



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Upstream Works Call Management Automation Server with Avaya AuraTM Communication Manager using Avaya AuraTM Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Upstream Works Call Management Automation Server (CMAS) contact center solution, with the TSAPI option, to interoperate with Avaya AuraTM Communication Manager using Avaya AuraTM Application Enablement Services. Upstream Works Call Management Automation Server uses the Avaya AuraTM Application Enablement Services Telephony Services Application Programming Interface (TSAPI) service to query and monitor devices such as VDNs, ACD/Skill groups, and agent extensions on Avaya AuraTM Communication Manager. Depending on the customer's specific application, incoming calls can be routed by Avaya AuraTM Communication Manager, or by Upstream Works Call Management Automation Server using the Telephony Services Application Programming Interface adjunct routing capabilities.

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

1. Introduction

Upstream Works Call Management Automation Server (with the TSAPI option) is a contact center solution that can integrate voice, data, and multimedia messaging services. The compliance testing focused on the voice integration with Avaya Aura™ Communication Manager via Avaya Aura™ Application Enablement Services (AES).

Upstream Works Call Management Automation Server uses the Telephony Services Application Programming Interface (TSAPI) service to query and monitor devices such as VDNs, ACD/Skill groups, and agent extensions on Avaya Aura™ Communication Manager. Depending on the customer's specific application, incoming calls can be routed by Avaya Aura™ Communication Manager, or by Upstream Works Call Management Automation Server using the TSAPI adjunct routing capabilities.

The contact center agents have their desktop computers running the Upstream Works Call Management Automation Server client software, and are networked to Upstream Works Call Management Automation Server via TCP/IP. Call related actions such as answering of incoming calls can be initiated via the physical telephone, or via the desktop utilizing the TSAPI call control capabilities. Upstream Works Call Management Automation Server populates the answering agent's desktop screen with call related information, by utilizing the TSAPI event reports received from Avaya Aura™ Communication Manager on the monitored devices.

1.1. Interoperability Compliance Testing

The interoperability compliance testing included both feature and serviceability testing.

The feature testing focused on verifying Upstream Works Call Management Automation Server handling of TSAPI messages in the areas of routing, call control, event notification, value query, and set value. Testing also included rainy day scenarios to verify handling of negative acknowledgements.

The serviceability testing focused on verifying the ability of Upstream Works Call Management Automation Server to recover from adverse conditions, such as busying out the CTI link and disconnecting the Ethernet cable from Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and Call Management Automation Server.

1.2. Support

Support for Upstream Works can be obtained through the following:

- **Web:** <http://www.upstreamworks.com/>
- **Phone:** 800-808-5220
- **Email:** support@upstreamworks.com

2. Configuration

Figure 1 illustrates the configuration used during compliance testing as described in these Application Notes.

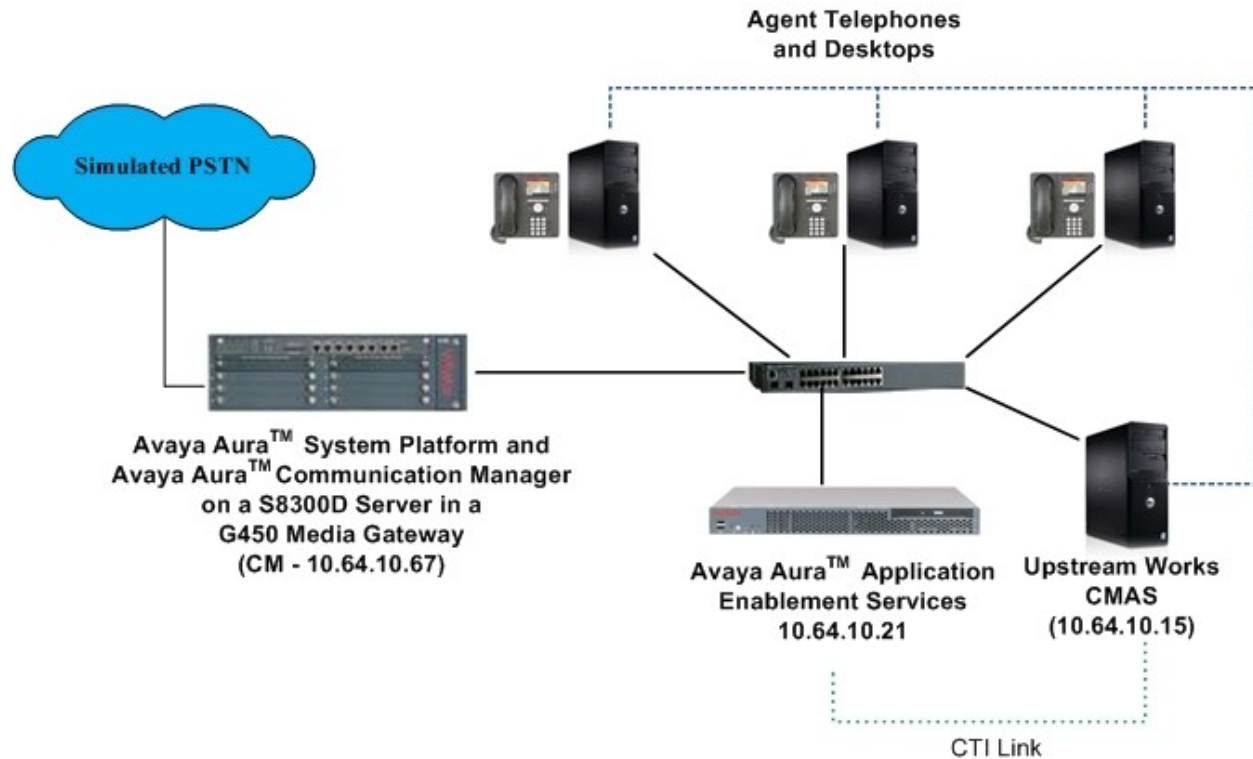


Figure 1: Upstream Works CMAS with Communication Manager using AES

Upstream Works recommends using the Avaya Site Administration (ASA) software to capture the administered VDNs, ACD/Skill groups, and agent devices from Avaya Aura™ Communication Manager. The captured data is exported and loaded onto Upstream Works Call Management Automation Server. For alternative methods of capturing the device information, consult with Upstream Works.

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8300D Media Server	Avaya Aura™ Communication Manager 6.0, R016x.00.0.345.0
Avaya S8500C Server	Avaya Aura™ Application Enablement Services 5.2.2
Avaya 9620 one-X™ Deskphone Edition (H.323)	S3.110b
Avaya 9630 one-X™ Deskphone Edition (H.323)	S3.110b
Avaya 9640 one-X™ Deskphone Edition (H.323)	S3.110b
Upstream Works Call Management Automation Server (with TSAPI option) on Dell PowerEdge 850	7.60 Windows Server 2003 R2 Enterprise x64 Edition SP2
Upstream Works Call Management Automation Server Clients and Avaya Site Administration on Dell Precision 380	7.60 5.0.4 Windows XP Professional SP3

4. Configure Avaya Aura™ Communication Manager

The detailed administration of contact center devices and basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described. For administration of contact center devices and basic connectivity to Application Enablement Services, refer to the appropriate documentation listed in Section 10. This section provides the procedures for the following:

- Verify Avaya Aura™ Communication Manager License
- Administer TSAPI CTI Link
- Administer Adjunct Routing Vector and VDN
- Capture Administered Devices

4.1. Verify Avaya Aura™ Communication Manager 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**.

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		
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y		
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y		
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y		
ATMS? y			
Attendant Vectoring? y			
(NOTE: You must logoff & login to effect the permission changes.)			

Navigate to **Page 6**, and verify that the **Vectoring (Basic)** customer option is set to “y”. If these options are not set to “y”, then contact the Avaya Sales team or Business Partner for a proper license file.

display system-parameters customer-options		Page	6 of 11
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 6.0			
ACD? y	Reason Codes? y		
BCMS (Basic)? y	Service Level Maximizer? n		
BCMS/VuStats Service Level? y	Service Observing (Basic)? y		
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y		
Business Advocate? n	Service Observing (VDNs)? y		
Call Work Codes? y	Timed ACW? y		
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y		
Dynamic Advocate? n	Vectoring (Prompting)? y		
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y		
EAS-PHD? y	Vectoring (3.0 Enhanced)? y		
Forced ACD Calls? n	Vectoring (ANI/II-Digits Routing)? y		
Least Occupied Agent? y	Vectoring (G3V4 Advanced Routing)? y		
Lookahead Interflow (LAI)? y	Vectoring (CINFO)? y		
Multiple Call Handling (On Request)? y	Vectoring (Best Service Routing)? y		
Multiple Call Handling (Forced)? y	Vectoring (Holidays)? y		
PASTE (Display PBX Data on Phone)? y	Vectoring (Variables)? y		
(NOTE: You must logoff & login to effect the permission changes.)			

4.2. Administer TSAPI 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. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field (optional). Default values may be used in the remaining fields. Submit these changes.

add cti-link 1		Page	1 of 3
CTI LINK			
CTI Link: 1			
Extension: 6201			
Type: ADJ-IP			
COR: 1			
Name: to AES-10.64.10.21			

4.3. Administer Adjunct Routing Vector and VDN

For customers that utilize Upstream Works CMAS to make the call routing decisions, administer a vector and a VDN for the adjunct routing feature. Modify a vector using the “change vector n” command, where “n” is an available vector number. The vector will be used to provide adjunct routing to the CTI link defined in **Section 4.2** (see vector step **02**). Provide sufficient wait-time for CMAS to route the call (see vector step **03**).

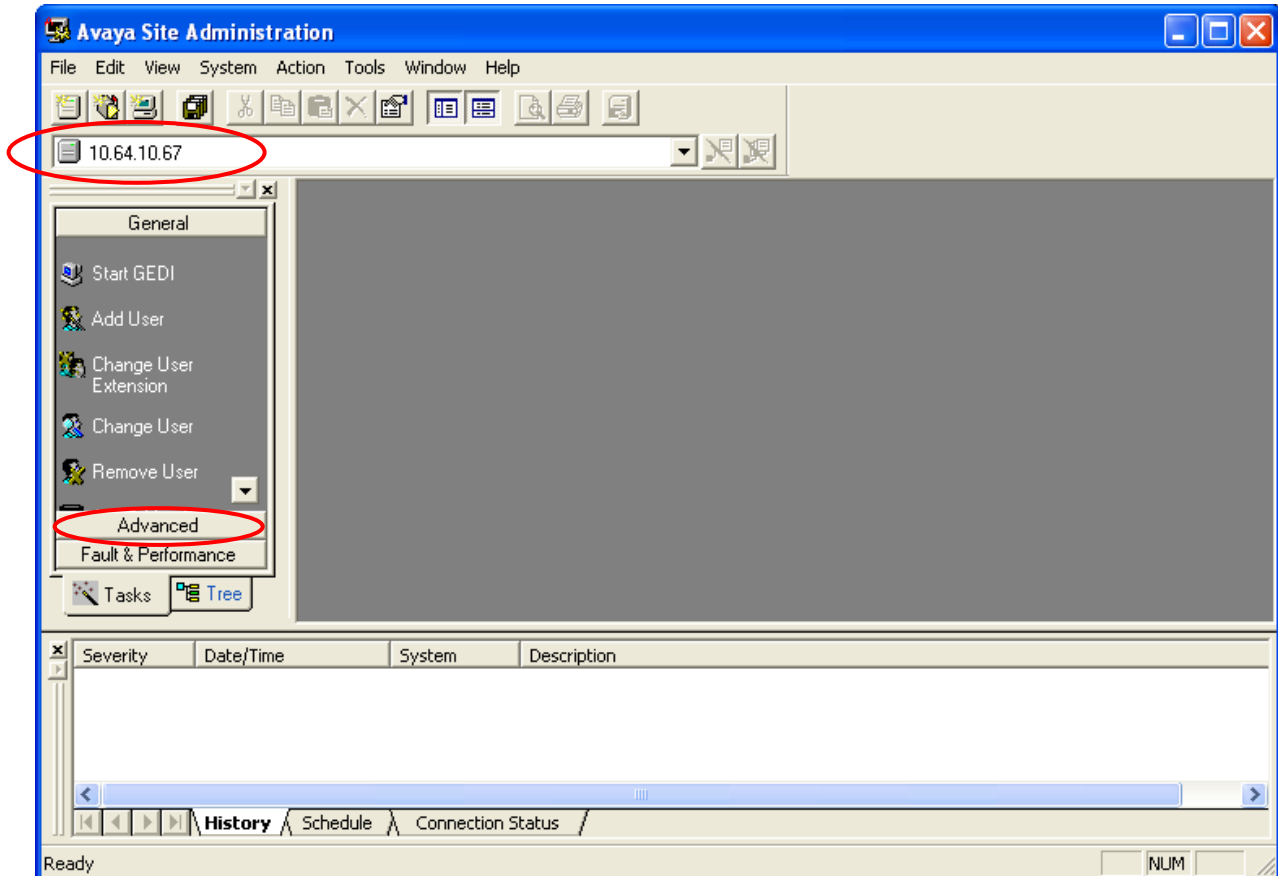
```
change vector 1                                     Page 1 of 6
                                                    CALL VECTOR
Number: 1                                           Name: Adjunct Route
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 wait-time      2 secs hearing ringback
02 adjunct        routing link 1
03 wait-time      600 secs hearing silence
04
05
```

Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive name for the **Name** field (optional), and add the vector number from above for the **Destination: Vector Number** field. Retain the default values for all remaining fields.

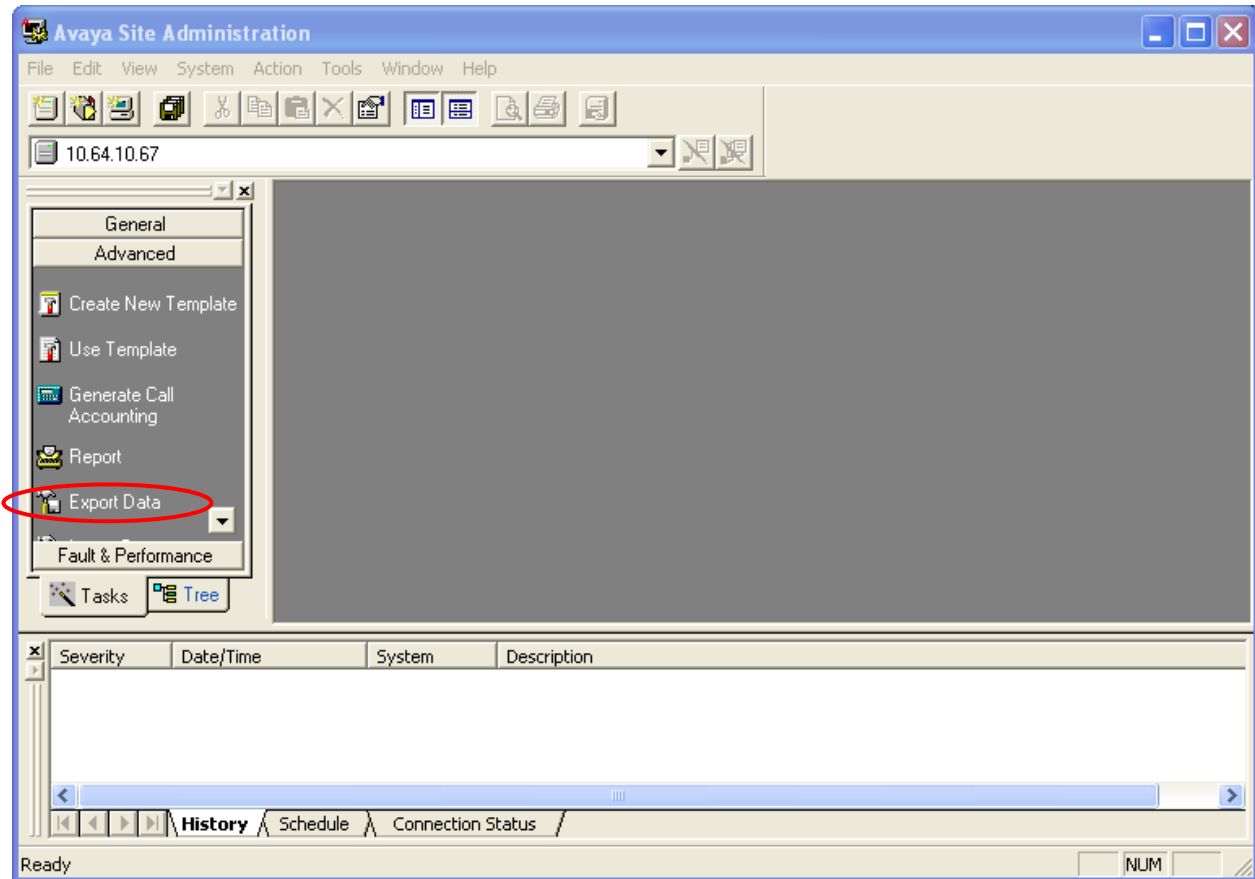
```
add vdn 6401                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
Extension: 6401
Name*: Adjunct Route VDN
Destination: Vector Number      1
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none
VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:
* Follows VDN Override Rules
```

4.4. Capture Administered Devices

From a networked PC with Avaya Site Administration installed, select **Start → All Programs → Avaya → Site Administration**. In the **Avaya Site Administration** screen below, select the relevant Communication Manager from the drop down list (in this case, “10.64.10.67”). Click on the **Advanced** tab in the left pane to expand it. These Application Notes assume the Avaya Site Administration has been installed with configuration in place to connect to Communication Manager.



In the updated **Avaya Site Administration** screen below, click on **Export Data** under **Advanced** in the left pane.



The **Export Data – Filter** screen is displayed. Select “station” from the **Select an object to export** drop down list, and retain the radio button for **Export to file**.

Note: The “station” object corresponds to the agent physical telephones, the “hunt-group” object corresponds to ACD/Skill groups, and the “vdn” object corresponds to VDNs.

Export Data - Filter

Data export allows you to retrieve information from a Voice or Messaging System and save it in a file.

Select an object to export: station

☒ Export to file
☐ Export to LDAP directory

Filter:


Field

Warning: Do not use punctuation in object names.

< Back Next > Cancel Help

In the **Filter** table below, click on an empty row under **Field**, and select “Extension” from the drop down list. In the associated **Value** column, enter a range of agent extensions to capture. Note that the customer can either apply the necessary filter here to only capture those extensions desired to be monitored, or the customer can capture all extensions now and remove the unnecessary ones via Upstream Works CMAS later. For compliance testing, three agents were administered with extensions values from 6001 to 6003. Click on **Next** to proceed.

Export Data - Filter



Data export allows you to retrieve information from a Voice or Messaging System and save it in a file.

Select an object to export: station

☒ Export to file
 ☐ Sort Field List

☐ Export to LDAP directory

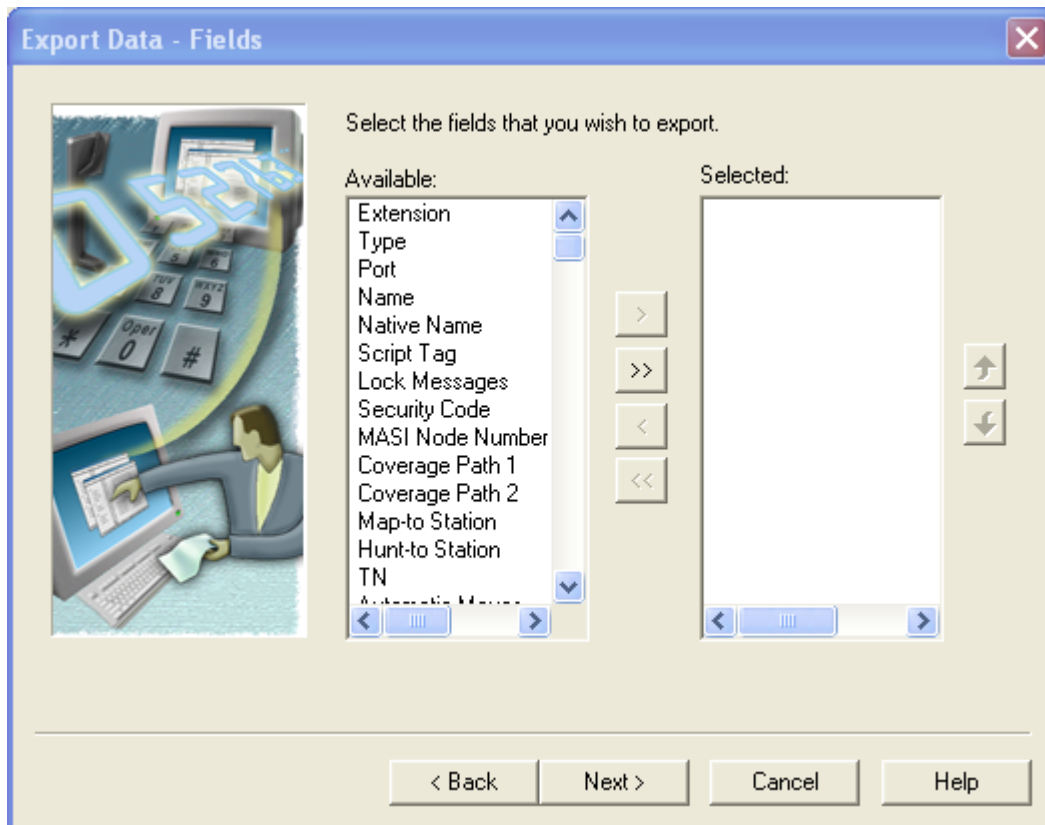
Filter:

Field	Value
Extension	6001-6003

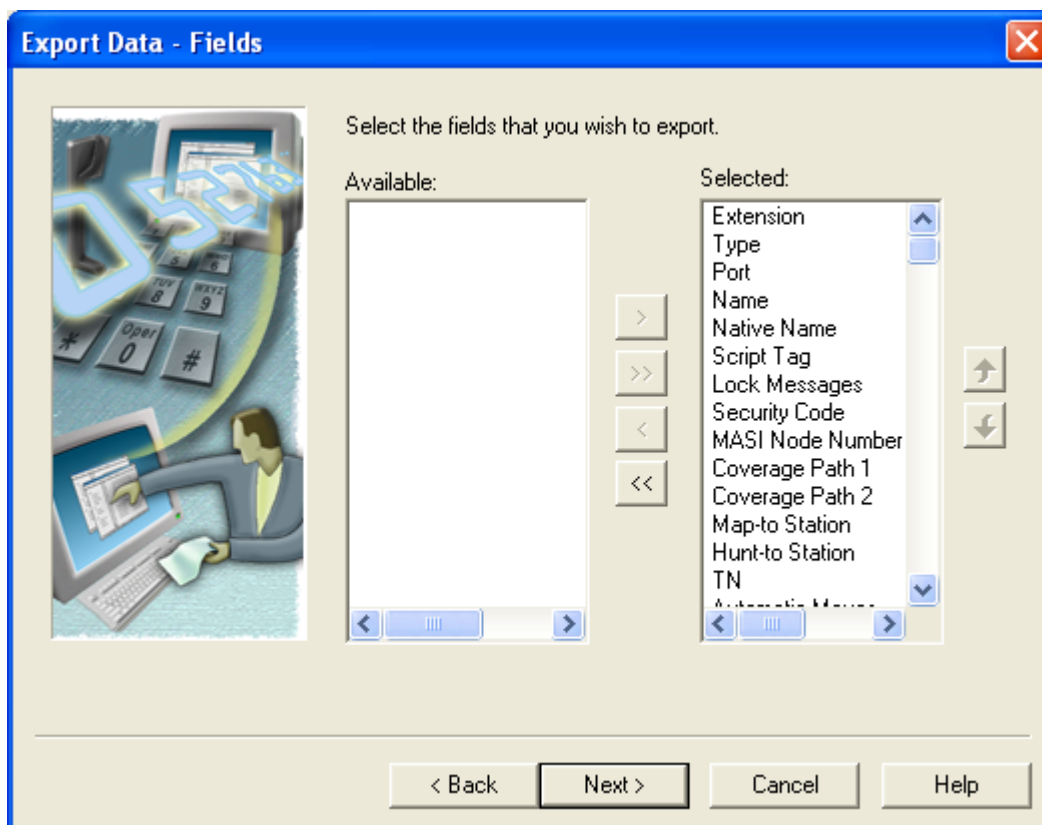
Warning: Do not use punctuation within the extension

< Back
Next >
Cancel
Help

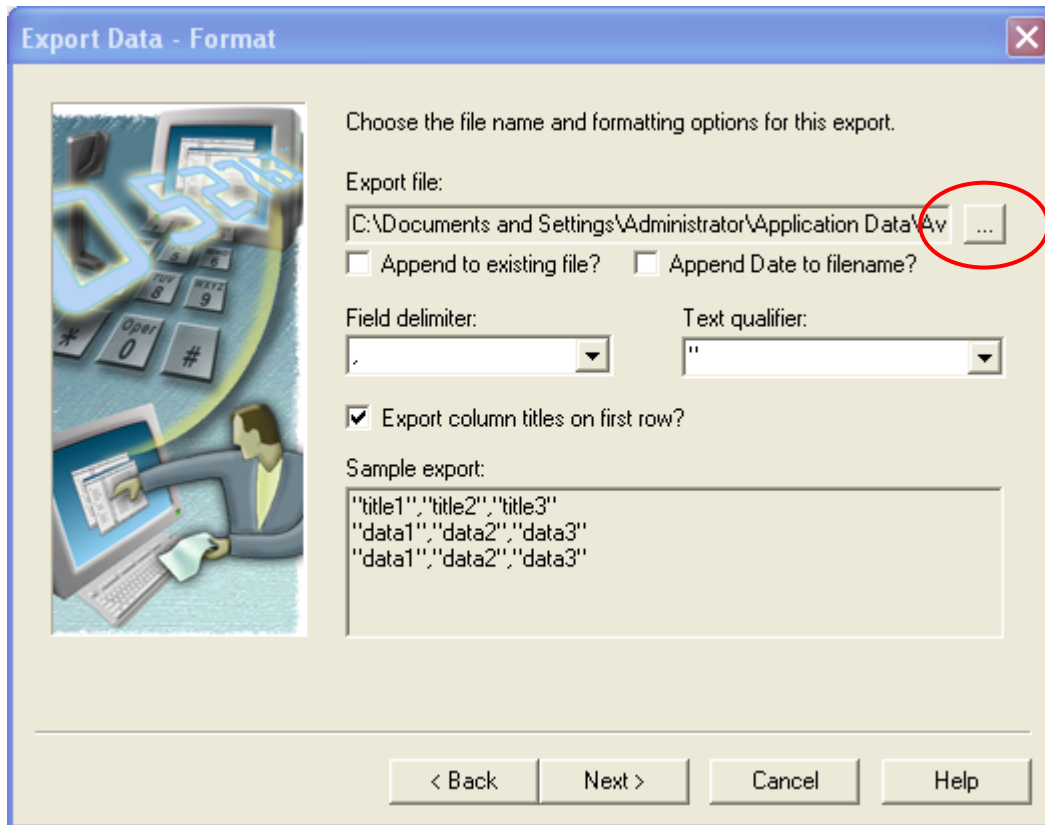
The **Export Data – Fields** screen is displayed. Select all fields under **Available** in the left pane, and use the double-arrow icon to move them under **Selected** in the right pane.



The resultant screen from the move is displayed below. Click on **Next** to proceed with the capturing.



The **Export Data – Format** screen is displayed next. Click on the browse icon for **Export file**.



Export Data - Format

Choose the file name and formatting options for this export.

Export file:
C:\Documents and Settings\Administrator\Application Data\Av ...

☐ Append to existing file? ☐ Append Date to filename?

Field delimiter: , Text qualifier: "

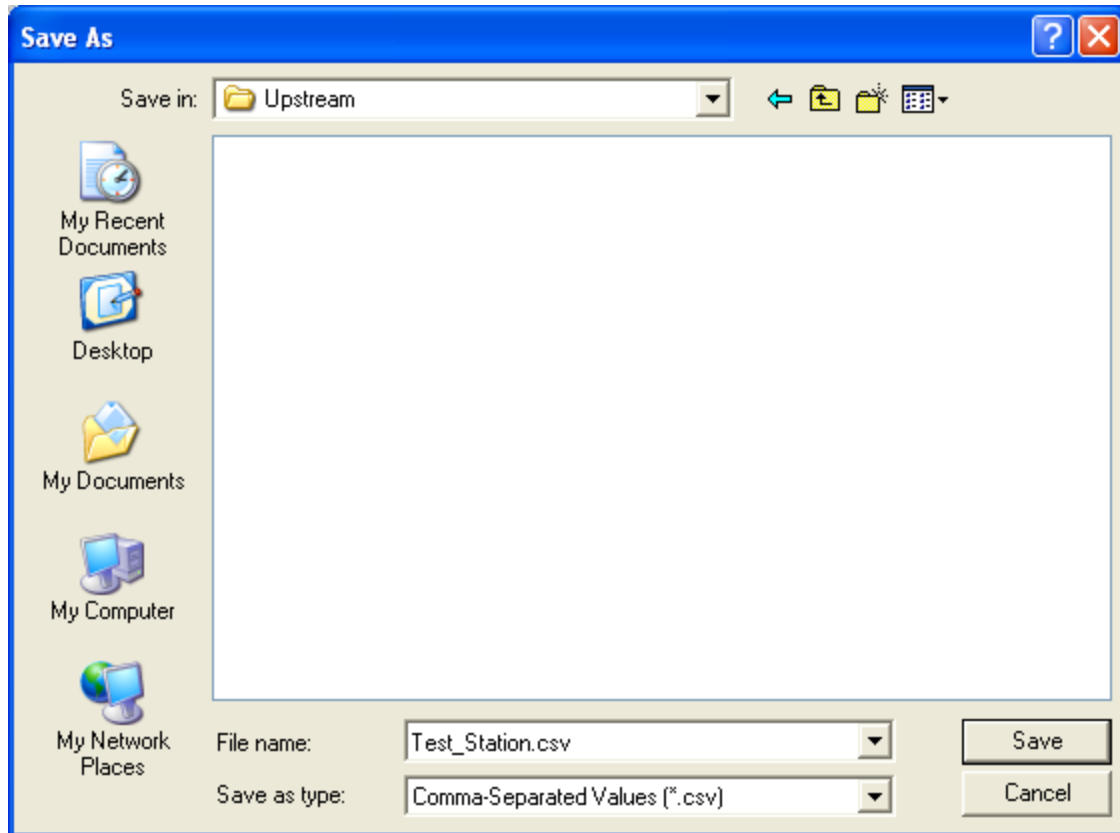
☒ Export column titles on first row?

Sample export:

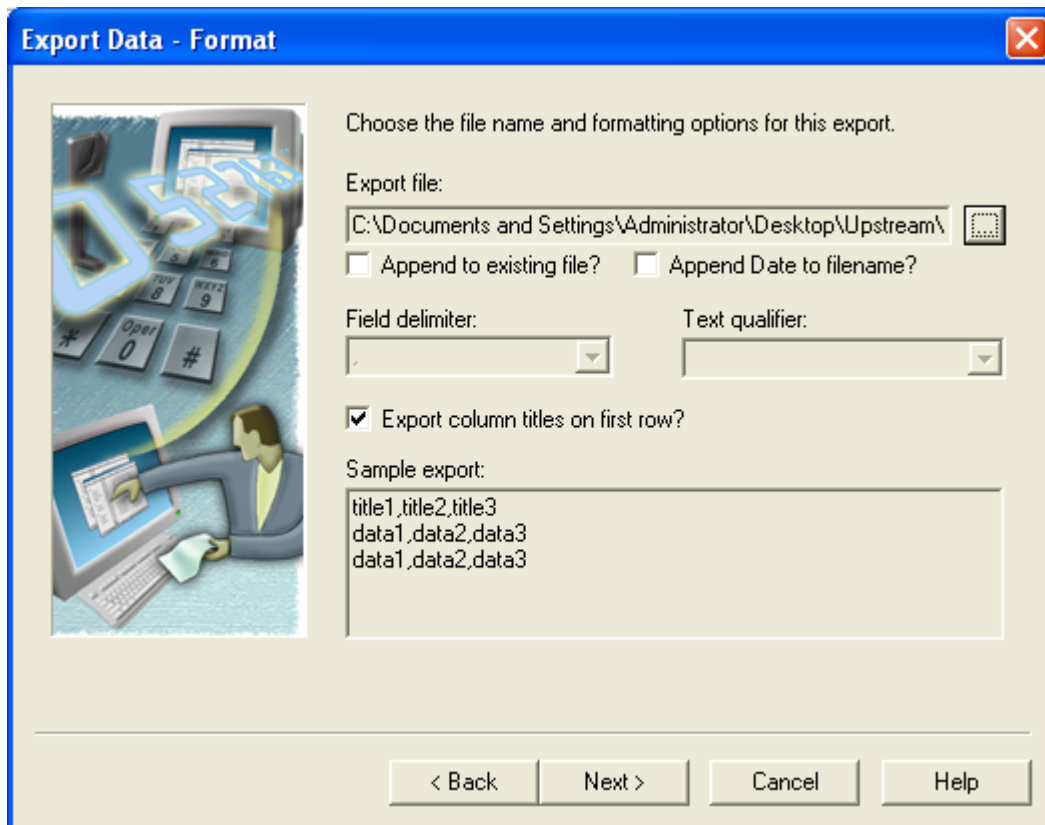
```
"title1","title2","title3"  
"data1","data2","data3"  
"data1","data2","data3"
```

< Back Next > Cancel Help

A **Save As** dialog box is displayed. Enter a descriptive name into **File name** (e.g. “Test_Station.csv”), and select “Comma-Separated Values (*.csv)” from the **Save as type** drop down list. This file type separates the fields by the comma character, and separates the records by the newline delimiter. Click **Save**.



The **Export Data – Format** screen is displayed again, and updated with the entered **Export file** name. Click **Next** to proceed.



The dialog box is titled "Export Data - Format" and contains the following elements:

- Instruction:** "Choose the file name and formatting options for this export."
- Export file:** A text field containing "C:\Documents and Settings\Administrator\Desktop\Upstream\" and a file icon button.
- Append options:** Two checkboxes: "Append to existing file?" (unchecked) and "Append Date to filename?" (unchecked).
- Field delimiter:** A dropdown menu showing a comma (`,`).
- Text qualifier:** A dropdown menu showing a double quote (`"`) and a file icon button.
- Export column titles:** A checked checkbox labeled "Export column titles on first row?".
- Sample export:** A text area containing the following text:

```
title1,title2,title3
data1,data2,data3
data1,data2,data3
```
- Navigation buttons:** "< Back", "Next >", "Cancel", and "Help".

The **Export Data – Schedule** screen is displayed next. Enter a descriptive name for **Name**, and maintain the check in **Run Now**. Click **Next**.

Export Data - Schedule

Give this task a name or description.

Name:

When you schedule or run this task, look for the name above in the Schedule Window. If you save this task, look for this name in the navigation tree.

Run, Schedule or Save

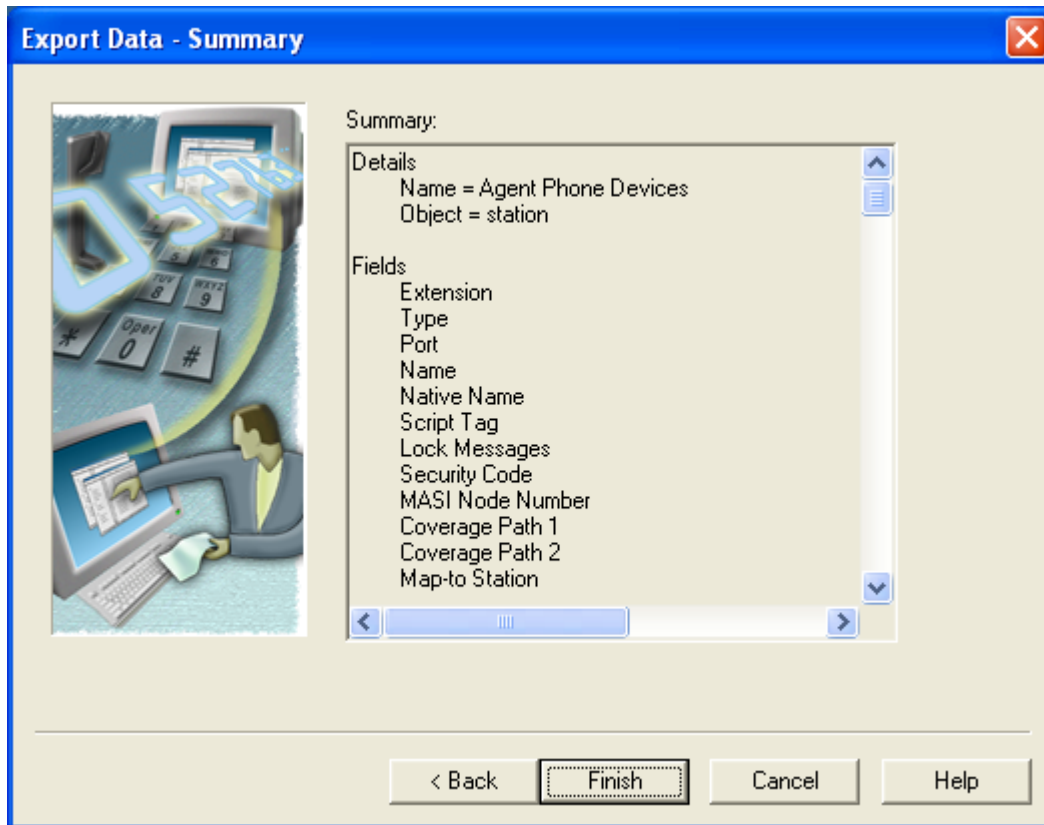
☒ Run Now

☐ Schedule this task to run

☐ Save information in tree

< Back Next > Cancel Help

In the **Export Data – Summary** screen, click **Finish** to complete the capture.



Repeat the same procedures in this section to capture the Agent Login IDs, VDN, and ACD/Skill Groups data. The following table lists the contact center device types, the associated object in Avaya Site Administration, and the created file name for the captured data from the compliance testing. The file names may vary, and they are used to administer the Upstream Works CMAS in **Section 6.1**.

Device Type	Object Name	File Name
Agent extensions	station	Test_Station.csv
Agent login IDs	agent-loginID	Test_AgentID.csv
VDN	vdn	Test_vdn.csv
ACD/Skill groups	hunt-group	Test_HuntGroup.csv

5. Configure Avaya Aura™ Application Enablement Services

The detailed administration of connectivity between Application Enablement Services (AES) and Communication Manager is not the focus of these Application Notes and will not be described. For administration of basic connectivity to Communication Manager, refer to the appropriate documentation listed in **Section 10**. This section provides the procedures for the following areas:

- Verify Avaya Aura™ Application Enablement Services License
- Administer TSAPI Link
- Administer CMA User
- Restart TSAPI Service

5.1. Verify Avaya Aura™ Application Enablement Services License

Access the AES 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 AES server. Click the “Continue to Login” link (not shown). The **Login** screen is displayed as shown below. Log in using appropriate credentials.



Application Enablement Services Management Console

[Help](#)

Please login here:

Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

© 2009 Avaya, Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed, as shown below. Select **AE Services** from the left pane.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right is the title "Application Enablement Services Management Console". In the top right corner, a welcome message is displayed: "Welcome: User craft", "Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51", "HostName/IP: aesserver2/205.168.62.111", "Server Offer Type: TURNKEY", and "SW Version: r5-2-2-105-0". Below the title bar is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following 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: "• 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.", and "• Help - Use Help to obtain a few tips for using the OAM Help system". Below the list, it states: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain." At the bottom of the page, the copyright notice "© 2009 Avaya, Inc. All Rights Reserved." is displayed.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Home Home | Help | Logout

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 both domains, or a separate administrator for each domain.

© 2009 Avaya, Inc. All Rights Reserved.

The **AE Services** screen is displayed next. Verify that Application Enablement Services is licensed for the **TSAPI Service**, as shown in the screen below (**License Mode = NORMAL MODE**). If the TSAPI service is not licensed, contact the Avaya Sales team or Business Partner for a proper license file.



Application Enablement Services
 Management Console

Welcome: User craft
 Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
 HostName/IP: aesserver2/205.168.62.111
 Server Offer Type: TURNKEY
 SW Version: r5-2-2-105-0

AE Services
Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)


* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
 You are licensed to run Application Enablement (CTI) version 5.0

© 2009 Avaya, Inc. All Rights Reserved.

5.2. Administer TSAPI Link

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

**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

AE Services | TSAPI | TSAPI LinkHome | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8300mobile	1	4	Unencrypted
2	devcon31	1	4	Unencrypted


Add Link Edit Link Delete Link

© 2009 Avaya, Inc. All Rights Reserved.

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the AES 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 “S8300DCM6” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 4.2**. Click on **Apply Changes**.

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 user 'craft' with login details. A red navigation bar contains 'AE Services | TSAPI | TSAPI Link' and links for 'Home | Help | Logout'. A left sidebar lists various services, with 'TSAPI Links' highlighted under the 'TSAPI' section. The main content area is titled 'Add TSAPI Links' and contains five dropdown menus: 'Link' (set to 3), 'Switch Connection' (set to S8300DCM6), 'Switch CTI Link Number' (set to 1), 'ASAI Link Version' (set to 4), and 'Security' (set to Unencrypted). At the bottom of this form are two buttons: 'Apply Changes' and 'Cancel Changes'. The footer of the console shows the copyright notice '© 2009 Avaya, Inc. All Rights Reserved.'

The **Apply Changes to Link** screen is displayed. Click on **Apply**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

AE Services | TSAPI | TSAPI Link

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

© 2009 Avaya, Inc. All Rights Reserved.

5.3. Administer CMA User

Administer an user account for the Upstream Works CMAS. Select **User Management** → **User Admin** → **Add User** from the left pane. The **Add User** screen is displayed, as shown below. Enter descriptive values for the **User Id**, **Common Name**, and **Surname**. Enter appropriate values for the **User Password** and **Confirm Password** fields to create a user account for Upstream Works CMAS. Retain the default value of “None” for **Avaya Role**, and select “Yes” from the **CT User** drop down list. Click on **Apply** at the bottom of the screen (not shown below).


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: 'Welcome: User craft', 'Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51', 'HostName/IP: aesserver2/205.168.62.111', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-2-105-0'. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'.

The left sidebar shows a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under User Admin, the options are: Add User, Change User Password, List All Users, Modify Default Users, and Search Users.

The main content area is titled 'Add User'. It includes a note: 'Fields marked with * can not be empty.' The form fields are as follows:

- * User Id: Upstream
- * Common Name: Upstream
- * Surname: Upstream
- * User Password: [masked]
- * Confirm Password: [masked]
- Admin Note: [empty text field]
- Avaya Role: None (dropdown menu)
- Business Category: [empty text field]
- Car License: [empty text field]
- CM Home: [empty text field]
- Css Home: [empty text field]
- CT User: Yes (dropdown menu)
- Department Number: [empty text field]
- Display Name: [empty text field]
- Employee Number: [empty text field]
- Employee Type: [empty text field]
- Enterprise Handle: [empty text field]
- Given Name: [empty text field]
- Home Phone: [empty text field]

Select **Security** → **Security Database** → **CTI Users** → **List All Users** to get a listing of all **CTI Users**, as shown below. Select the **User ID** created for Upstream Works CMAS and click the **Edit** button.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

▪ Tlinks

▪ Tlink Groups

▪ Worktops

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> Devtest	Devtest	NONE	NONE
<input type="radio"/> MobileMax	MobileMax	NONE	NONE
<input checked="" type="radio"/> Upstream	Upstream	NONE	NONE
<input type="radio"/> envision	envision	NONE	NONE

EditList All

The **Edit CTI User** screen is displayed, as shown below. Check the **Unrestricted Access** checkbox and click **Apply Changes**. This will provide the user with unrestricted access.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Security | Security Database | CTI Users | List All Users Home | Help | Logout

AE Services

- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security**
 - Account Management
 - Audit
 - Certificate Management
 - Enterprise Directory
 - Host AA
 - PAM
 - Security Database**
 - Control
 - CTI Users**
 - List All Users
 - Search Users
 - Devices
 - Device Groups
 - Tlinks
 - Tlink Groups
 - Worktops

Edit CTI User

User Profile:

User ID	Common Name	Upstream
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>

Call Origination and Termination / Device Status

None

Call and Device Monitoring:

Device	None
Call / Device	None
Call	<input type="checkbox"/>

Routing Control:


Allow Routing on Listed Devices

None

Apply Changes Cancel Changes

5.4. Restart TSAPI Service

Select **Maintenance** → **Service Controller**. The **Service Controller** screen shows a listing of the services and the associated status of each service. Check the **TSAPI Service** and click on **Restart Service**.

**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input 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

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

© 2009 Avaya, Inc. All Rights Reserved.

The following **Restart Service** screen is displayed. Click on **Restart** to confirm.

The screenshot displays the Avaya Application Enablement Services Management Console. The interface includes a top header with the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for user 'craft' with login details. A red navigation bar contains 'Maintenance | Service Controller' and links for 'Home | Help | Logout'. A left sidebar lists various system components, with 'Maintenance' expanded to show 'Service Controller' as the active selection. The main content area features a 'Restart Service' dialog box with a warning message and two buttons: 'Restart' and 'Cancel'.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Fri Jul 23 13:35:28 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Maintenance | Service Controller Home | Help | Logout

Restart Service

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

Restart Cancel

© 2009 Avaya, Inc. All Rights Reserved.

6. Configure Upstream Works CMA

This section provides the procedures for configuring Upstream Works CMAS. The procedures include the following areas:

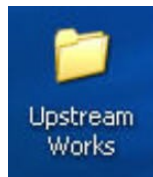
- Load Switch Devices
- Enable Agent Devices
- Enable VDN and ACD/Skill devices
- Administer Agent Workstations
- Administer Agent Logins
- Save Configuration Changes

Note: There is no configuration necessary on the Upstream Works CMA client, as all agent workstation login name and password are administered on the server. However, during the installation of the client, the IP address of the CMAS must be provided for the client to obtain its configuration data.

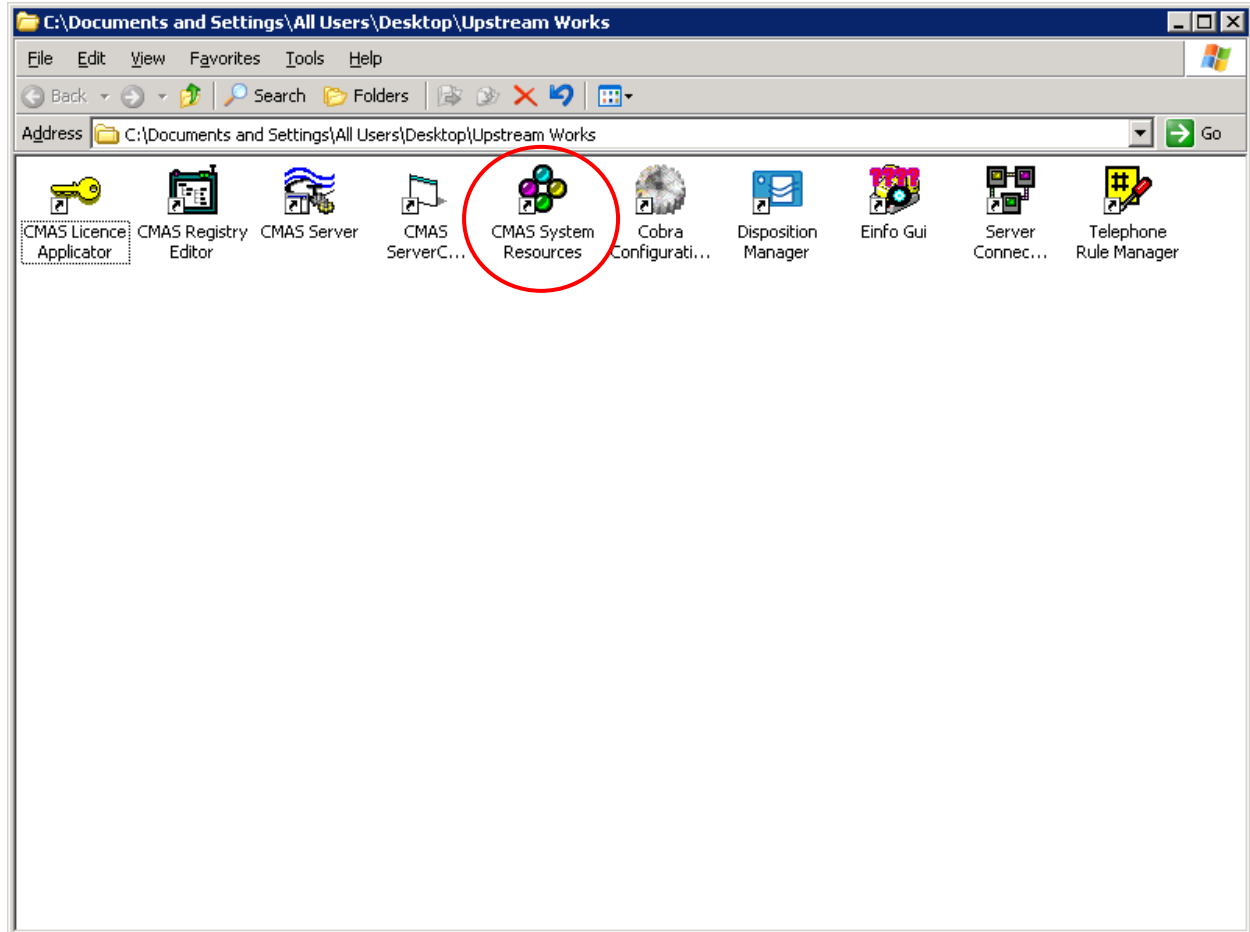
Prior to any configuration, copy the captured files from Communication Manager in **Section 4.4** to a directory on Upstream Works CMAS.

6.1. Load Switch Devices

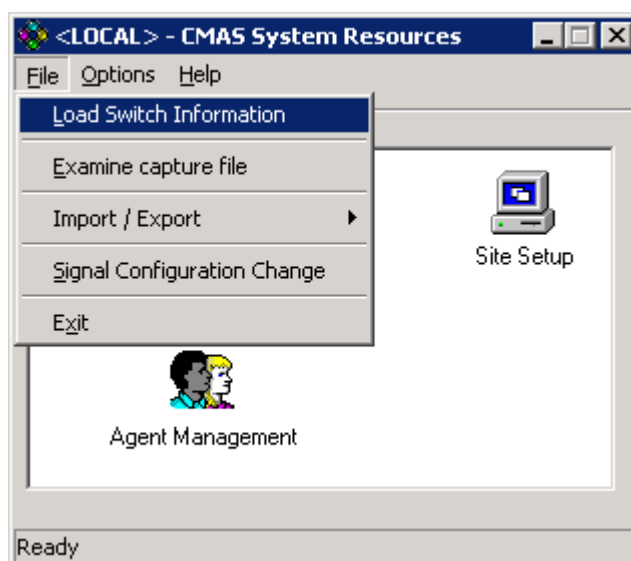
From Upstream Works CMAS, double-click on the Upstream Works folder icon shown below. This icon is created as part of the Upstream Works CMAS installation.



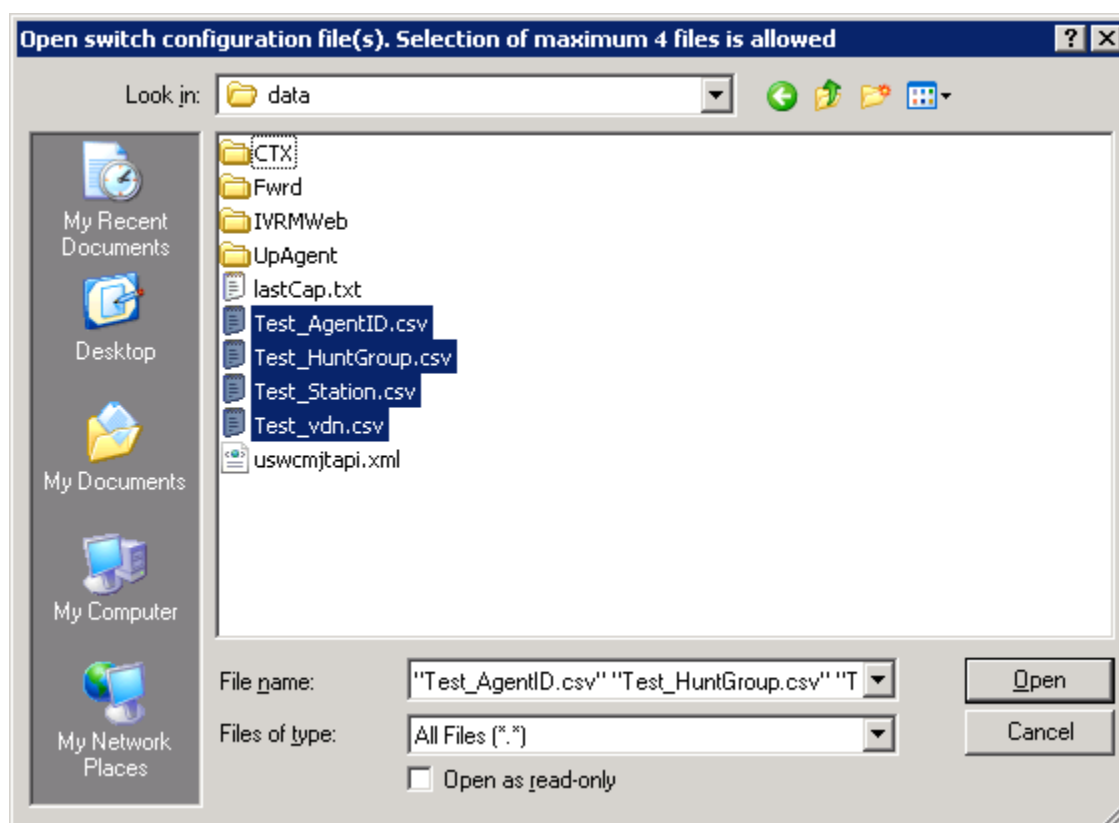
The screen below is displayed. Double-click on **CMAS System Resources**.



The **CMAS System Resources** screen is displayed. Select **File → Load Switch Information** as shown below, to load all switch device information captured from **Section 4.4**.

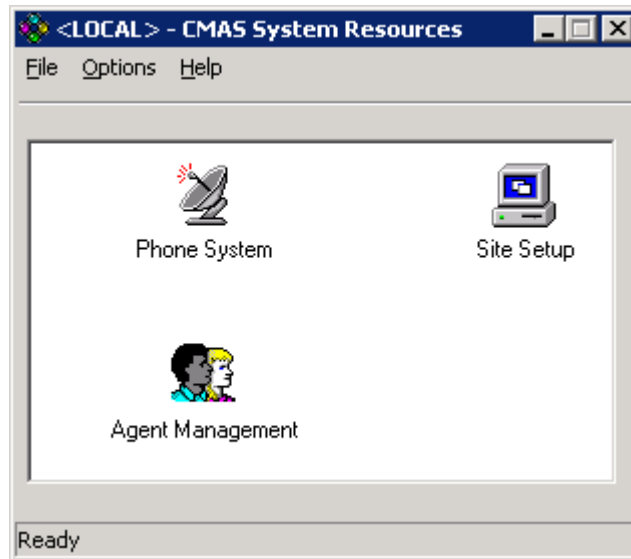


The **Open switch configuration file(s)** dialog box is displayed next. Navigate to the directory where the captured contact center device information from Communication Manager is stored. Select these files and click **Open**.

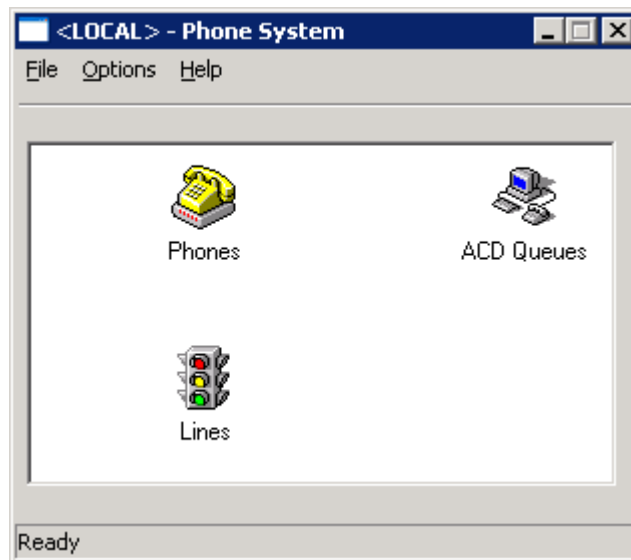


6.2. Enable Agent Devices

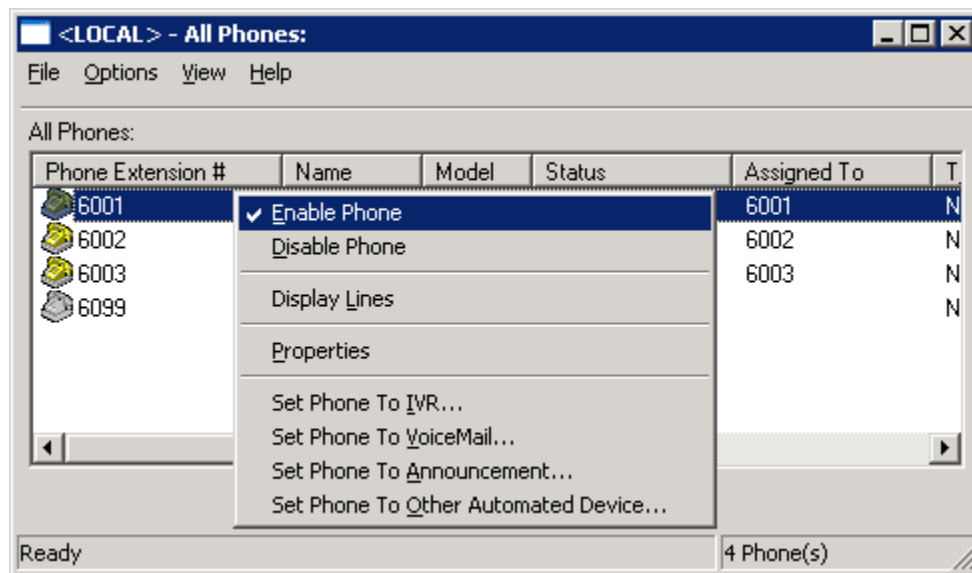
The **CMAS System Resources** screen is displayed again. Double-click on **Phone System**.



The **Phone System** screen is displayed next. Double-click on **Phones** to review all agent device information.

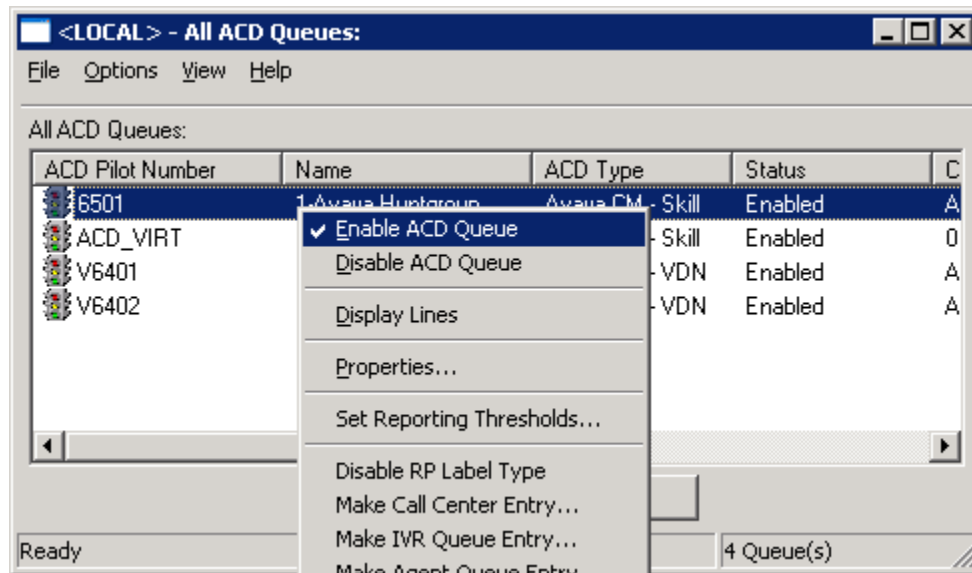


The **All Phones** screen is displayed and filled in with agent device information captured from Communication Manager. By default, all agent devices will be enabled for monitoring, as indicated by the “Enabled” value in the **Status** column. Review the list of agent phone devices, and disable any device that does not need to be monitored. Monitoring can be enabled or disabled by right-clicking on the device **Phone Extension #**, and selecting the appropriate action from the drop down list. After making all necessary changes, close the screen by clicking on the **X** icon in the top right corner of the screen.



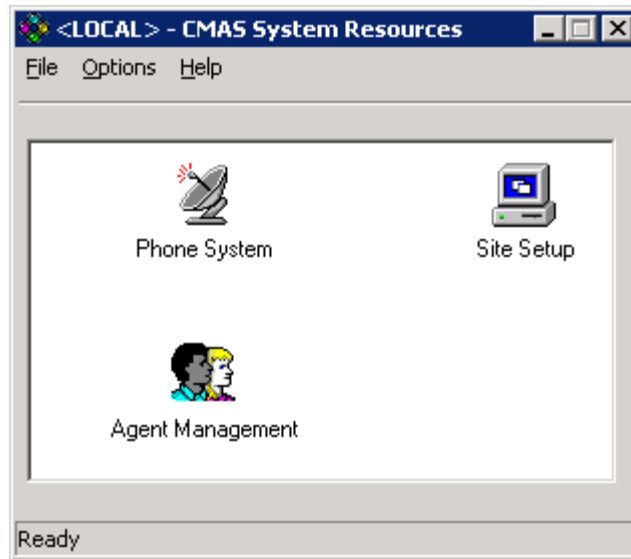
6.3. Enable VDN and ACD/Skill Devices

The **Phone System** screen from **Section 6.2** is displayed again. Double-click on **ACD Queues** to review all VDN and ACD/Skill device information. The **All ACD Queues** screen is displayed, and filled in with VDN and ACD/Skill information captured from Communication Manager. Review the list and follow the procedure in **Section 6.2** to disable any device that does not need to be monitored. Note that the “ACD_VIRT” entry is automatically created and needed by Upstream Works CMAS. After making all necessary changes, close the screen by clicking on the **X** icon in the top right corner of the screen.

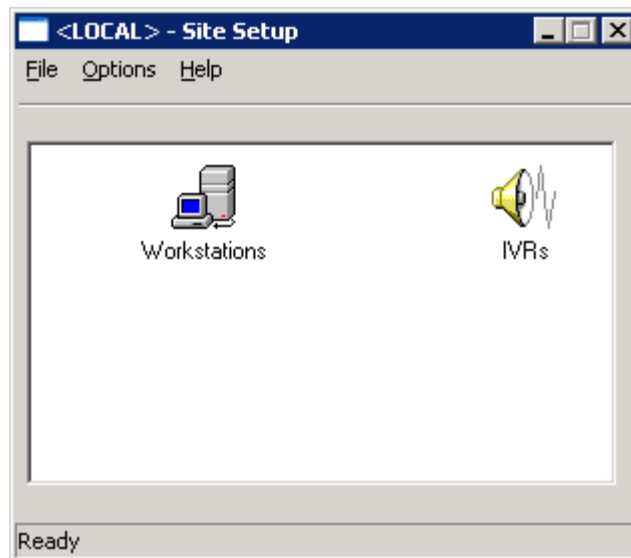


6.4. Administer Agent Workstation

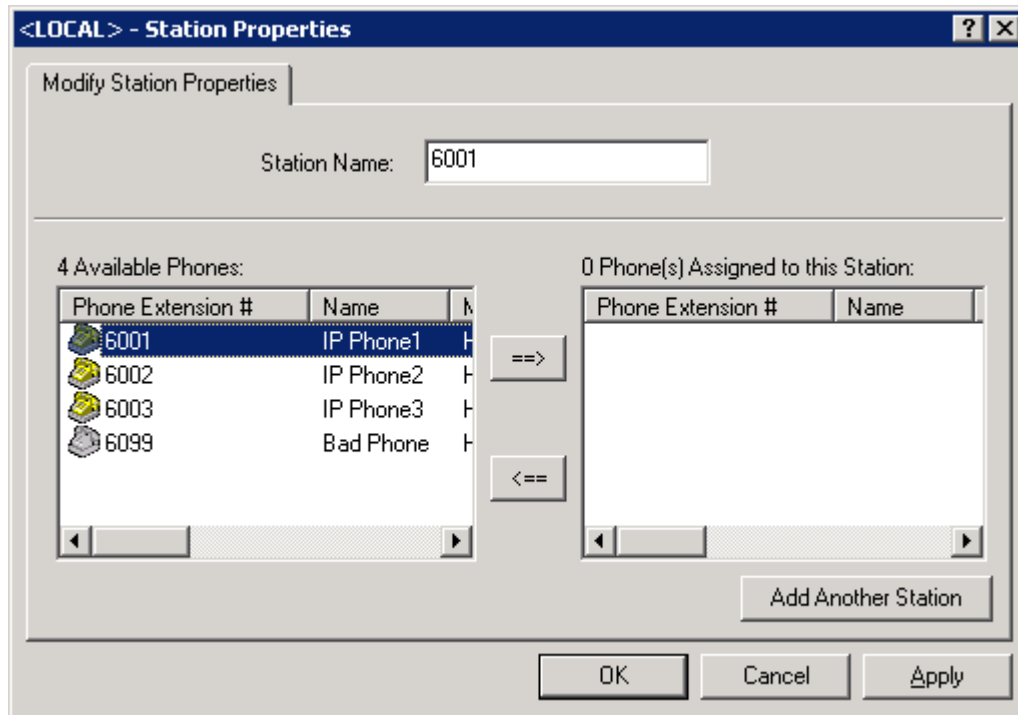
The **Phone System** screen from Section 6.2 is displayed again, close the screen by clicking on the **X** icon in the top right corner. The **CMAS System Resource** screen is displayed next, as shown below. Double-click on **Site Setup**.



In the **Site Setup** screen, double-click on **Workstations** to administer agent workstations.

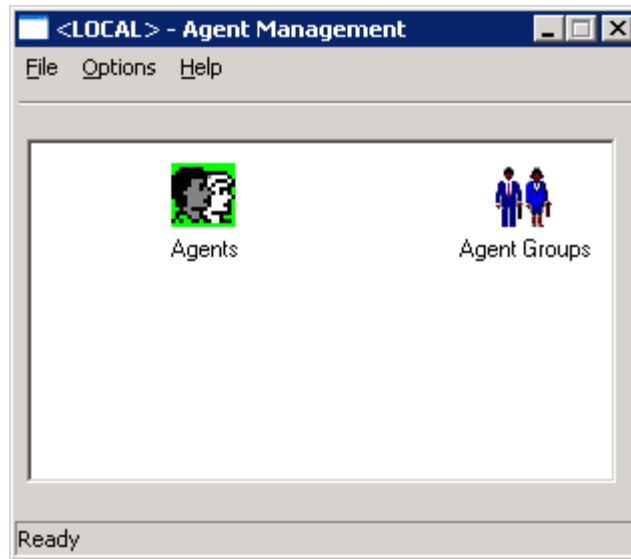


The **Station Properties** screen is displayed next. For each agent workstation, enter the **Station Name**. Select the physical phone extension associated with this agent from the left pane, and use the right arrow icon to move the extension to the right pane. In this case, “6001” is the associated extension, as shown below. Click on **Add Another Station** and repeat this procedure to add all necessary agent workstations. After adding all workstations, click on **OK**.

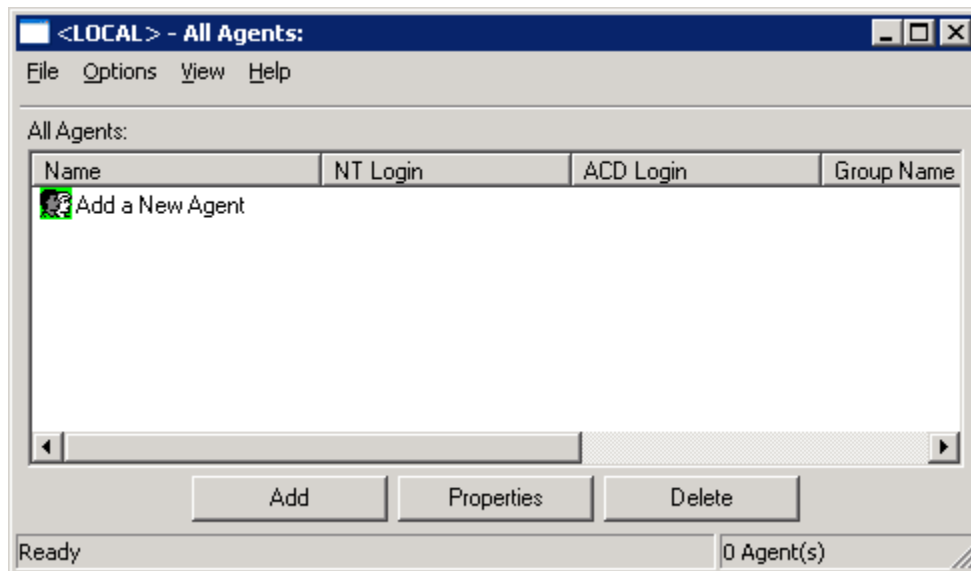


6.5. Administer Agent Logins

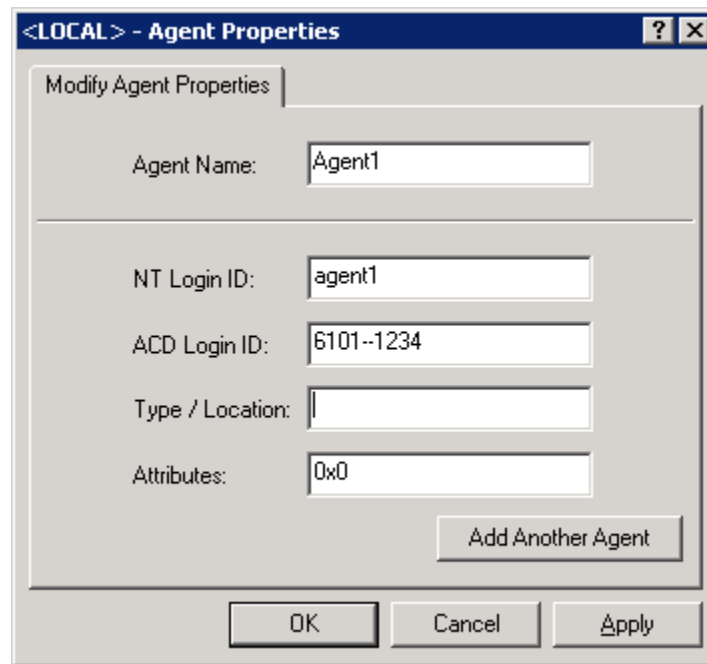
Navigate back to the **CMAS System Resources** screen shown in **Section 6.4**, and double-click on **Agent Management**. In the **Agent Management** screen shown below, double-click on **Agents**.



The **All Agents** screen is displayed. Click on **Add** to add an agent.



In the **Agent Properties** screen, enter a descriptive name for **Agent Name**. For **NT Login ID**, enter the Windows login name that the agent uses to log into the computer. For agents in an Expert Agent Selection (EAS) environment, enter “<logical agent extension>--<logical agent password>” into the **ACD Login ID** field. In this case, “6101” is the logical agent extension, and “1234” is the logical agent password. Note that the two dashes between the extension and password must be maintained. For agents in a non-EAS environment, enter “<physical agent extension>-<ACD group extension>-<physical agent password>” into the **ACD Login ID** field. Click **OK**.



<LOCAL> - Agent Properties

Modify Agent Properties

Agent Name: Agent1

NT Login ID: agent1

ACD Login ID: 6101--1234

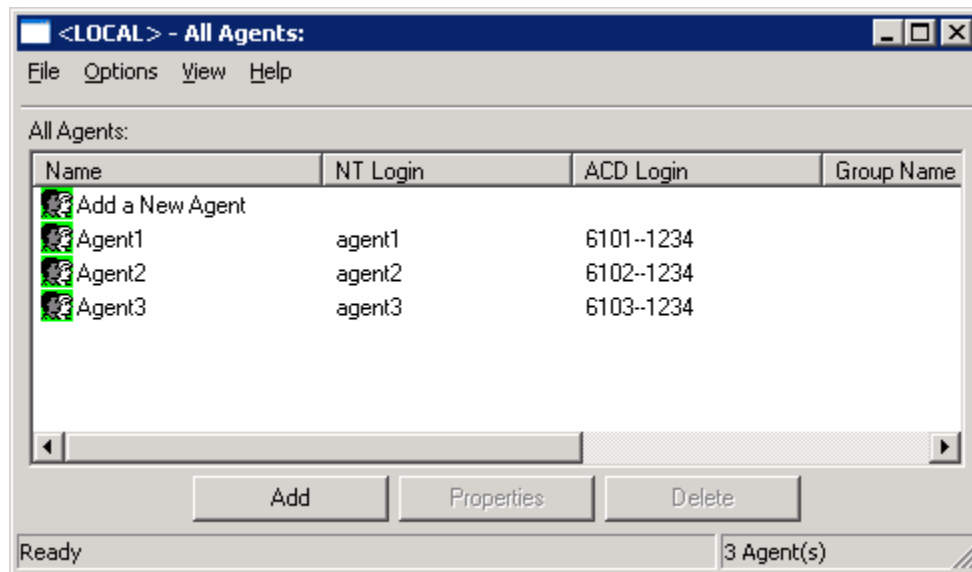
Type / Location:

Attributes: 0x0

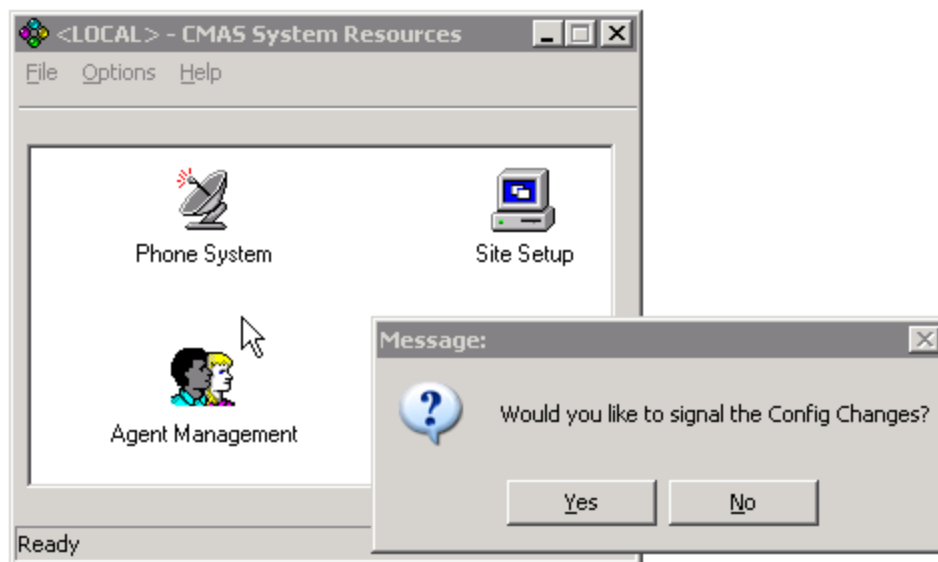
Add Another Agent

OK Cancel Apply

The **All Agents** screen is displayed and updated with the newly added agent, as shown below. Repeat the same procedure to add all remaining agents. After adding all agents, close the screen by clicking on the **X** icon in the top right corner.



Navigate back to the **CMAS System Resources** screen and close the screen by clicking on the **X** icon in the top right corner. A **Message** dialog box is displayed, as shown below. Click on **Yes** to activate the configuration changes.



7. General Test Approach and Test Results

The interoperability compliance testing included feature and serviceability testing.

The feature testing focused on verifying Upstream Works CMAS handling of TSAPI messages in the areas of routing, call control, event notification, value query, and set value. Testing also included rainy day scenarios to verify handling of negative acknowledgements.

The serviceability testing focused on verifying the ability of Upstream Works CMAS to recover from adverse conditions, such as busying out the CTI link and disconnecting the Ethernet cable from Communication Manager, Application Enablement Services, and CMAS.

7.1. General Test Approach

The feature test cases were performed both automatically and manually. Upon start of the Upstream Works CMAS application, the application automatically queries Communication Manager for device status and requests monitoring and routing.

For the manual part of the testing, incoming calls were made to the adjunct routing VDN. Upstream Works CMAS specifies where to route each call, based on agent status information that the application keeps track of from the TSAPI event reports received from Communication Manager. Manual call controls from both the agent desktop and the agent telephones were exercised to verify call control and event reports associated with features such as conferencing and transferring of calls.

The serviceability test cases were performed manually by busying out and releasing the CTI link, and by disconnecting and reconnecting the LAN cables from Upstream Works CMAS, Application Enablement Services, and Communication Manager.

The verification of all tests included checking for the proper states at the agent telephones and workstations, and verifying the TSAPI message traces from Upstream Works CMAS.

7.2. Test Results


All feature test cases were executed and passed.

8. Verification Steps

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

8.1. Verify Avaya Aura™ Application Enablement Services

On Application Enablement Services, verify the status of the switch connection by selecting **Status → Status and Control → Switch Conn Summary** from the left pane. Verify that the **Conn State** is “Talking” for the relevant switch connection. In this case, the switch connection is “S8300DCM6”.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:36:37 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Status | Status and Control | Switch Conn 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

Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Since	Online/Offline	Active/ Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
	S8300DCM6	Talking	Wed Jul 21 10:06:28 2010	Online	1 / 1	2	Enabled	614	629	30
	S8300mobile	Talking	Wed Jul 21 09:56:46 2010	Online	1 / 1	2	Enabled	615	630	30
	devcon31	Talking	Wed Jul 21 09:56:46 2010	Online	1 / 1	2	Enabled	615	630	30

Online

Offline

Connection Details

Per Service Connections Details

© 2009 Avaya, Inc. All Rights Reserved.

Verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is “Talking” for the TSAPI link administered in **Section 4.2**, as shown below.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jul 23 13:36:37 2010 from 10.64.10.51
HostName/IP: aesserver2/205.168.62.111
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Status | Status and Control | TSAPI 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

TSAPI Link Details

☐ Enable page refresh every seconds

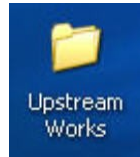
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	S8300mobile	1	Talking	Wed Jul 21 09:57:19 2010	Online	14	0	15	15	30
	2	devcon31	1	Talking	Wed Jul 21 09:57:19 2010	Online	15	0	15	15	30
	3	S8300DCM6	1	Talking	Fri Jul 23 13:41:04 2010	Online	16	0	15	15	30

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

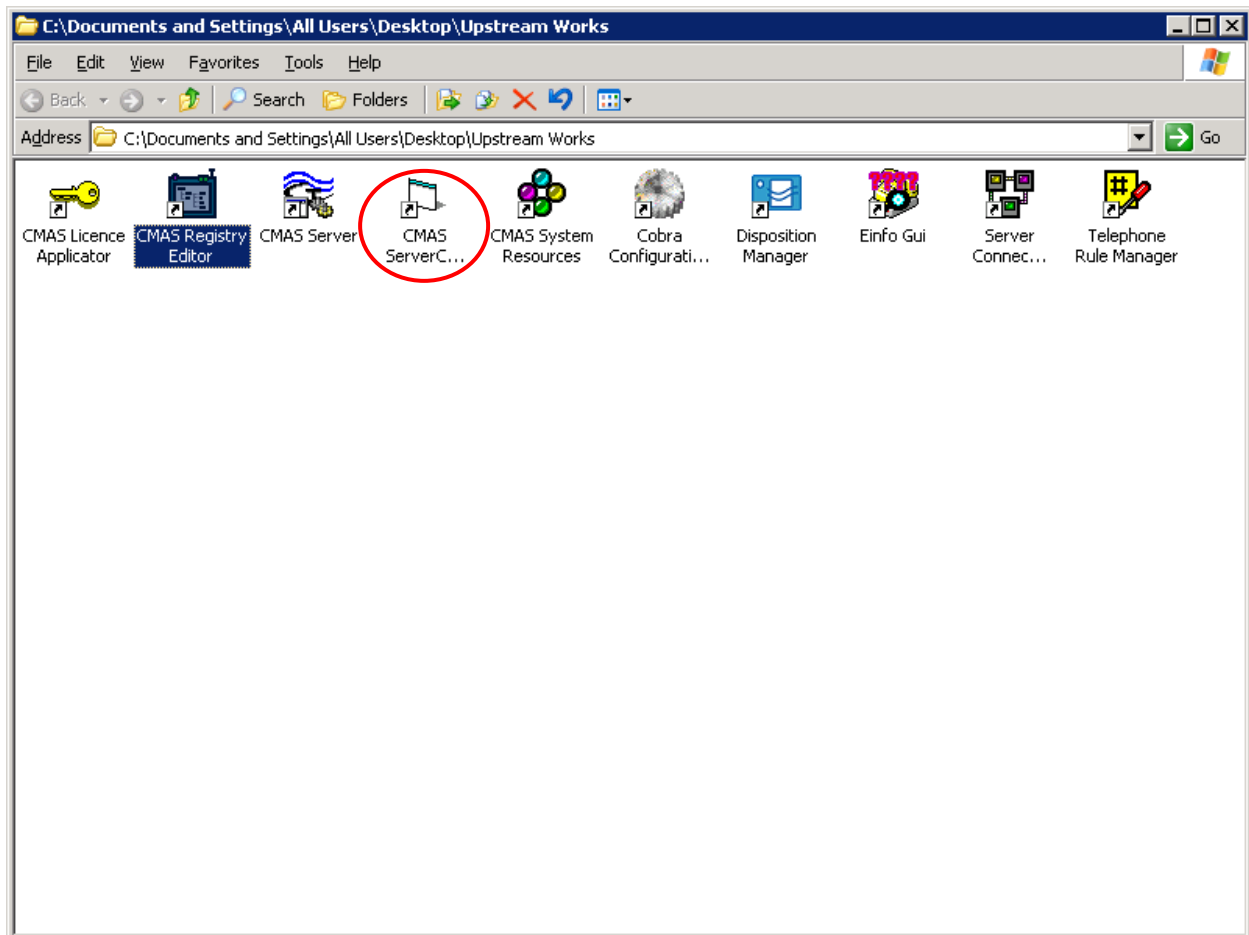
© 2009 Avaya, Inc. All Rights Reserved.

8.2. Verify Upstream Works Call Management Automation Server

From the Upstream Works CMAS, double-click on the **Upstream Works** folder icon.

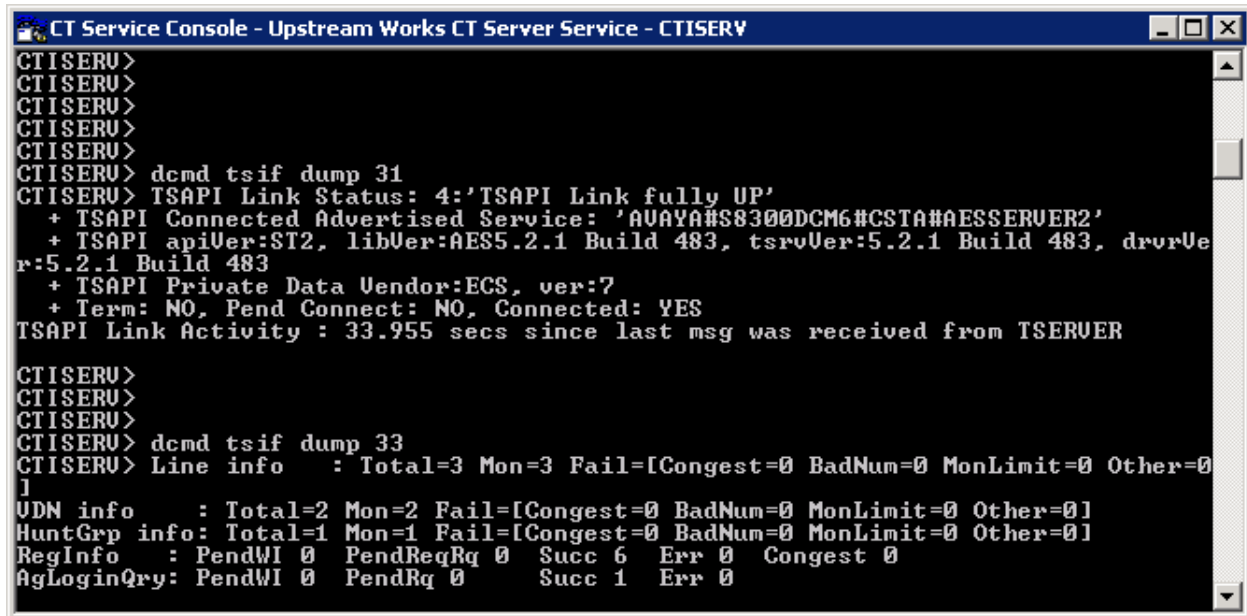


The **Upstream Works** screen is displayed. Double-click on **CMAS ServerConsole**.



In the **CT Service Console** screen, enter the command “dcmd tsif dump 31” to display the status of the TSAPI link. Verify that the status is “TSAPI Link fully UP”, as shown below.

Enter the command “dcmd tsif dump 33” to display a summary of the monitored devices. As shown in the screen below, three agents are shown to be monitored in the **Line info** line, two VDNs shown in the **VDN info** line, and one ACD/Skill group shown in the **HuntGrp info** line.



```
CT Service Console - Upstream Works CT Server Service - CTISERV
CTISERV>
CTISERV>
CTISERV>
CTISERV>
CTISERV>
CTISERV> dcmd tsif dump 31
CTISERV> TSAPI Link Status: 4:'TSAPI Link fully UP'
+ TSAPI Connected Advertised Service: 'AVAYA#S8300DCM6#CSTA#AESSEVER2'
+ TSAPI apiVer:ST2, libVer:AES5.2.1 Build 483, tsrvVer:5.2.1 Build 483, drvrVer:5.2.1 Build 483
+ TSAPI Private Data Vendor:ECS, ver:7
+ Term: NO, Pend Connect: NO, Connected: YES
TSAPI Link Activity : 33.955 secs since last msg was received from TSERVER

CTISERV>
CTISERV>
CTISERV>
CTISERV> dcmd tsif dump 33
CTISERV> Line info      : Total=3 Mon=3 Fail=[Congest=0 BadNum=0 MonLimit=0 Other=0]
VDN info      : Total=2 Mon=2 Fail=[Congest=0 BadNum=0 MonLimit=0 Other=0]
HuntGrp info: Total=1 Mon=1 Fail=[Congest=0 BadNum=0 MonLimit=0 Other=0]
RegInfo      : PendWI 0  PendReqRq 0  Succ 6  Err 0  Congest 0
AgLoginQry: PendWI 0  PendRq 0  Succ 1  Err 0
```

9. Conclusion

These Application Notes describe the configuration steps required for the Upstream Works Call Management Automation Server 7.60 to interoperate with Avaya Aura™ Communication Manager 6.0 using Avaya Aura™ Application Enablement Services 5.2.2. All feature and serviceability test cases were completed successfully.

10. Additional References

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

- *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Release 6.0, Issue 6.0, June 2010, available at <http://support.avaya.com>.
- *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Document ID 02-300357, Release 5.2, Issue 11, November 2009, available at <http://support.avaya.com>.
- *Upstream Works CMA Server Installation Guide*, Version 7.60, available from Upstream Works
- *Upstream Works CMA Server Operations Manual*, Version 7.60, available from Upstream Works

©2010 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.