Welcome: User", "Last login: Mon Nov 12 08:18:47 2014 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_ON_SP", "SW Version: 6.3.3.1.10-0", "Server Date and Time: Mon Nov 10 08:42:14 MST 2014", and "HA Status: Not Configured". A red navigation bar contains "Home | Help | Logout". A left sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains the text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their uses. At the bottom, it notes that these domains can be served by one administrator for all domains or separate administrators 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 using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The main content area is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" with a bullet point for "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" with a bullet point for "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" with a bullet point for "Reserved Licenses". The user information box at the top right is identical to the previous screenshot.

The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen 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 during automated testing, and that both the TSAPI and DMCC licenses are used during remote troubleshooting.

AVAYA Web License Manager (WebLM v6.3) Help | About | Change Password

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 7:07:47 PM -04:00

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

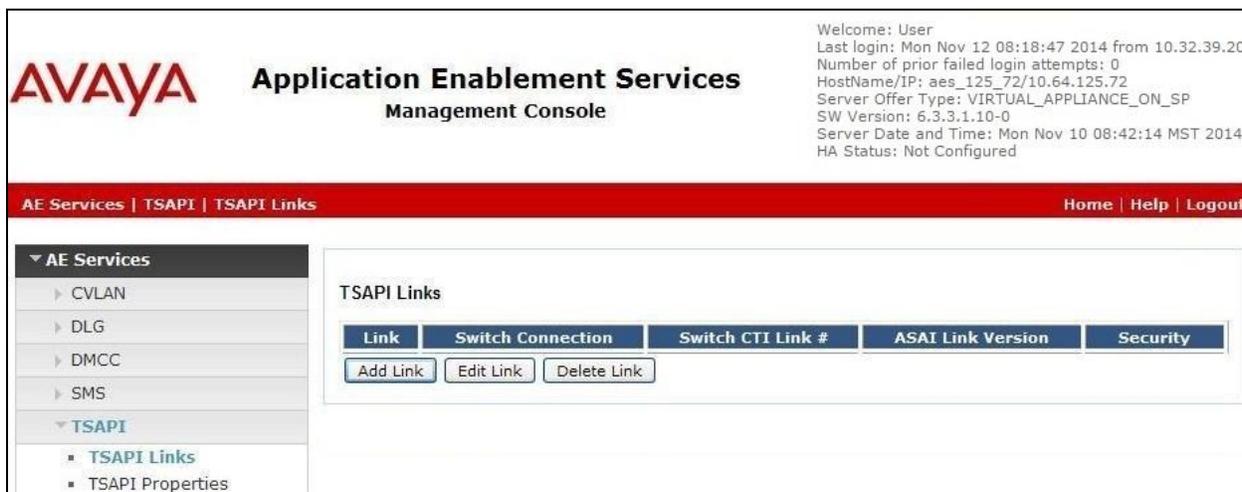
Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_2 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestrict DMCUnrestricted; 1XM_001, BasicUnrestrict DMCUnrestricted; PC_001, BasicUnrestrict DMCUnrestricted; CIE_001, BasicUnrestrict DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestrict DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DM CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

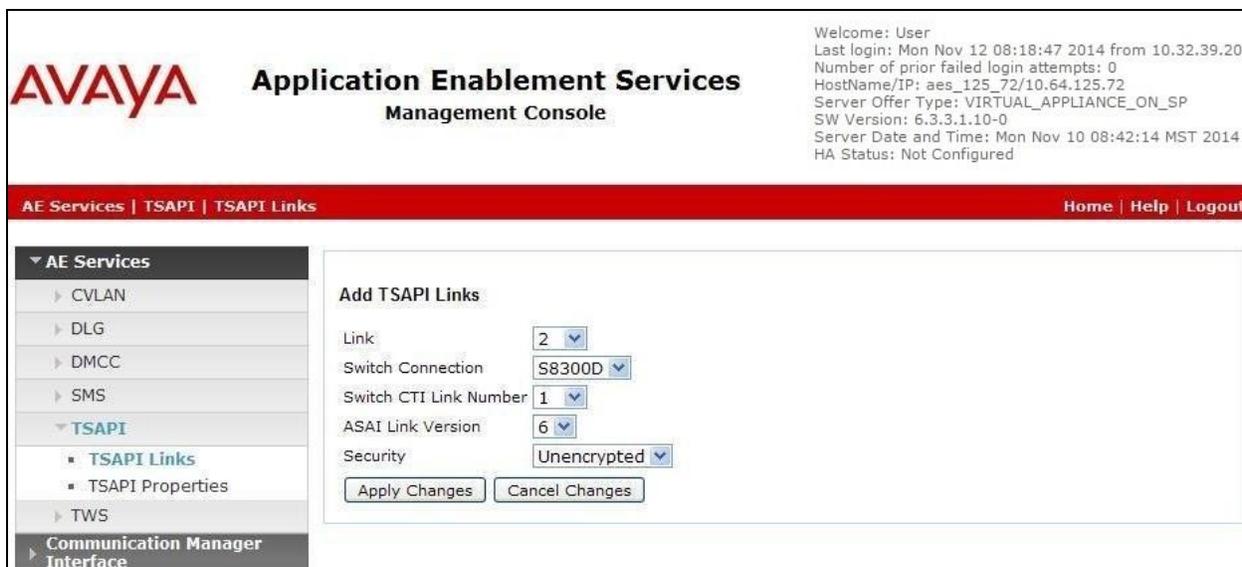
Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The screenshot shows the Avaya Management Console interface. The top left features the Avaya logo and the text "Application Enablement Services Management Console". The top right displays user information: "Welcome: User", "Last login: Mon Nov 12 08:18:47 2014 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_ON_SP", "SW Version: 6.3.3.1.10-0", "Server Date and Time: Mon Nov 10 08:42:14 MST 2014", and "HA Status: Not Configured". A red navigation bar contains "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded to "TSAPI Links". The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “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 top left features the Avaya logo and the text "Application Enablement Services Management Console". The top right displays user information: "Welcome: User", "Last login: Mon Nov 12 08:18:47 2014 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_ON_SP", "SW Version: 6.3.3.1.10-0", "Server Date and Time: Mon Nov 10 08:42:14 MST 2014", and "HA Status: Not Configured". A red navigation bar contains "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded to "TSAPI Links". The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (value: 2), "Switch Connection" (value: S8300D), "Switch CTI Link Number" (value: 1), "ASAI Link Version" (value: 6), and "Security" (value: Unencrypted). Below the form are two buttons: "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 top right corner displays user information: Welcome: User, Last login: Mon Nov 12 08:18:47 2014 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_ON_SP, SW Version: 6.3.3.1.10-0, Server Date and Time: Mon Nov 10 08:42:14 MST 2014, HA Status: Not Configured. The main navigation pane on the left includes AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, High Availability, Licensing, Maintenance, Networking, and Security. The main content area is titled "Switch Connections" and features an "Add Connection" button and a table with the following data:

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

Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

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 use 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 top right corner displays the same user information as the previous screenshot. The main navigation pane on the left is the same as the previous screenshot. The main content area is titled "Edit H.323 Gatekeeper - S8300D" and features a text input field containing "10.32.39.83" and an "Add Name or IP" button. Below the input field is the label "Name or IP Address" and two buttons: "Delete IP" and "Back".

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 displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title "Application Enablement Services Management Console". The top right shows system information: "Welcome: User", "Last login: Mon Nov 12 08:18:47 2014 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_ON_SP", "SW Version: 6.3.3.1.10-0", "Server Date and Time: Mon Nov 10 08:42:14 MST 2014", and "HA Status: Not Configured".

A red navigation bar contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar menu includes: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), and Control (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

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 top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user welcome message with system details. A navigation bar below the header shows "Maintenance | Service Controller" and links for "Home | Help | Logout".

The left sidebar contains a tree view of navigation options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (selected), Server Data, Networking, Security, Status, and User Management.

The main content area is titled "Service Controller" and contains a table with the following data:

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

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

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 UCExpert.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES_125_72”. 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 left features the Avaya logo and the title "Application Enablement Services Management Console". The top right shows a welcome message for the user, including login details and system status. The main navigation bar includes "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security Database" expanded to show "Tlinks". The main content area displays a list of Tlinks with radio buttons for selection and a "Delete Tlink" button.

Welcome: User
Last login: Mon Nov 12 08:18:47 2014 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_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Nov 10 08:42:14 MST 2014
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

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 CT 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 right corner shows system information: Welcome: User, Last login: Mon Nov 12 08:18:47 2014 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_ON_SP, SW Version: 6.3.3.1.10-0, Server Date and Time: Mon Nov 10 08:42:14 MST 2014, HA Status: Not Configured.

The navigation bar includes **User Management | User Admin | Add User** and **Home | Help | Logout**.

The left sidebar menu shows the following structure:

- AE Services
- Communication Manager Interface
- High Availability
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management**
 - Service Admin
 - User Admin**
 - Add User**
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- Utilities
- Help

The main content area is titled **Add User** and contains the following form fields:

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:
- Given Name:

6.9. Administer 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 **Encrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



Application Enablement Services Management Console

Welcome: User
 Last login: Mon Nov 12 08:18:47 2014 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_ON_SP
 SW Version: 6.3.3.1.10-0
 Server Date and Time: Mon Nov 10 08:42:14 MST 2014
 HA Status: Not Configured

Networking | Ports
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▼ Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

CVLAN Ports Enabled Disabled

Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port TCP Port 5678

TSAPI Ports Enabled Disabled

TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

DMCC Server Ports Enabled Disabled

Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input type="radio"/>	<input checked="" type="radio"/>

7. Configure Riverbed UCExpert

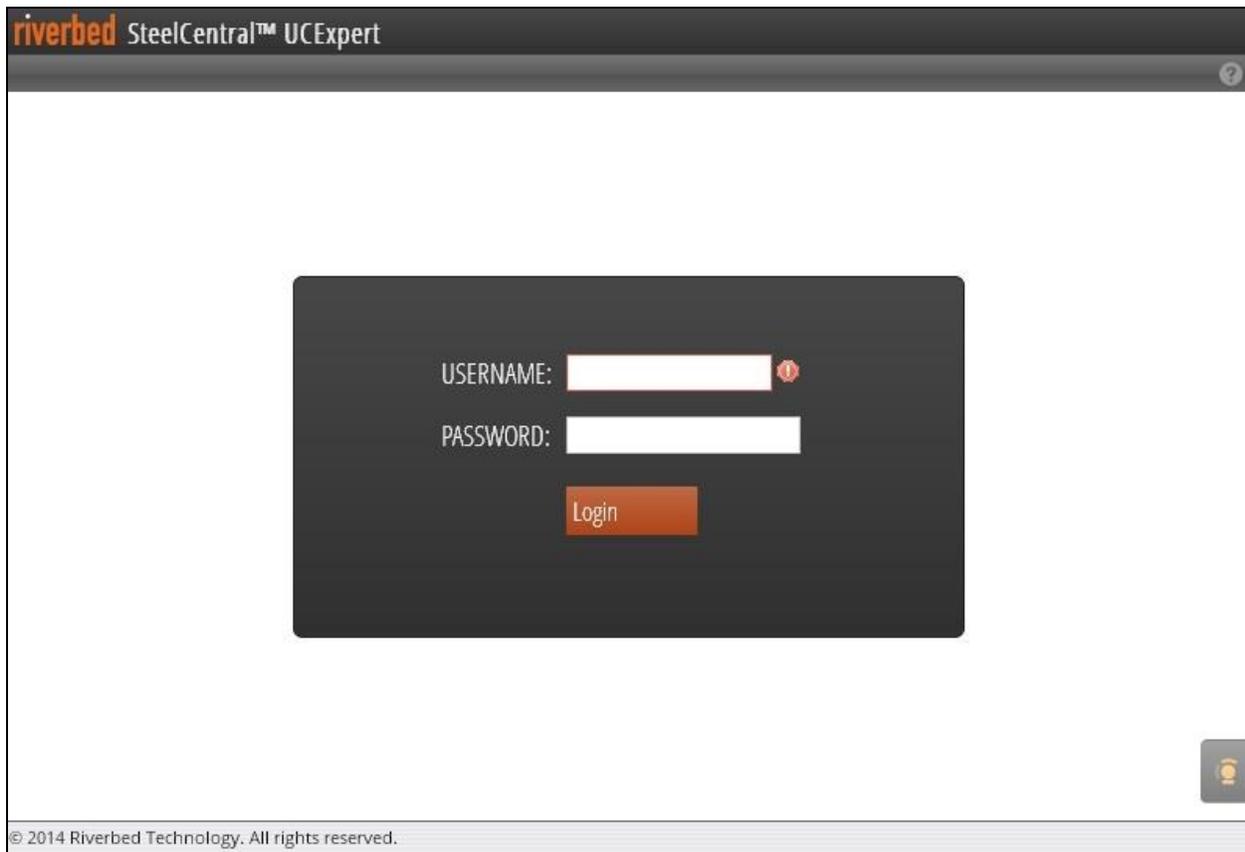
This section provides the procedures for configuring UCExpert. The procedures include the following areas:

- Launch web interface
- Administer systems
- Administer tasks

7.1. Launch Web Interface

Access the web-based interface by using the URL “https://ip-address:8443/ucxgui” in an Internet browser window, where “ip-address” is the IP address of the UCExpert server.

The screen below is displayed. Log in using the appropriate credentials.



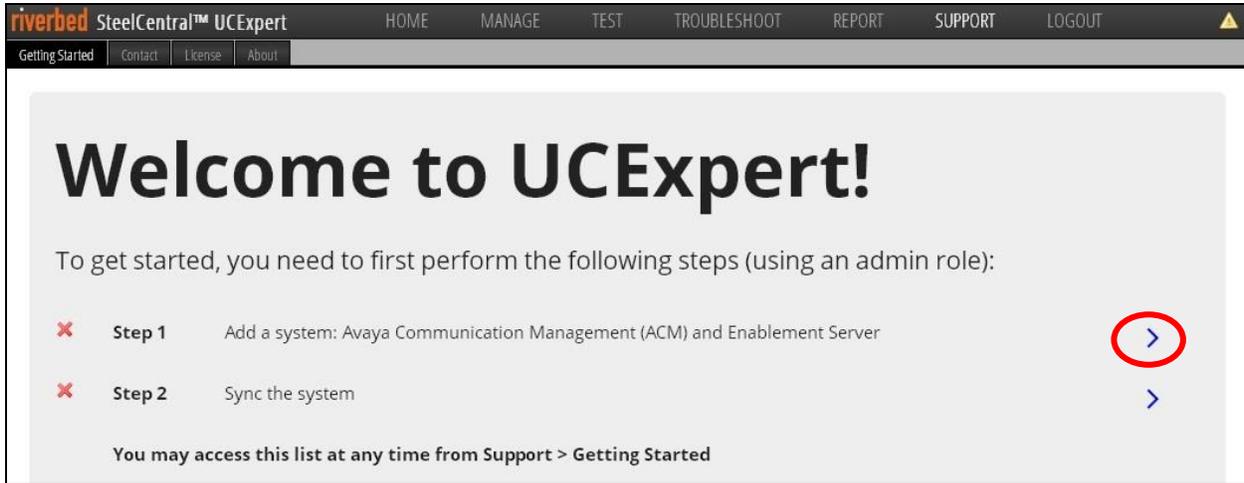
The screenshot shows a web browser window with the title "riverbed SteelCentral™ UCExpert". The main content area displays a dark gray login form with the following elements:

- A "USERNAME:" label followed by a white text input field and a red help icon.
- A "PASSWORD:" label followed by a white password input field.
- An orange "Login" button.

At the bottom left of the browser window, the text "© 2014 Riverbed Technology. All rights reserved." is visible. A small help icon is also present in the bottom right corner of the browser window.

7.2. Administer Systems

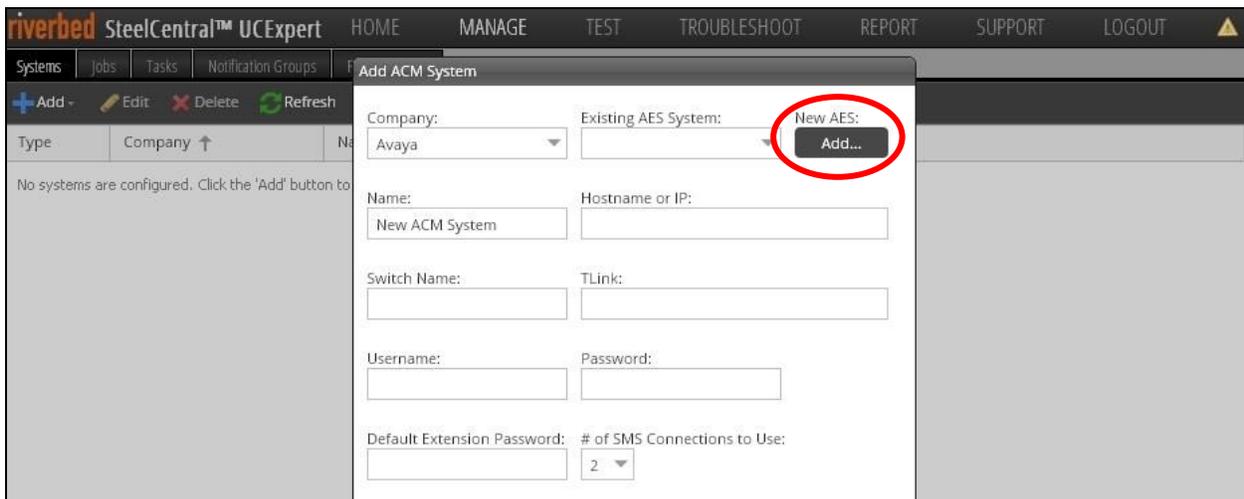
The **Welcome to UCExpert!** screen below is displayed. Click on the arrow for **Step 1**.



The screen below is displayed next. Click on **Add**, and select **Avaya ACM** from the subsequent drop-down list (not shown).



The screen is updated with an **Add ACM System** pop-up box. Enter a desired name for **Company**, and click on the **Add** icon under **New AES**.



The screen is updated with an **Add AES System** pop-up box. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Name:** Enter a desired name, in this case “DevConnect AES”.
- **Hostname or IP:** The IP address of Application Enablement Services.
- **DMCC Username:** The CT user credentials from **Section 6.8**.
- **DMCC Password:** The CT user credentials from **Section 6.8**.
- **TSAPI Username:** The CT user credentials from **Section 6.8**.
- **TSAPI Password:** The CT user credentials from **Section 6.8**.
- **SMS Secure:** Check this field.

The screenshot shows the 'Add AES System' pop-up box in the SteelCentral UCExpert interface. The form is titled 'Add AES System' and contains the following fields and values:

- Company:** Avaya
- Version:** 6.3
- Name:** DevConnect AES
- Hostname or IP:** 10.64.125.72
- DMCC Section:**
 - Username:** ucx
 - Password:** [masked]
 - Port:** 4721
 - Secure:**
 - Session Duration Timer:** 20
 - Session Cleanup Timer:** 40
 - Allowed Licenses:** 10
- TSAPI Section:**
 - Username:** ucx
 - Password:** [masked]
 - Allowed Licenses:** 10
- SMS Section:**
 - Port:** 443
 - Secure:**

At the bottom right of the form, there are 'Save' and 'Cancel' buttons. The background shows the SteelCentral UCExpert interface with a navigation bar (HOME, MANAGE, TEST, TROUBLESHOOT, REPORT, SUPPORT, LOGOUT) and a main content area with a table header (Type, Company) and a message: 'No systems are configured. Click the 'Add' button'.

The screen is updated with the **Add ACM System** pop-up box again. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Hostname or IP:** The IP address of the H.323 gatekeeper from **Section 6.4**.
- **Switch Name:** The switch connection name from **Section 6.3**.
- **TLink:** The TLink name from **Section 6.7**.
- **Username:** The account credentials from **Section 5.5**.
- **Password:** The account credentials from **Section 5.5**.

For **Default Extension Password**, enter the password to be used by the IP softphones for Multiple Registration against the stations for remote troubleshooting.

The screenshot shows the 'Add ACM System' pop-up form in the SteelCentral UCExpert interface. The form is titled 'Add ACM System' and has a toolbar with '+ Add', 'Edit', 'Delete', and 'Refresh' buttons. The form contains the following fields and values:

- Company:** Avaya
- Existing AES System:** DevConnect AES
- New AES:** Add...
- Name:** New ACM System
- Hostname or IP:** 10.32.39.83
- Switch Name:** S8300D
- TLink:** AVAYA#S8300D#CSTA#AES_125_72
- Username:** ucxs8300d
- Password:**
- Default Extension Password:**
- # of SMS Connections to Use:** 2
- Detailed:**
- Include Softphones:**

At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Verify'.

7.3. Administer Tasks

Select **MANAGE** → **Tasks** from the top menu. Follow reference [4] to administer desired tasks for SMS sync and automated proactive testing.

The screenshot below shows the two tasks that were configured in the compliance testing, one for SMS sync and one for automated proactive testing.

The screenshot shows the 'Tasks' management interface in the Riverbed SteelCentral UCExpert application. The top navigation bar includes 'HOME', 'MANAGE', 'TEST', 'TROUBLESHOOT', 'REPORT', 'SUPPORT', and 'LOGOUT'. The 'Tasks' section is active, showing a list of tasks for the 'Avaya' system. The tasks listed are 'SMS Sync' and 'Auto Test 1', both of which are enabled and completed. Below the task list, there is a 'Task Job Details' section which is currently empty, indicating no running jobs.

Name	Enabled	State	Start At	Last Run Time	Stop By	Next Run Time	...
SMS Sync	Yes	Completed	6-17-14 11:30 AM	11-13-14 11:30 ...		11-18-14 11:30
Auto Test 1	Yes	Completed	6-20-14 12:00 PM	11-13-14 12:00 ...		11-18-14 12:00

© 2014 Riverbed Technology. All rights reserved.

8. Verification Steps

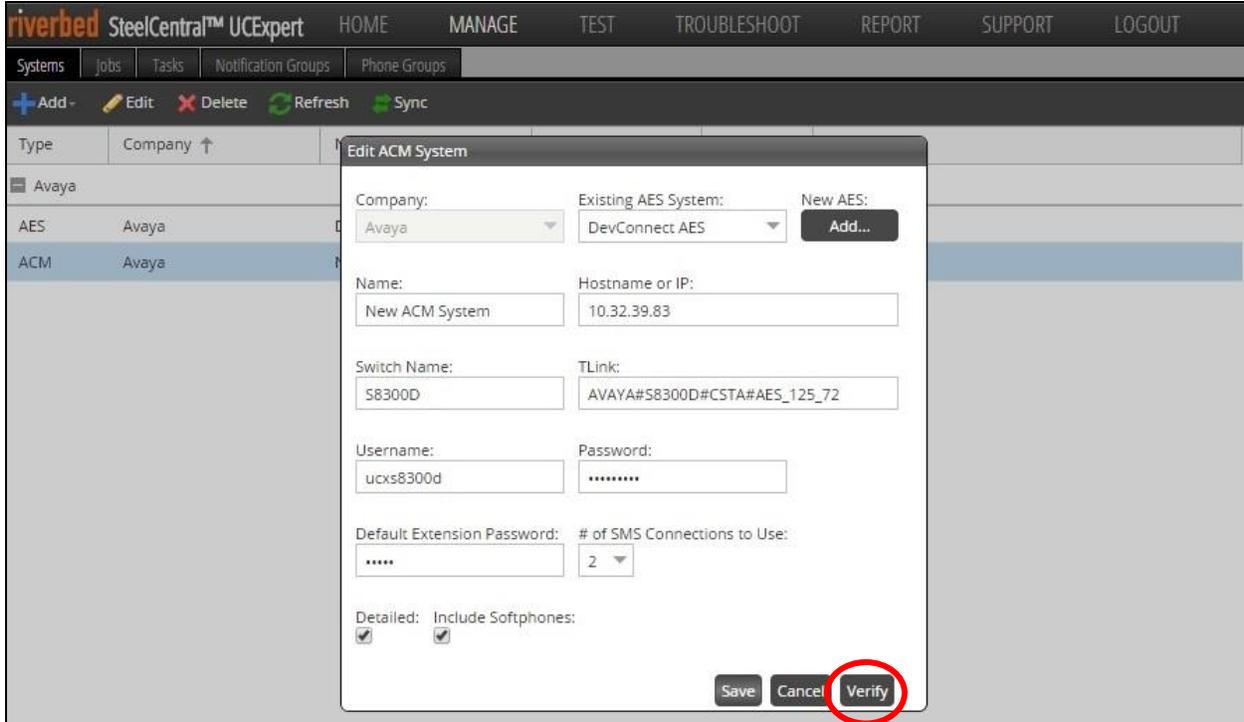
This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and UCExpert.

Follow the procedures in **Section 7.1** to launch the UCExpert web interface. Select **MANAGE** → **Systems** to display a list of configured systems, as shown below. Select the entry corresponding to the **ACM** system from **Section 7.2**, and click **Edit**.



Type	Company ↑	Name	Hostname or IP	Vendor	Sync Status
Avaya					
AES	Avaya	DevConnect AES	10.64.125.72	AVAYA	
ACM	Avaya	New ACM System	10.32.39.83	AVAYA	

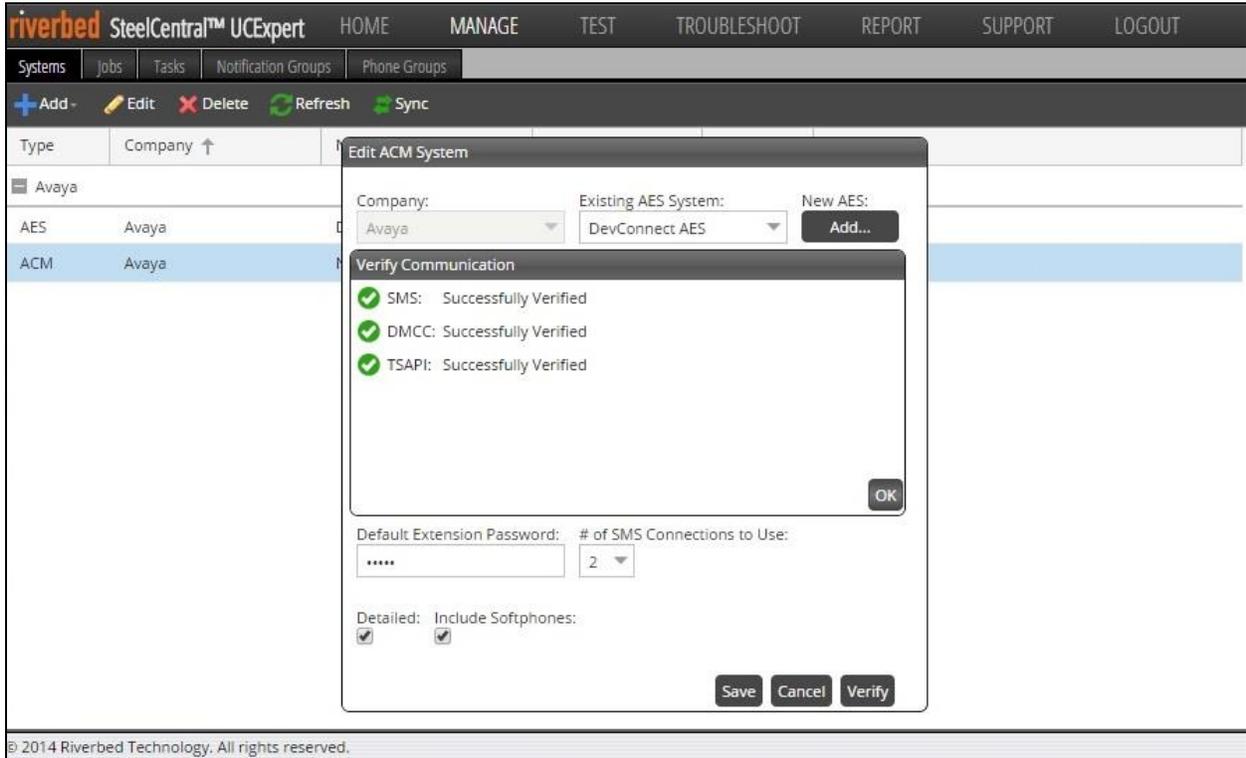
The screen is updated with an **Edit ACM System** pop-up box, as shown below. Click **Verify** to test all interface connections.



Edit ACM System

Company:	Existing AES System:	New AES:
Avaya	DevConnect AES	<input type="button" value="Add..."/>
Name:	Hostname or IP:	
New ACM System	10.32.39.83	
Switch Name:	TLink:	
S8300D	AVAYA#S8300D#CSTA#AES_125_72	
Username:	Password:	
ucxs8300d	*****	
Default Extension Password:	# of SMS Connections to Use:	
*****	2	
Detailed:	Include Softphones:	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Verify that the **Edit ACM System** pop-up box is updated with successful connections to **SMS**, **DMCC**, and **TSAPI**, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Riverbed UCExpert 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 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *Riverbed® SteelCentral™ UCExpert Implementation Guide*, Release 5.0, Modified June 9, 2014, available at <http://support.riverbed.com>.
4. *Riverbed® SteelCentral™ OVA Quick Start Guide*, Release 5.0, available at <http://support.riverbed.com>.

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.