Avaya Solution & Interoperability Test Lab

Application Notes for VXI China VisionWFM 3.0 with Avaya Call Management System Release 16 and Avaya Aura® Application Enablement Services 5.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate VXI China VisionWFM 3.0 with Avaya Call Management System (CMS) Release 16 and Avaya Aura® Application Enablement Services 5.2 to capture real-time call center data from Avaya Aura® Communication Manager. VisionWFM is a workforce management solution for the management of business operation such as improving quality and reduce operating costs. VisionWFM uses the Generic Real Time Adherence (RTA) interface to capture real-time agent work-mode changes from Avaya CMS. This interface is provided by Avaya Professional Services. VisionWFM also uses the Telephony Services Application Programming Interface (TSAPI) to monitor the agent extensions for real-time call information and status.

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 to integrate VXI China VisionWFM 3.0 with Avaya Call Management System (CMS) Release 16 and Avaya Aura® Application Enablement Services 5.2 to capture real-time call center data from Avaya Aura® Communication Manager. VisionWFM is a workforce management solution for the management of business operation such as improving quality and reduce operating costs. VisionWFM uses the Generic Real Time Adherence (Generic-RTA) interface to capture real-time agent work-mode changes from Avaya CMS. This interface is provided by Avaya Professional Services. VisionWFM also uses the Telephony Services Application Programming Interface (TSAPI) interface to Application Enablement Services to monitor the agent extensions for real-time call information and status.

The Generic-RTA interface software on Avaya CMS connects to the VisionWFM server and sends data to the VisionWFM application every 10 seconds (configurable). Avaya Professional Services installs and configures the Generic-RTA interface on Avaya CMS, and provides the TCP port number associated with the Generic-RTA session to VXI China for configuring VisionWFM.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying that a Generic-RTA connection can be established between Avaya CMS and VisionWFM server and that VisionWFM can parse and display the real-time agent data in VisionWFM. The feature testing also verifys that VisionWFM can capture call related information such as talk-time, calls abandoned and calls answered using the TSAPI interface.

The serviceability testing focused on verifying the ability of VisionWFM to recover from adverse conditions, such as disrupting the network connection to the VisionWFM server and rebooting the VisionWFM server.

2.1. Interoperability Compliance Testing

The feature test cases were performed manually. Incoming calls were made to the monitored split/skills to generate data streams with agent state changes to be sent to VisionWFM. Manual call controls and work mode changes from agent telephones were exercised as necessary to generate the required real-time data.

The serviceability test cases were performed manually by removing the network connection to the VisionWFM server and rebooting the VisionWFM server.

The verification of all tests included checking the proper display and data accuracy of real-time agent data in VisionWFM.

2.2. Test Results

All test cases were executed and passed.

2.3. Support

For technical support on VisionWFM, contact VXI China as shown below.

- **Web:** http://www.vxichina.com/about/contact.asp
- **Toll-free hotline:** +86 800 820 2040 (China only)

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the solution. VXI China VisionWFM was installed on a Microsoft Windows 2003 Server with Service Pack 2, with the client PC using the Microsoft Internet Explorer 7.0 to access the VisionWFM Server. Calls were placed to the Vector Directory Numbers (VDNs) and were answered by the agent telephones connected to Avaya Aura® Communication Manager. Call related information was captured by Avaya Aura® Application Enablement Services and sent to VisionWFM using the TSAPI interface. The Avaya Call Management System was used to capture the agent work mode changes to generate the real-time data used in this testing.

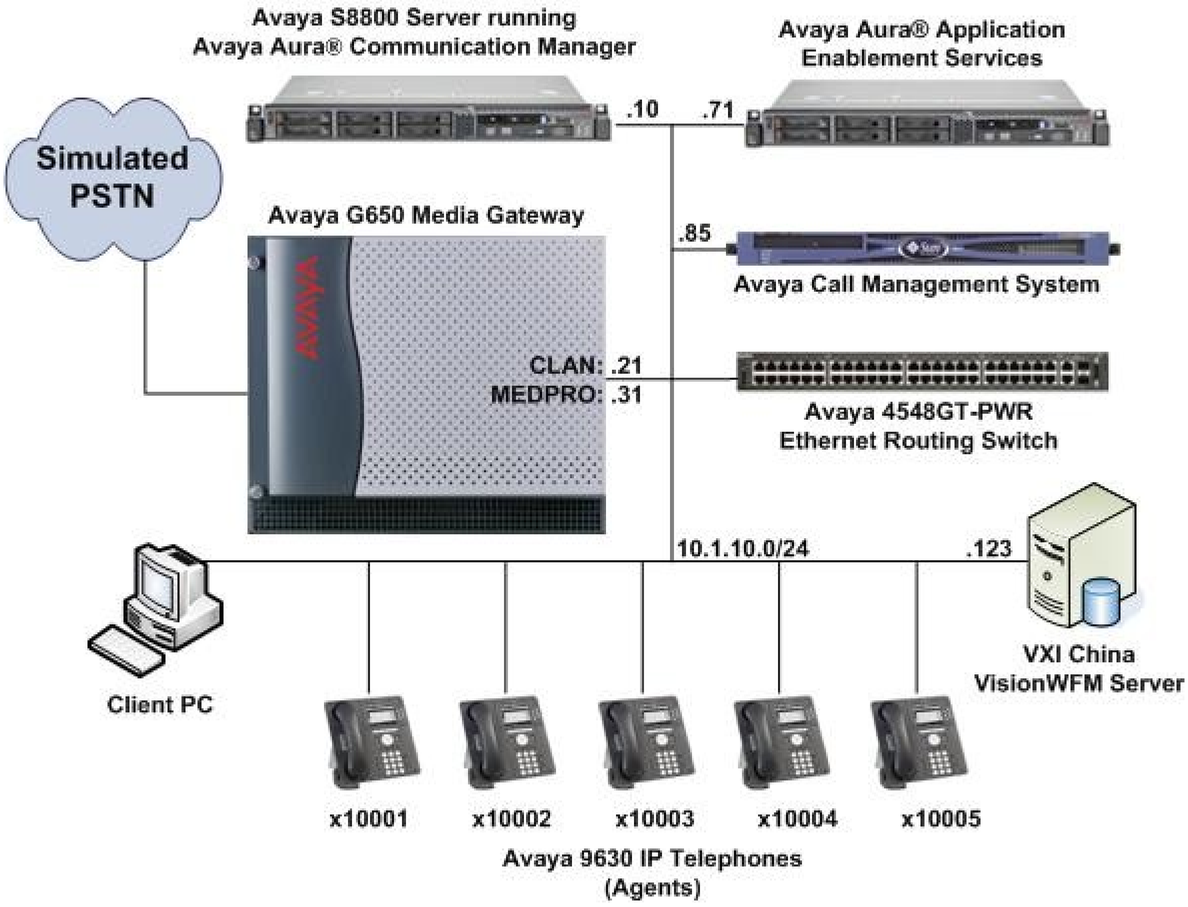


Figure 1: VXI China VisionWFM with Avaya Call Management System

4. Equipment and Software Validated

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

Equipment	Software
Avaya Call Management System	R16 (r16aa.m)
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0 (Service Pack 00.0.345.0-18567)
Avaya Aura® Application Enablement Services	5.2.2 Patch 3
Avaya G650 Media Gateway • TN2312BP IP Server Interface • TN799DP C-LAN Interface • TN2302AP IP Media Processor	- HW07, FW053 HW01, FW039 HW20, FW121
Avaya 9630 IP Telephones	3.1 Service Pack 1 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
Microsoft Windows Server 2003 Standard Edition	Service Pack 2
VXI China VisionWFM	3.0

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager software options
- Administer adjunct CMS release
- Administer IP node name for CMS
- Administer processor interface channel
- Administer measured Skilled Hunt Group
- Configure AES and CTI Links

The detailed administration of contact center devices such as Skilled Hunt Group, VDN, Vector, and Agents are assumed to be in place. These Application Notes will only cover how to enable Skilled Hunt Group and Agent data to be sent to Avaya CMS.

5.1. Verify Communication Manager Software Options

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 **G3 Version** field is set to **V16** on Page 1, as shown below.

```
display system-parameters customer-options                      Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                             Software Package: Enterprise
       Location: 2                                System ID (SID): 1
       Platform: 28                               Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 65000 280
                                      Maximum Stations: 1000  166
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 1000  0
                    Maximum Off-PBX Telephones -   OPS: 1000  15
                    Maximum Off-PBX Telephones - PBFMC: 1000  0
                    Maximum Off-PBX Telephones - PVFMC: 1000  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 10    1

        (NOTE: You must logoff & login to effect the permission changes.)
```

Navigate to Page 6, and verify that the **Call Center Release** field is set to 6**.0**, as shown below.

```
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.)
```

5.2. Administer Adjunct CMS Release

Use the **change system-parameters features** command and navigate to **Page 12**. Set the **CMS (appl mis)** field to the software release of the Avaya CMS. In this case, **R15/R16** is used to correspond to Avaya CMS software release R16.

```
change system-parameters features                               Page  12 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

  AGENT AND CALL SELECTION
                         MIA Across Splits or Skills? n
                          ACW Agents Considered Idle? y
                          Call Selection Measurement: current-wait-time
    Service Level Supervisor Call Selection Override? n
                                 Auto Reserve Agents: none


  CALL MANAGEMENT SYSTEM
                           REPORTING ADJUNCT RELEASE
                                      CMS (appl mis): R15/R16
                                      IQ  (appl ccr):

                               BCMS/VuStats LoginIDs? y
                   BCMS/VuStats Measurement Interval: hour
           BCMS/VuStats Abandon Call Timer (seconds):
                     Validate BCMS/VuStats Login IDs? n
                            Clear VuStats Shift Data: on-login
                 Remove Inactive BCMS/VuStats Agents? n
```

5.3. Administer IP Node Name for CMS

Use the **change node-names ip** command, to add an entry for Avaya CMS. In this case, **cms1** and **10.1.10.85** are entered as **Name** and **IP Address** for the Avaya CMS server. The actual node names and IP addresses may vary. Submit these changes.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Gateway001          10.1.10.1
cms1                10.1.10.85
default             0.0.0.0
msgserver           10.1.10.20
procr               10.1.10.10
```

5.4. Administer Processor Interface Channel

Assign a new processor interface channel with the **change communication-interface processor-channels** command. Add an entry with the following values, and submit these changes.

- **Enable:** “y”.
- **Appl.:** “mis”.
- **Mode:** “s” for server mode.
- **Interface Link:** “pv4” for processor ethernet running IP version 4 (IPv4).
- **Interface Chan:** TCP channel number for Avaya CMS. In this case “5001”.
- **Destination Node:** Avaya CMS server node name from **Section 5.3**.
- **Destination Port:** “0”.
- **Session Local:** Corresponding channel number in **Proc Chan** field. In this case “1”.
- **Session Remote:** Corresponding channel number in **Proc Chan** field. In this case “1”.

The **Interface Chan** field contains the Avaya CMS TCP channel number, which is defined as part of the Avaya CMS installation. For the compliance testing, the default TCP channel number of **5001** was used. Refer to **Section 6.1** to verify the settings on Avaya CMS.

```
change communication-interface processor-channels              Page   1 of  24
                        PROCESSOR CHANNEL ASSIGNMENT
Proc                 Gtwy      Interface         Destination      Session   Mach
Chan Enable   Appl.   To  Mode Link/Chan       Node       Port  Local/Remote ID
  1:   y    mis            s    pv4 5001  cms1            0      1     1
```

5.5. Administer Measured Skilled Hunt Group

Use the **change hunt-group n** command, where **n** is the hunt group number to be measured by Avaya CMS. On Page 2, set the **Measured** field to **external** or **both** to enable real-time measurement data on the skilled hunt group and the associated agents to be sent to Avaya CMS. Repeat this step for all skilled hunt groups that will be measured by Avaya CMS.

```
change hunt-group 1                                             Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: both
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:
 Timed ACW Interval (sec):
   Multiple Call Handling: none
```

5.6. Configure AES and CTI Links

Application Enablement Services forwards CTI requests, responses, and events between VisionWFM server and Communication Manager. Application Enablement Services communicates with Communication Manager over an AES link. Within the AES link, CTI links are configured to provide CTI services to CTI applications such as VisionWFM. The following steps demonstrate the configuration of the Communication Manager side of the AES and CTI links. See **Section 7** for the details of configuring the Application Enablement Services side of the AES and CTI links.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enter the <b>display system-parameters customer-options</b> command. On Page 3, verify that <b>Computer Telephony Adjunct Links</b> is set to <b>y</b>. If not, contact an authorized Avaya account representative to obtain the license.
<pre>
display system-parameters customer-options   Page   3 of 11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n   Audible Message Waiting? n
        Access Security Gateway (ASG)? n   Authorization Codes? y
        Analog Trunk Incoming Call ID? n   CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n   CAS Main? n
Answer Supervision by Call Classifier? n   Change COR by FAC? n
                                 ARS? y Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? n
          ARS/AAR Dialing without FAC? y   DCS (Basic)? n
          ASAI Link Core Capabilities? n   DCS Call Coverage? n
          ASAI Link Plus Capabilities? n   DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n   Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n   DS1 MSP? y
                                ATMS? n   DS1 Echo Cancellation? y
                  Attendant Vectoring? n
</pre></td></tr>
<tr><td>2.</td><td>Enter the <b>add cti-link n</b> command, where <b>n</b> is a number between 1 and 64, inclusive. Enter a valid <b>Extension</b> under the provisioned dial plan in Avaya Communication Manager, set the <b>Type</b> field to <b>ADJ-IP</b>, and assign a descriptive <b>Name</b> to the CTI link. The CTI Link number corresponds to the <b>Switch CTI Link Number</b> in <b>Section 7.4 Step 2</b>.
<pre>
add cti-link 1   Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 10091
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI Services
</pre></td></tr>
</table>

Step	Description
3.	Enter the **change ip-services** command. On Page 1, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. During the compliance test, the **Local Node** field is set to the processor Ethernet interface **procr** which is IP address of the S8800 Server as shown in **Figure 1**. The default port **8765** was utilized for the **Local Port** field.

```
change ip-services                                                Page   1 of   3

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS          y       procr            8765
```

On Page 3, enter the hostname of the Application Enablement Services server for the **AE Services Server** field. The server name may be obtained by logging in to the Application Enablement Services server using Secure Shell (SSH), and running the **uname -a** command. Enter an alpha-numeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services server in **Section 7.3 Step 2**.

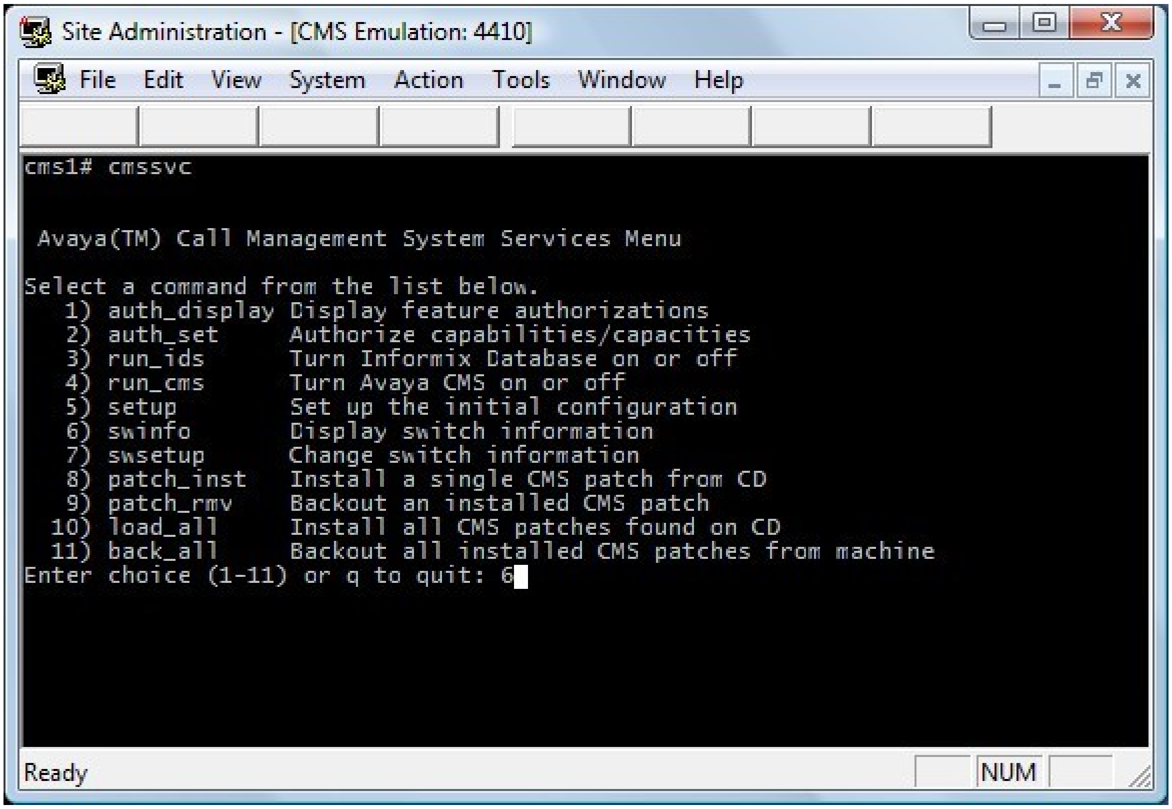
```
change ip-services                                                Page   3 of   3
                              AE Services Administration

   Server ID     AE Services        Password           Enabled     Status
                    Server
      1:        aes1                xxxxxxxxxxxxxxxx        y
      2:
      3:
```

6. Configure Avaya Call Management System

The initial configuration of Avaya Call Management System to interface with Communication Manager is assumed to be in place and thus will not be described in these application notes. Refer to Reference [2] for further information.

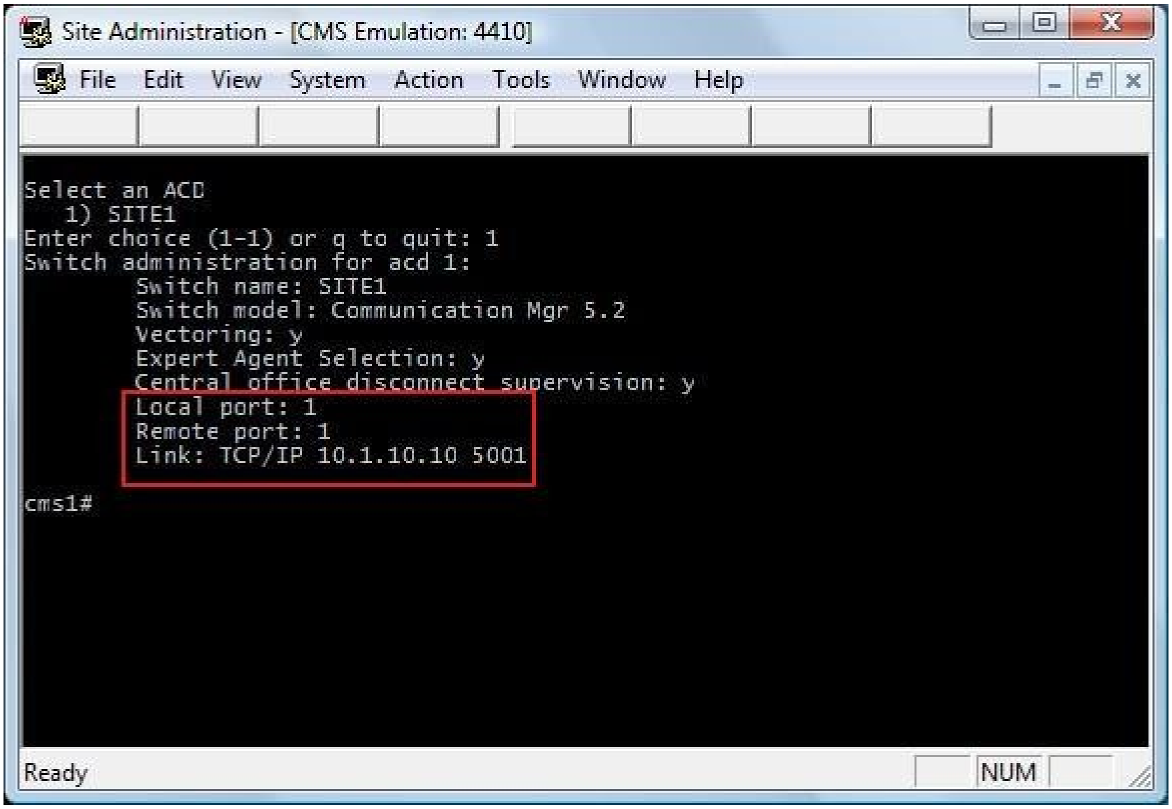
6.1. Verify CMS Setup

Use a terminal emulator to connect to the Avaya CMS server, and log in with the proper credentials. Enter “cmssvc” at the command prompt to display the **Avaya Call Management System Services Menu** screen. Select “6” to display the switch information.



```
cms1# cmssvc


 Avaya(TM) Call Management System Services Menu

Select a command from the list below.
   1) auth_display Display feature authorizations
   2) auth_set     Authorize capabilities/capacities
   3) run_ids      Turn Informix Database on or off
   4) run_cms      Turn Avaya CMS on or off
   5) setup        Set up the initial configuration
   6) swinfo       Display switch information
   7) swsetup      Change switch information
   8) patch_inst   Install a single CMS patch from CD
   9) patch_rmv    Backout an installed CMS patch
  10) load_all     Install all CMS patches found on CD
  11) back_all     Backout all installed CMS patches from machine
Enter choice (1-11) or q to quit: 6
```

Enter “1” to select the ACD defined. Verify that the **Local port**, **Remote port** and **Link** correspond to the configuration on Communication Manager in **Section 5.4**.

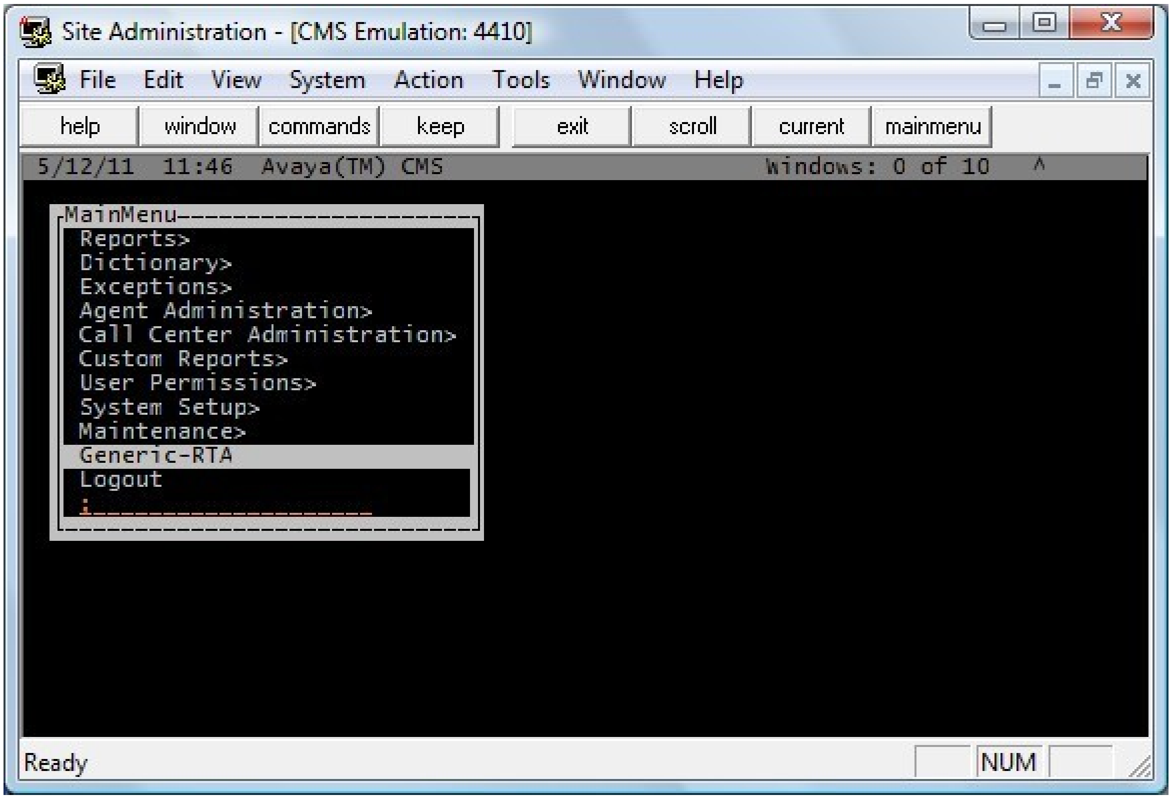

Site Administration - [CMS Emulation: 4410]
File Edit View System Action Tools Window Help
Ready
NUM

```
Select an ACD
   1) SITE1
Enter choice (1-1) or q to quit: 1
Switch administration for acd 1:
        Switch name: SITE1
        Switch model: Communication Mgr 5.2
        Vectoring: y
        Expert Agent Selection: y
        Central office disconnect supervision: y
        Local port: 1
        Remote port: 1
        Link: TCP/IP 10.1.10.10 5001

cms1#
```

6.2. Configure Generic-RTA Interface

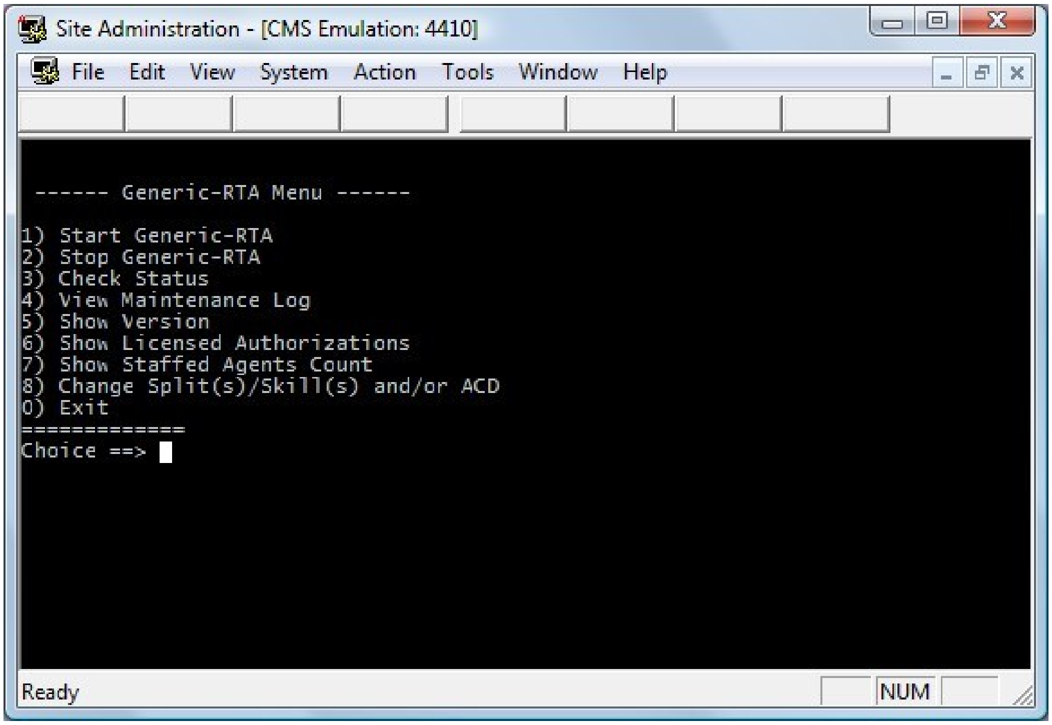
Configuration of the Generic-RTA interface is performed by Avaya Professional Services and is outside the scope of these Application Notes. After the interface is configured, the user can follow the procedure below to start the interface. For this testing, the Generic-RTA interface connects to the VisionWFM server on TCP port 6996. The port number is specified in the configuration file **rta.conf** located in the directory where Generic-RTA is installed.

Use a terminal emulator to connect to the Avaya CMS server, and log in with the proper credentials. Enter “cms” at the command prompt to display the **MainMenu** screen. Select the option that corresponds to **Generic-RTA** and press the **Enter** key.



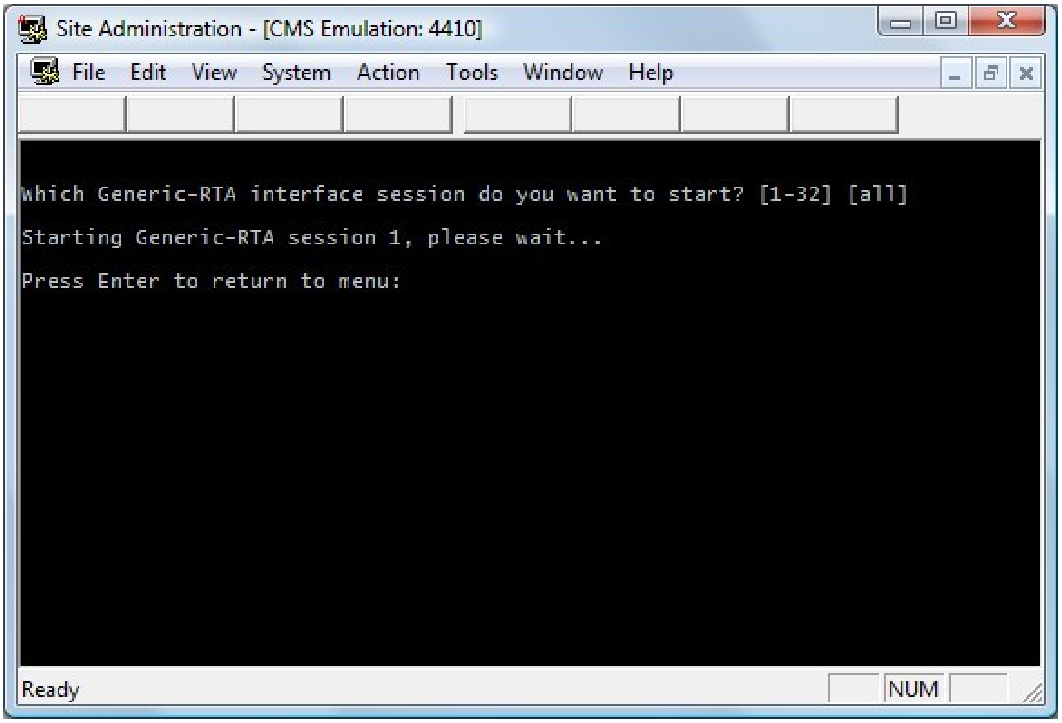
```
5/12/11  11:46  Avaya(TM) CMS                   Windows: 0 of 10   ^

 MainMenu
  Reports>
  Dictionary>
  Exceptions>
  Agent Administration>
  Call Center Administration>
  Custom Reports>
  User Permissions>
  System Setup>
  Maintenance>
  Generic-RTA
  Logout
  :____________________
```

The **Generic-RTA Menu** is displayed as shown below. Enter “1” to start the interface.


Site Administration - [CMS Emulation: 4410]
File Edit View System Action Tools Window Help
Ready
NUM

```
 ------ Generic-RTA Menu ------

1) Start Generic-RTA
2) Stop Generic-RTA
3) Check Status
4) View Maintenance Log
5) Show Version
6) Show Licensed Authorizations
7) Show Staffed Agents Count
8) Change Split(s)/Skill(s) and/or ACD
0) Exit
=============
Choice ==>
```

Enter “all” for all sessions.


Site Administration - [CMS Emulation: 4410]
File Edit View System Action Tools Window Help
Ready
NUM

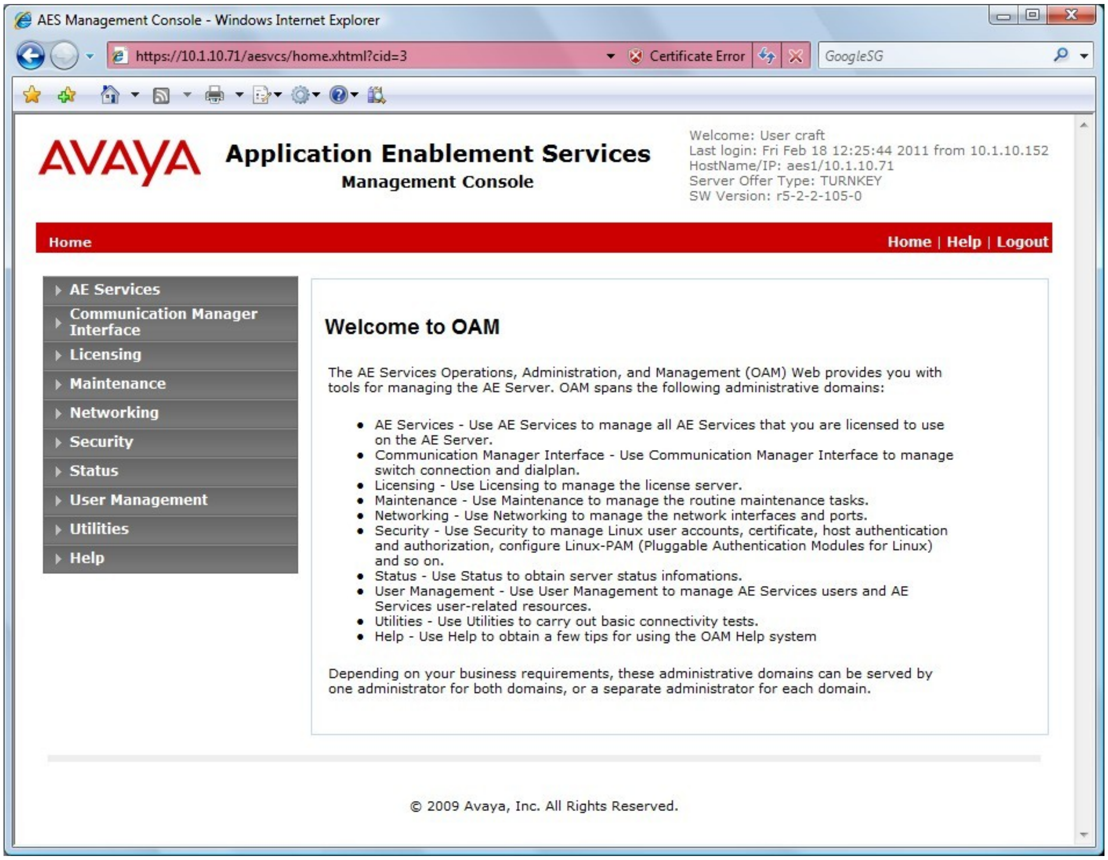
```
Which Generic-RTA interface session do you want to start? [1-32] [all]

Starting Generic-RTA session 1, please wait...

Press Enter to return to menu:
```

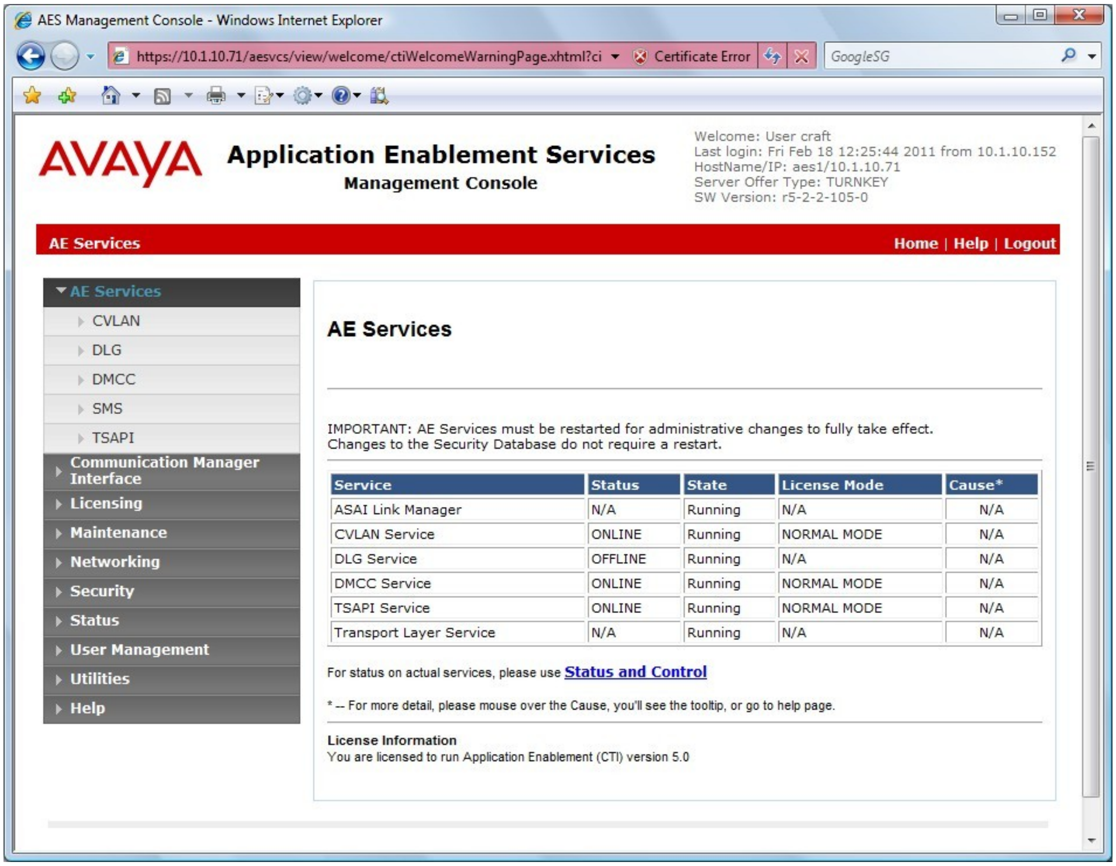
7. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services (AES). The procedures fall into the following areas:

- Verify Application Enablement Services License
- Administer CTI User
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user permission

7.1. Verify Application Enablement Services License

Step	Description
1.	Launch a web browser and enter **https://<IP address of AES server>** to access the Application Enablement Services Management Console. Log in using an administrative login and password (not shown), and the Welcome To OAM screen will be displayed.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/home.xhtml?cid=3 Certificate Error GoogleSG AVAYA Application Enablement Services Management Console Home Home | Help | Logout AE Services Communication Manager Interface Licensing Maintenance Networking Security Status User Management Utilities Help Welcome: User craft Last login: Fri Feb 18 12:25:44 2011 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 **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 infomations. • 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.

Step	Description
2.	Select **AE Services** from the left menu. From the Welcome to AE Services page, verify that the Application Enablement Services has proper license for the feature illustrated in these Application Notes by ensuring the **License Mode** for **TSAPI Service** is **NORMAL MODE**, as shown below. If the TSAPI Service is not licensed, then contact the Avaya sales team or business partner for the proper license to install onto the WebLM Server. 

AES Management Console - Windows Internet Explorer
https://10.1.10.71/aesvcs/view/welcome/ctiWelcomeWarningPage.xhtml?ci
Certificate Error
GoogleSG
AVAYA
Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Feb 18 12:25:44 2011 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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	ONLINE	Running	NORMAL MODE	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

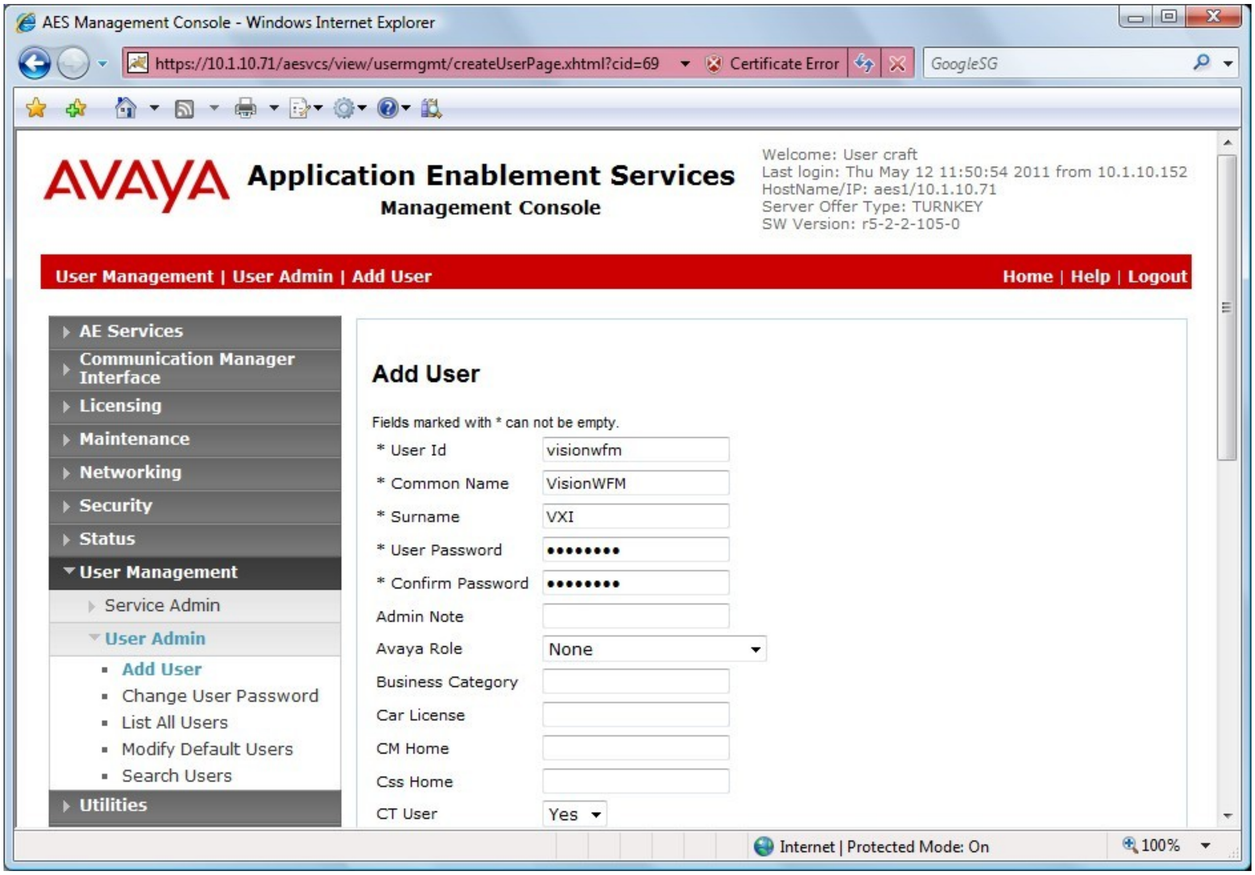
For status on actual services, please use **Status and Control**

* -- 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

7.2. Administer CTI User

Click **User Management**, then **User Admin > Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure VisionWFM in **Section 8** to access the TSAPI Service on the Application Enablement Services. Scroll down to the bottom of the page and click **Apply** (not shown).



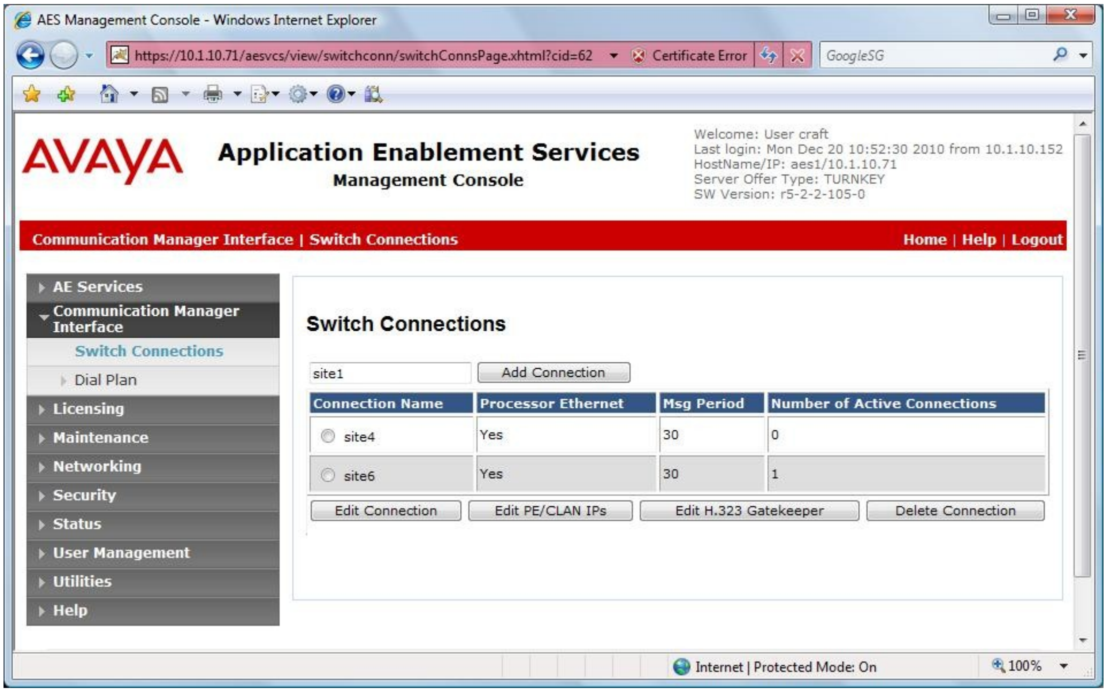
Welcome: User craft
Last login: Thu May 12 11:50:54 2011 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Add User

Fields marked with * can not be empty.

* User Id	visionwfm
* Common Name	VisionWFM
* Surname	VXI
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

7.3. Administer Switch Connection

Step	Description
1.	From the left menu, select **Communication Manager Interface > Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **site1** is used. 

AES Management Console - Windows Internet Explorer

https://10.1.10.71/aesvcs/view/switchconn/switchConnsPage.xhtml?cid=62 Certificate Error

Application Enablement Services
Management Console

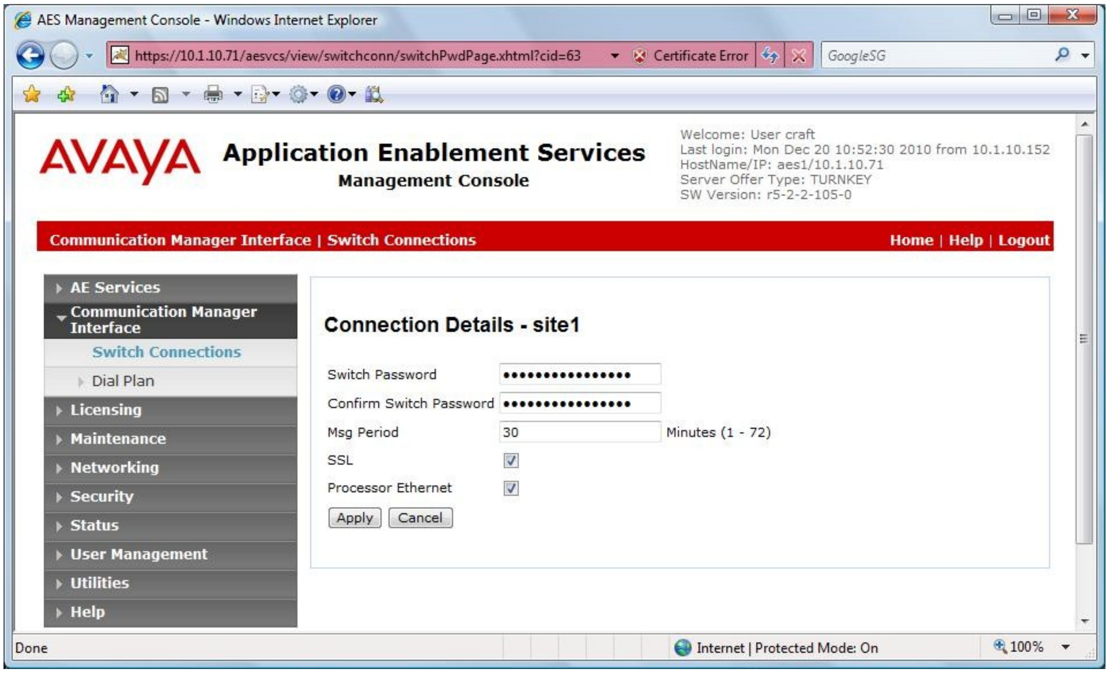
Welcome: User craft
Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

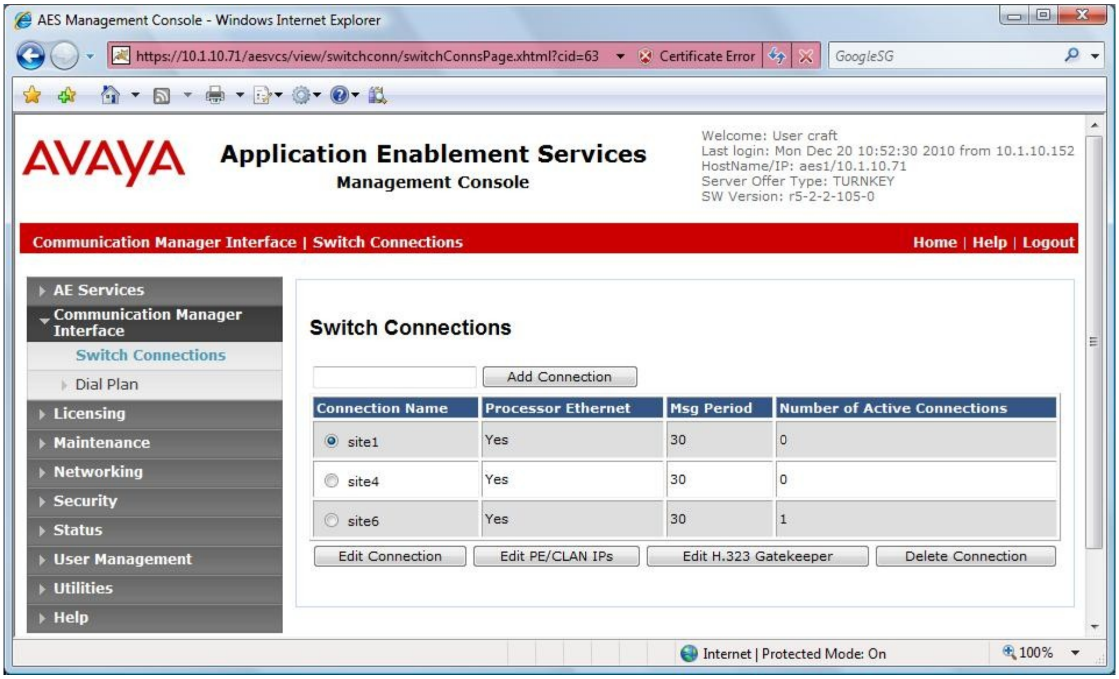
Communication Manager Interface | Switch Connections

Switch Connections

site1 Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ site4	Yes	30	0
○ site6	Yes	30	1

Step	Description
2.	The Connection Details – site1 screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 5.6 Step 3**. Both the **SSL** and **Processor Ethernet** fields need to be checked. Click on **Apply**.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/view/switchconn/switchPwdPage.xhtml?cid=63 Application Enablement Services Management Console Welcome: User craft Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 Communication Manager Interface | Switch Connections Connection Details - site1 Switch Password •••••••••••••••• Confirm Switch Password •••••••••••••••• Msg Period 30 Minutes (1 - 72) SSL ☑ Processor Ethernet ☑ Certificate Error GoogleSG AVAYA Home | Help | Logout AE Services Communication Manager Interface Switch Connections Dial Plan Licensing Maintenance Networking Security Status User Management Utilities Help Apply Cancel Done Internet | Protected Mode: On 100%

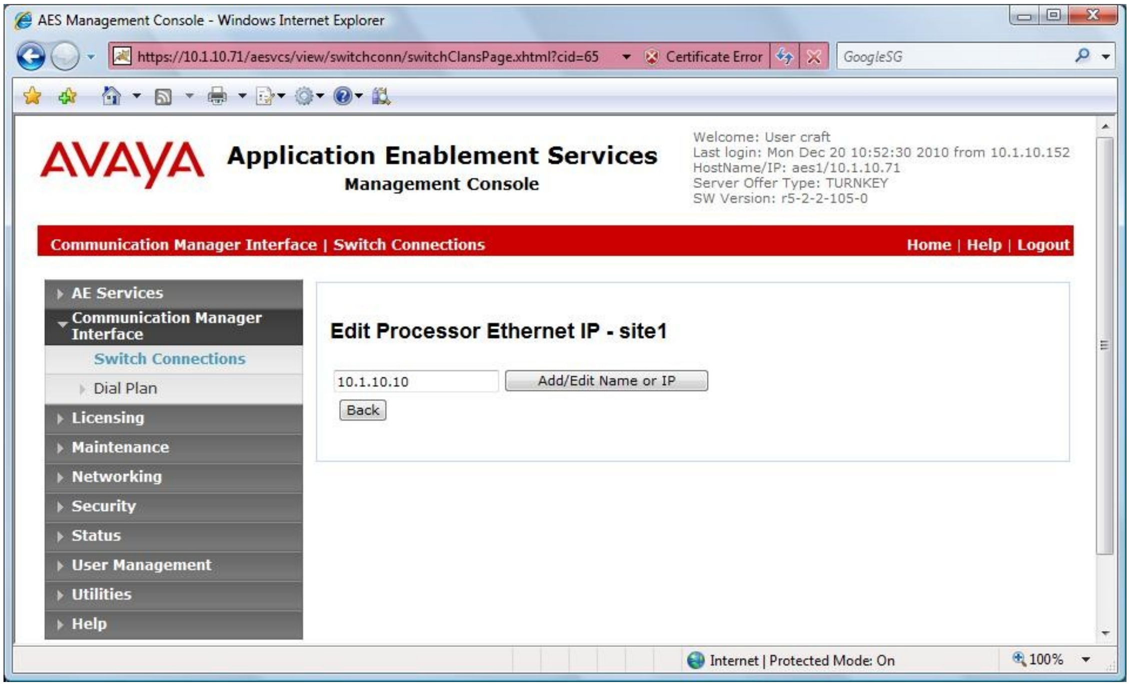
Step	Description
3.	The Switch Connections screen is displayed again. Select the new switch connection name **site1** and click **Edit PE/CLAN IPs**. 

AES Management Console - Windows Internet Explorer
https://10.1.10.71/aesvcs/view/switchconn/switchConnsPage.xhtml?cid=63
Certificate Error
GoogleSG
AVAYA
Application Enablement Services
Management Console

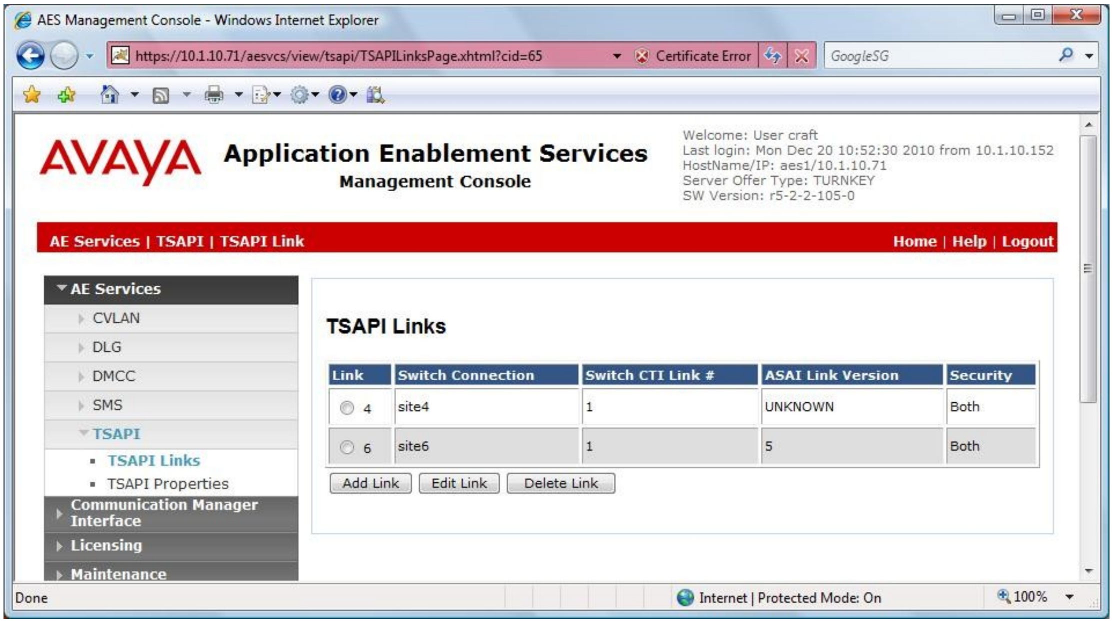
Welcome: User craft
Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● site1	Yes	30	0
○ site4	Yes	30	0
○ site6	Yes	30	1

Step	Description
4.	In the Edit Processor Ethernet IP – site1 screen, enter the host name or IP address of the Communication Manager processor Ethernet. In this case, **10.1.10.10** is used, which corresponds to the IP address of the S8800 Server as shown in **Figure 1**. Click **Add/Edit Name or IP**.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/view/switchconn/switchClansPage.xhtml?cid=65 Welcome: User craft Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 Communication Manager Interface | Switch Connections Edit Processor Ethernet IP - site1 10.1.10.10

7.4. Administer TSAPI Link

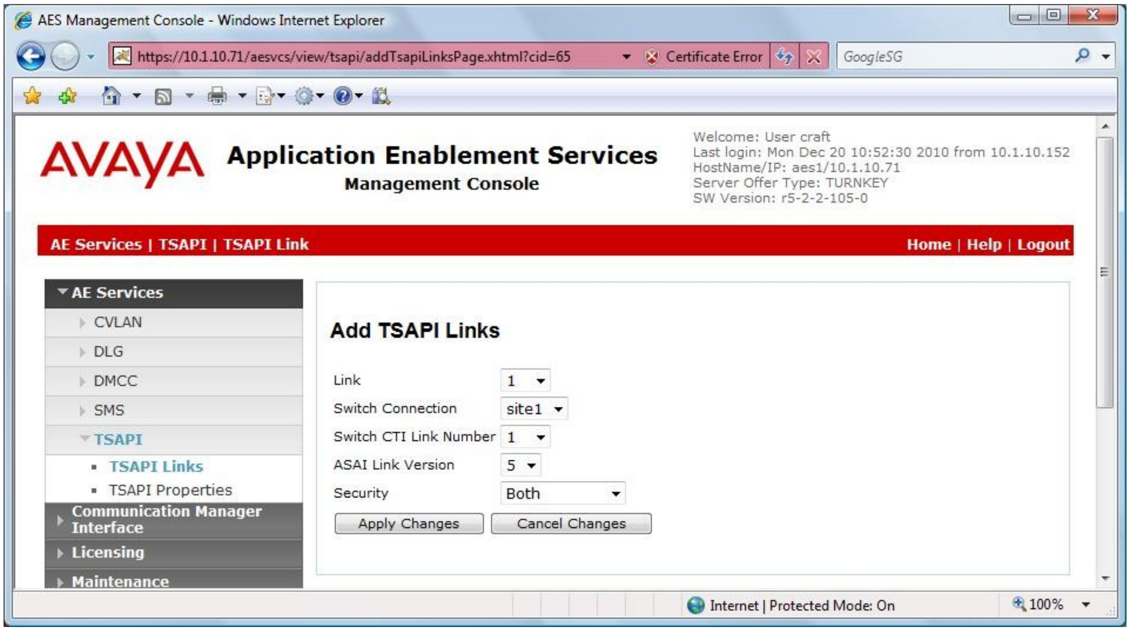
Step	Description
1.	To administer a TSAPI Link, select **AE Services > TSAPI > TSAPI Links** from the left menu. Click **Add Link**. 

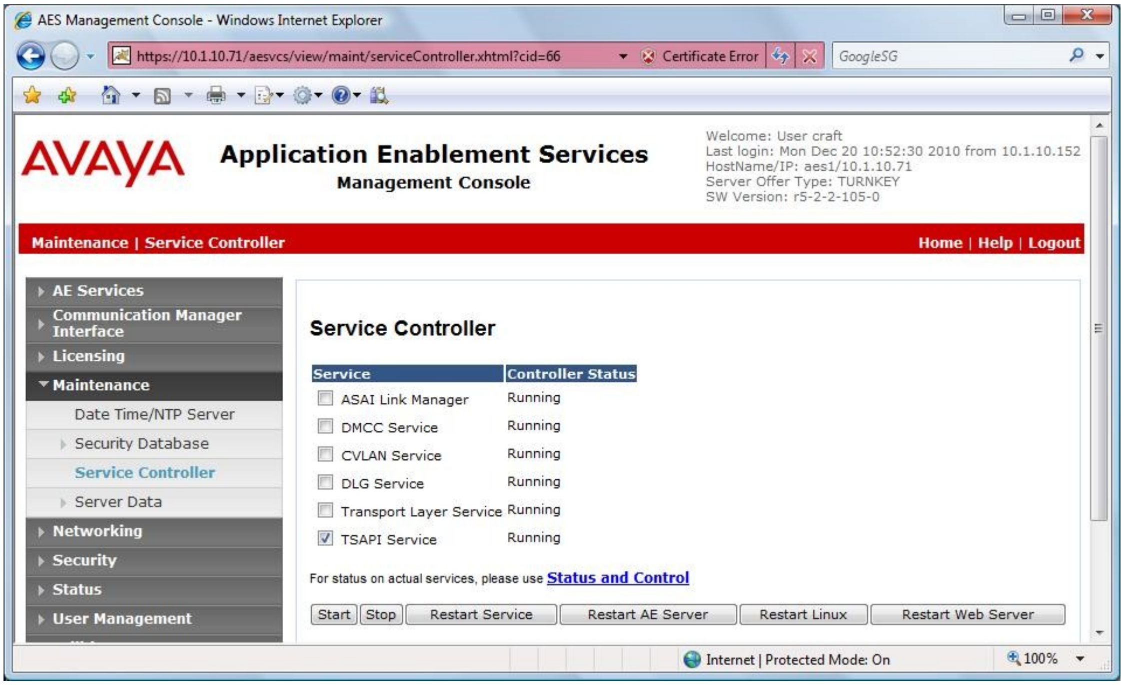
AES Management Console - Windows Internet Explorer
https://10.1.10.71/aesvcs/view/tsapi/TSAPILinksPage.xhtml?cid=65
Certificate Error
GoogleSG
AVAYA
Application Enablement Services
Management Console
AE Services | TSAPI | TSAPI Link
Home | Help | Logout
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
Communication Manager Interface
Licensing
Maintenance
Add Link
Edit Link
Delete Link
Done
Internet | Protected Mode: On
100%

Welcome: User craft
Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
○ 4	site4	1	UNKNOWN	Both
○ 6	site6	1	5	Both

Step	Description
2.	In the Add TSAPI Links screen, select the following values: • **Link:** Select an available Link number from 1 to 16. • **Switch Connection:** Select the switch connection in **Section 7.3 Step 1**. • **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.6 Step 2**. • **ASAI Link Version:** Set to **5**. • **Security:** Set to **Both** so that both encrypted and unencrypted TSAPI Links can be used. Note that the actual values may vary. Click **Apply Changes**.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/view/tsapi/addTsapiLinksPage.xhtml?cid=65 Application Enablement Services Management Console Welcome: User craft Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 AE Services | TSAPI | TSAPI Link Add TSAPI Links Link: 1 Switch Connection: site1 Switch CTI Link Number: 1 ASAI Link Version: 5 Security: Both Certificate Error GoogleSG Home | Help | Logout AE Services CVLAN DLG DMCC SMS TSAPI TSAPI Links TSAPI Properties Communication Manager Interface Licensing Maintenance Apply Changes Cancel Changes Internet | Protected Mode: On 100% In the next page, click **Apply** to confirm the changes (not shown).

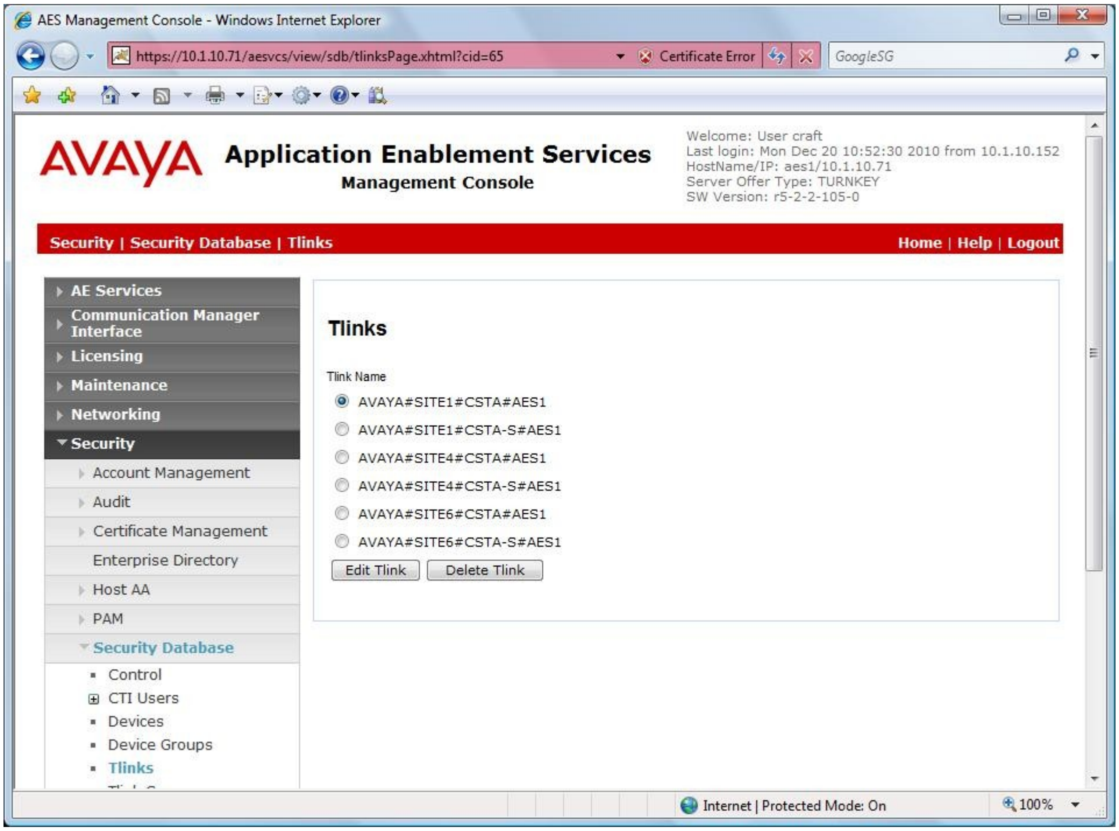
Step	Description
3.	To restart the TSAPI Service, select **Maintenance > Service Controller** from the left menu. Check the **TSAPI Service** checkbox and click **Restart Service**. In the next page, click **Restart** to confirm the restart (not shown). 

Welcome: User craft
Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

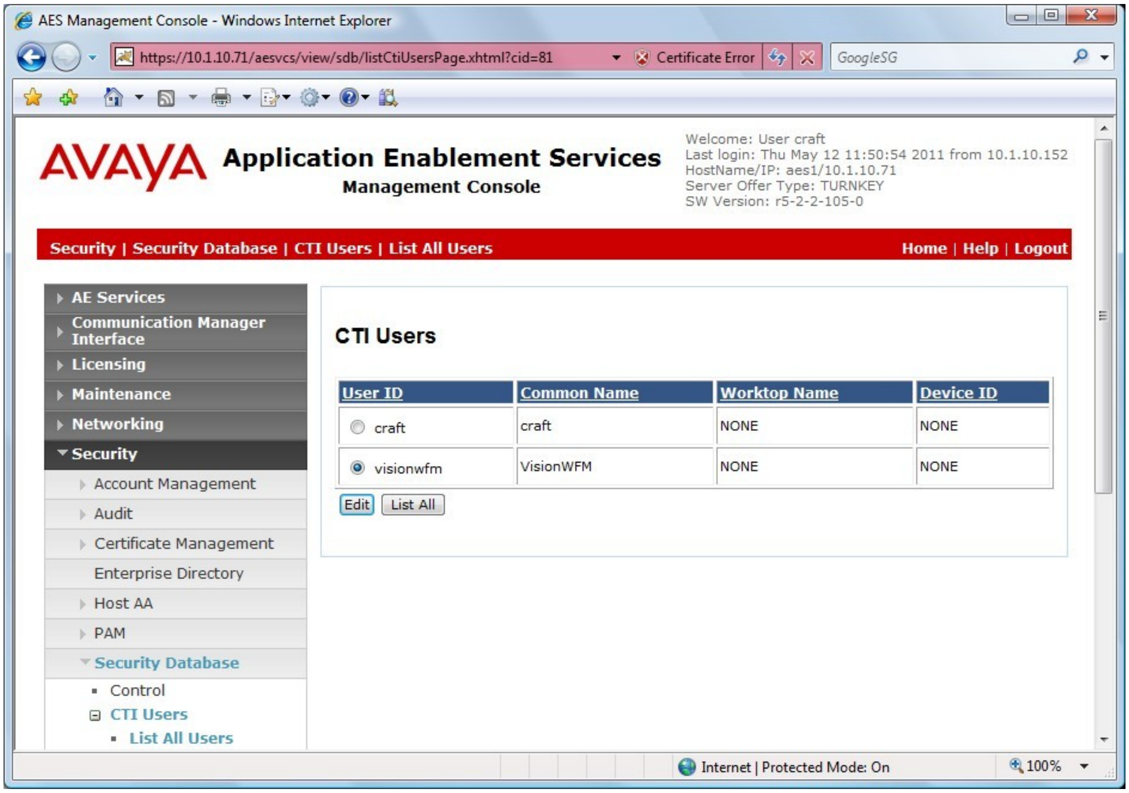
Service Controller

Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

Step	Description
4.	Navigate to the Tlinks screen by selecting **Security > Security Database > Tlinks** from the left menu. Note the value of the **Tlink Name**, as this will be needed to configure VisionWFM in **Section 8**. In this configuration, the unencrypted **Tlink Name AVAYA#SITE1#CSTA#AES1** is used.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/view/sdb/tlinksPage.xhtml?cid=65 Certificate Error GoogleSG AVAYA Security | Security Database | Tlinks 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 Devices Device Groups Tlinks Edit Tlink Delete Tlink Internet | Protected Mode: On 100% Application Enablement Services Management Console Welcome: User craft Last login: Mon Dec 20 10:52:30 2010 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 Tlinks Tlink Name ● AVAYA#SITE1#CSTA#AES1 ○ AVAYA#SITE1#CSTA-S#AES1 ○ AVAYA#SITE4#CSTA#AES1 ○ AVAYA#SITE4#CSTA-S#AES1 ○ AVAYA#SITE6#CSTA#AES1 ○ AVAYA#SITE6#CSTA-S#AES1

7.5. Administer CTI User Permission

Step	Description
1.	Select **Security > Security Database > CTI Users > List All Users** from the left menu. Select the **User ID** created in **Section 7.2** and click **Edit**. 

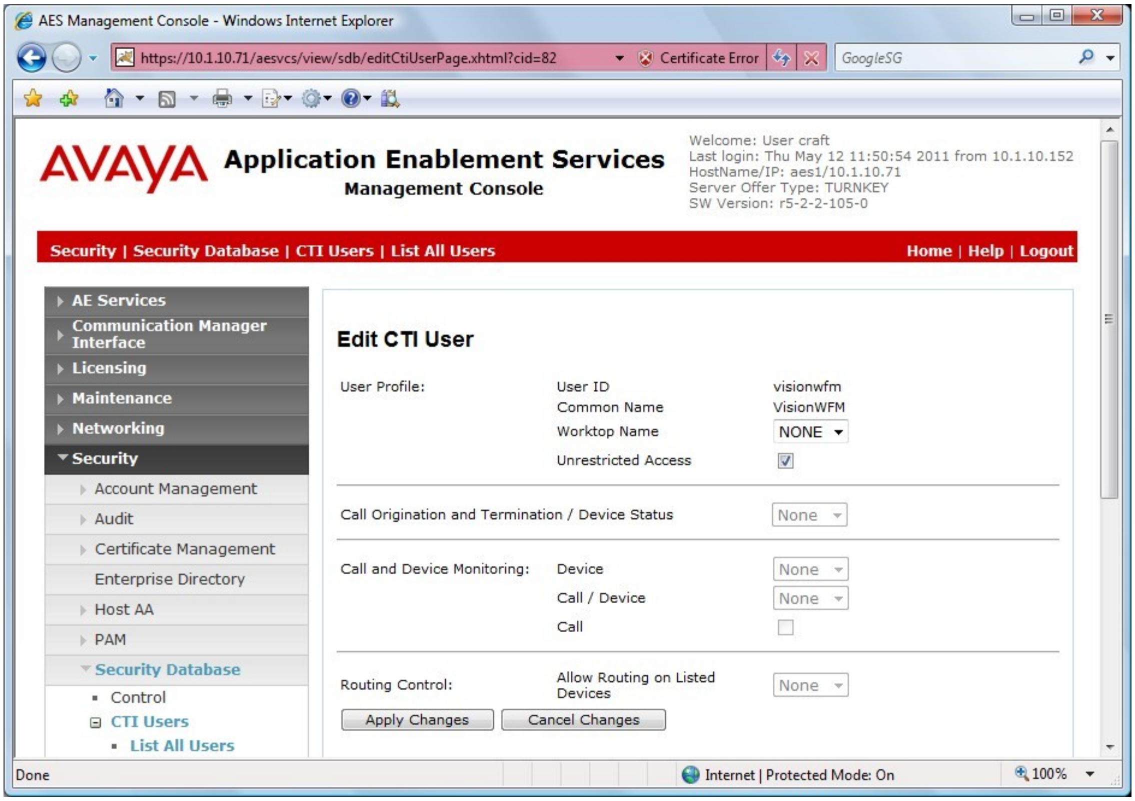
AES Management Console - Windows Internet Explorer
https://10.1.10.71/aesvcs/view/sdb/listCtiUsersPage.xhtml?cid=81
Certificate Error
GoogleSG
AVAYA
Application Enablement Services
Management Console
Security | Security Database | CTI Users | List All Users
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Internet | Protected Mode: On
100%

Welcome: User craft
Last login: Thu May 12 11:50:54 2011 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

CTI Users

User ID	Common Name	Worktop Name	Device ID
○ craft	craft	NONE	NONE
● visionwfm	VisionWFM	NONE	NONE

Edit | List All

Step	Description
2.	Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, **Unrestricted Access** was enabled during compliance testing. If **Unrestricted Access** is not desired, then consult Reference [4] for guidance on configuring the call/device privileges as well as devices and device groups. Click **Apply Changes**.  AES Management Console - Windows Internet Explorer https://10.1.10.71/aesvcs/view/sdb/editCtiUserPage.xhtml?cid=82 Certificate Error GoogleSG AVAYA Application Enablement Services Management Console 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 Apply Changes Cancel Changes Done Internet | Protected Mode: On 100% Welcome: User craft Last login: Thu May 12 11:50:54 2011 from 10.1.10.152 HostName/IP: aes1/10.1.10.71 Server Offer Type: TURNKEY SW Version: r5-2-2-105-0 Edit CTI User User Profile: User ID: visionwfm Common Name: VisionWFM Worktop Name: NONE Unrestricted Access: ☑ Call Origination and Termination / Device Status: None Call and Device Monitoring: Device: None Call / Device: None Call: □ Routing Control: Allow Routing on Listed Devices: None In the next page, click **Apply** to confirm the changes (not shown).

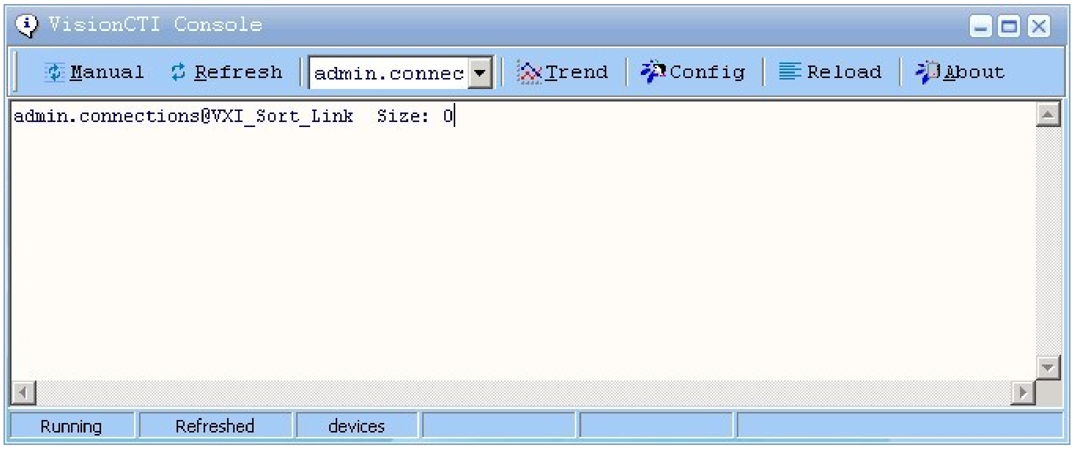
8. Configure VXI China VisionWFM

This section provides the procedures for installing and configuring VisionWFM. The procedures include the following areas:

- Configure VisionCTI Service
- Configure devices to be monitored

8.1. Configure VisionCTI Service

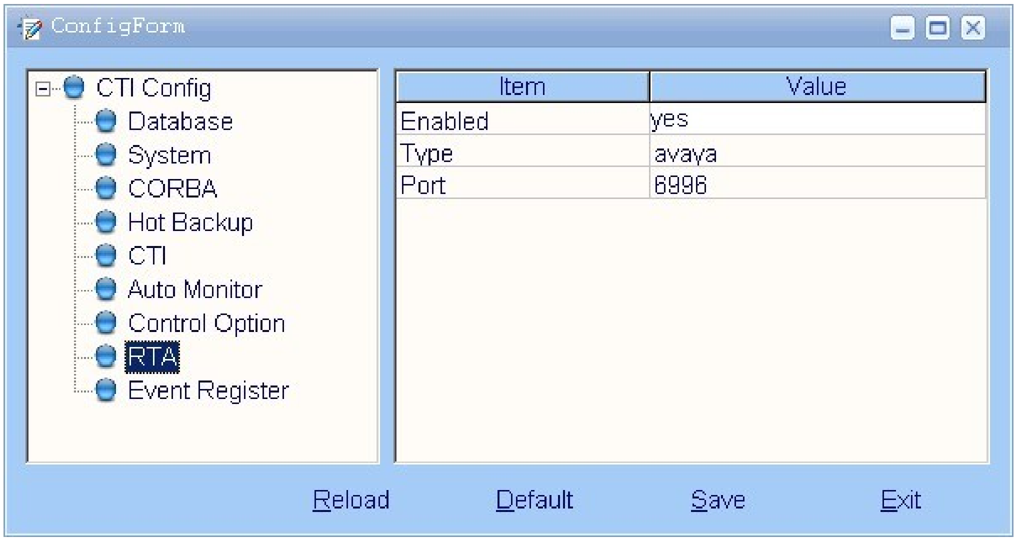
Log in to the VisionWFM server using an administrator account and click **Start > All Programs > Vision-X > VisionCTI > VisionCTI**. From the VisionCTI Console, click **Config**.



```
admin.connections@VXI_Sort_Link  Size: 0
```

Select **RTA** from the left menu and configure the following for the Generic-RTA interface.

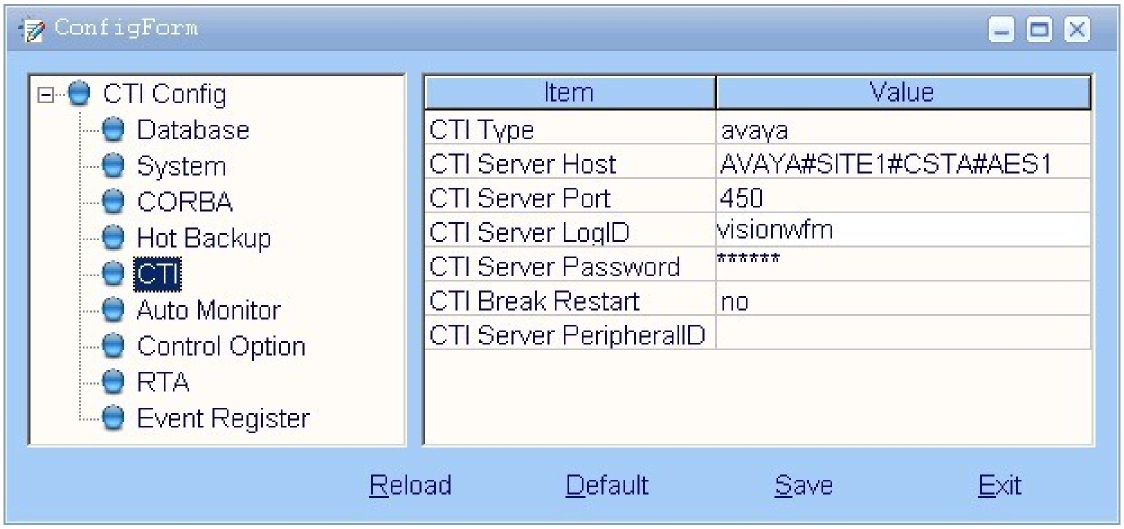
- **Enabled:** "yes"
- **Type:** "avaya"
- **Port:** "6996". This must match the port configured on Avaya CMS in **Section 6**.



Item	Value
Enabled	yes
Type	avaya
Port	6996

Select **CTI** from the left menu and configure the following for the TSAPI interface. Use the default values for all other fields.

- **CTI Type:** "avaya"
- **CTI Server Host:** Enter the **Tlink Name** in **Section 7.4 Step 4**.
- **CTI Server Port:** "450". This is the default port for TSAPI.
- **CTI Server LogID:** Enter the **User Id** created in **Section 7.2**.
- **CTI Server Password:** Enter the **User Password** created in **Section 7.2**.



Item	Value
CTI Type	avaya
CTI Server Host	AVAYA#SITE1#CSTA#AES1
CTI Server Port	450
CTI Server LogID	visionwfm
CTI Server Password	******
CTI Break Restart	no
CTI Server PeripheralID	

8.2. Configure Devices to be Monitored

In this compliance testing, the management platform VisionONE was not installed. As such, the configuration of the devices (extensions, skilled hunt groups and agent-IDs) to be monitored by VisionWFM was done using an SQL script. A sample SQL script is shown below.

```
-- add devices
insert into vxi_sys..devices(device,sortid,devname,devtype,enabled)
    select 10001,20100000,'Ext.10001',1,1

-- add skills
insert into vxi_sys..skill(skill,sortid,skillname,skilltype,prjid,enabled)
    select '13001',20100000,'13001',1,0,1

-- add agents
insert into vxi_sys..agent(agent,sortid,agentname,regdate,state,enabled)
    select '11001',20100000,'11001',getdate(),1,1

-- sync into to database vxi_ucd
exec vxi_ucd..sp_syn_device_setup
```

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Avaya Call Management System, Application Enablement Services and VXI China VisionWFM.

9.1. Verify Communication Manager

Verify the status of the processor interface channel by using the **status processor-channels n** command, where **n** is the processor channel number from **Section 5.4**. Verify that the **Session Layer Status** is **In Service**, and that the **Socket Status** is **TCP connected**, as shown below.

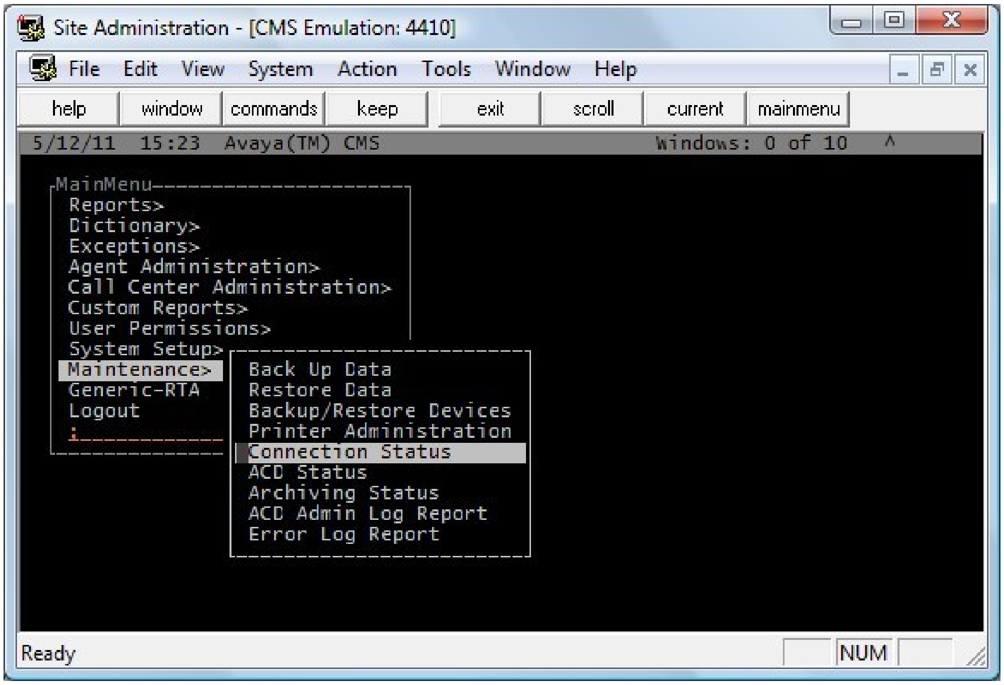
```
status processor-channels 1
                        PROCESSOR-CHANNEL STATUS

          Channel Number: 1
    Session Layer Status: In Service
           Socket Status: TCP connected
             Link Number: pv4
               Link Type: processor ethernet
   Message Buffer Number: 0

            Last Failure: None
                      At: 04/12/11 12:24
```

Verify the status of the processor ethernet link by using the **status link procr** command. Verify that the **Link Status** is **inservice** as shown below.

```
status link procr                                              Page   1 of   2
                               LINK/PORT STATUS


                 Link Status: inservice
                   Link Type: processor

       Service Port Location: eth0

                   V4 Parameters
                   Node Name: procr
           Source IP Address: 10.1.10.10/24

           Broadcast Address: 10.1.10.255

                     Enabled? yes
            Maintenance Busy? no
             Active Channels: 1
```

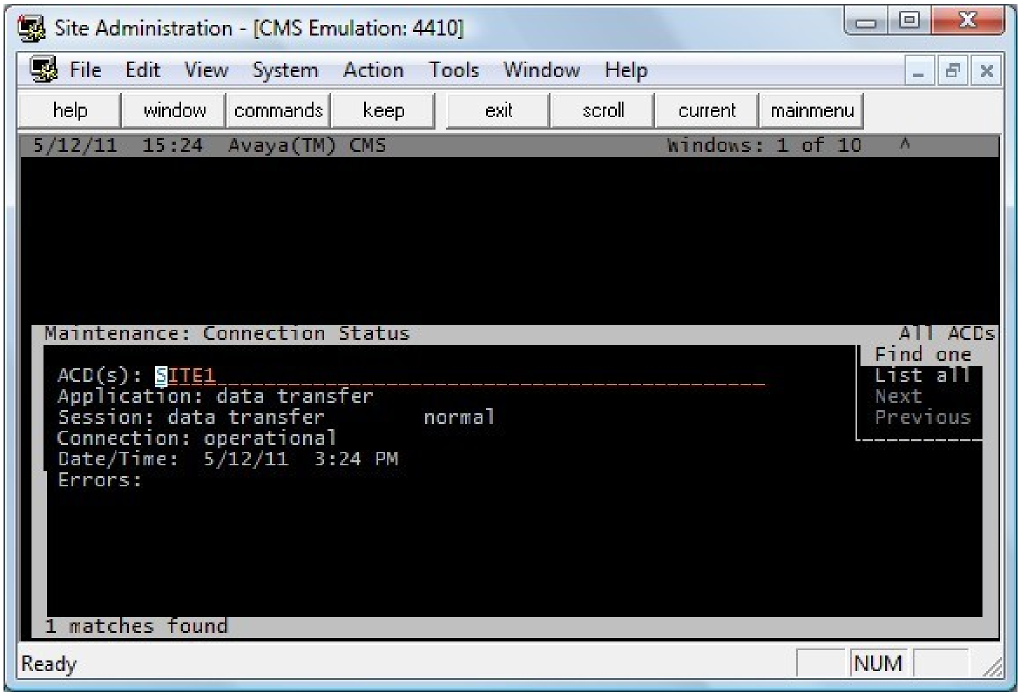
9.2. Verify Call Management System

From the **MainMenu**, verify the status of the connection to Communication Manager by selecting **Maintenance → Connection Status**, as shown below.



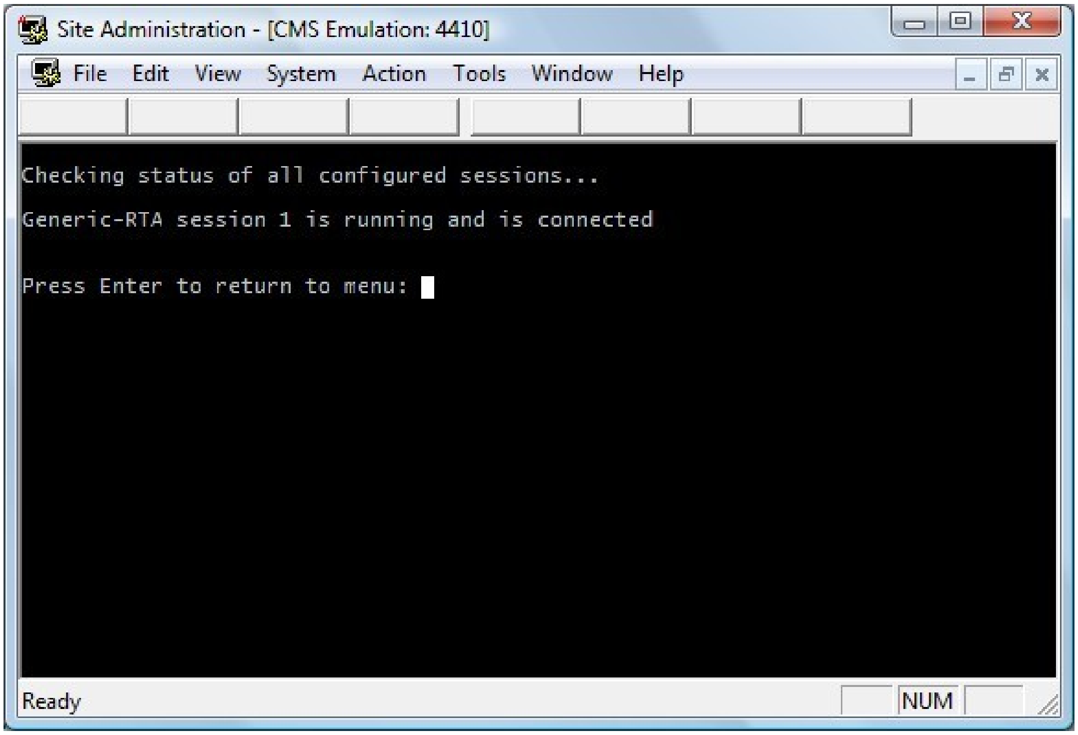
```
5/12/11  15:23  Avaya(TM) CMS                         Windows: 0 of 10   ^

 MainMenu
  Reports>
  Dictionary>
  Exceptions>
  Agent Administration>
  Call Center Administration>
  Custom Reports>
  User Permissions>
  System Setup>
  Maintenance>    Back Up Data
  Generic-RTA     Restore Data
  Logout          Backup/Restore Devices
  :               Printer Administration
                  Connection Status
                  ACD Status
                  Archiving Status
                  ACD Admin Log Report
                  Error Log Report
```

Tab over to **Find one** and press **Enter**. The switch connection status is displayed. Check the status in the **Session** and **Connection** fields, as shown below.



```
5/12/11  15:24  Avaya(TM) CMS                         Windows: 1 of 10   ^

 Maintenance: Connection Status                                  All ACDs
                                                                 Find one
   ACD(s): SITE1                                                 List all
   Application: data transfer                                    Next
   Session: data transfer        normal                          Previous
   Connection: operational
   Date/Time:  5/12/11  3:24 PM
   Errors:

 1 matches found
```

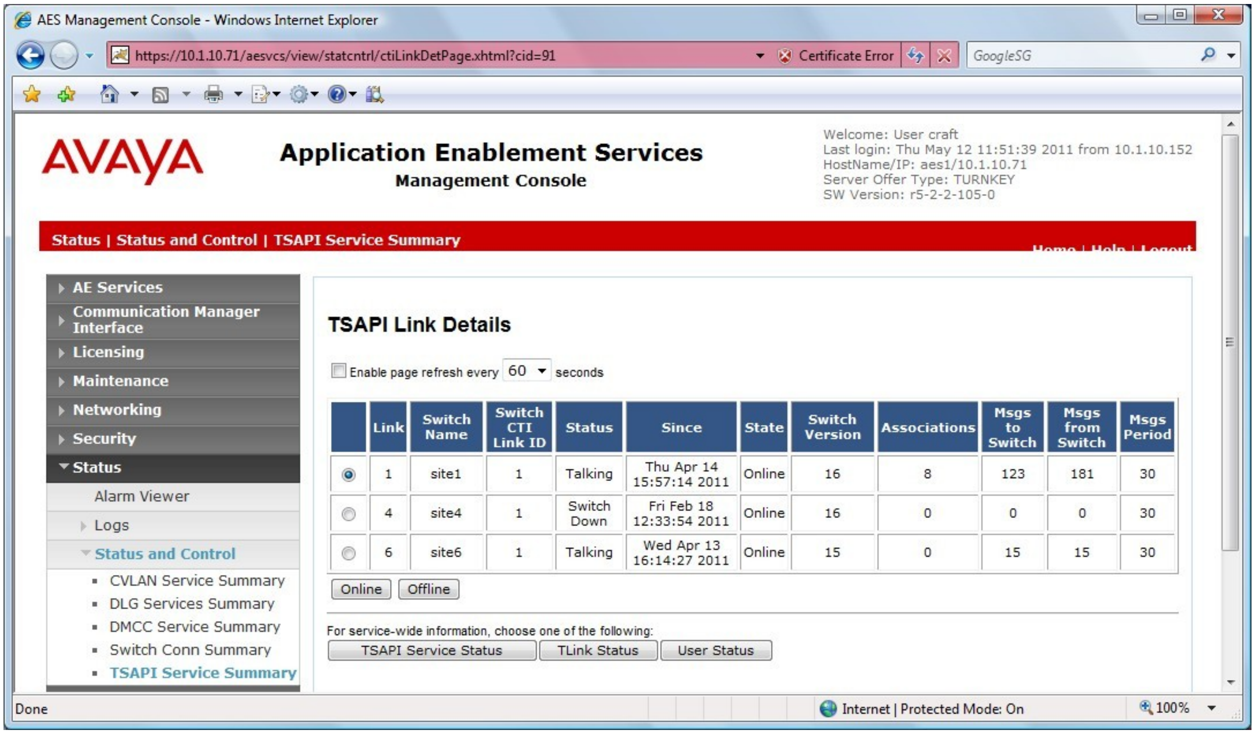
From the Generic-RTA menu, select option ‘3’ to check the status of the Generic-RTA interface. The Generic-RTA session should be **running** and **connected** as shown below.



```
Checking status of all configured sessions...

Generic-RTA session 1 is running and is connected

Press Enter to return to menu:
```

9.3. Verify Application Enablement Services

From the Application Enablement Services Management Console web page, verify the status of the TSAPI Link by selecting **Status > Status and Control > TSAPI Service Summary** from the left pane. The **Status** field for the **Switch Name** "site1" should display **Talking**.



AES Management Console - Windows Internet Explorer
https://10.1.10.71/aesvcs/view/statcntrl/ctiLinkDetPage.xhtml?cid=91
Certificate Error
GoogleSG
AVAYA
Application Enablement Services
Management Console

Welcome: User craft
Last login: Thu May 12 11:51:39 2011 from 10.1.10.152
HostName/IP: aes1/10.1.10.71
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

TSAPI Link Details

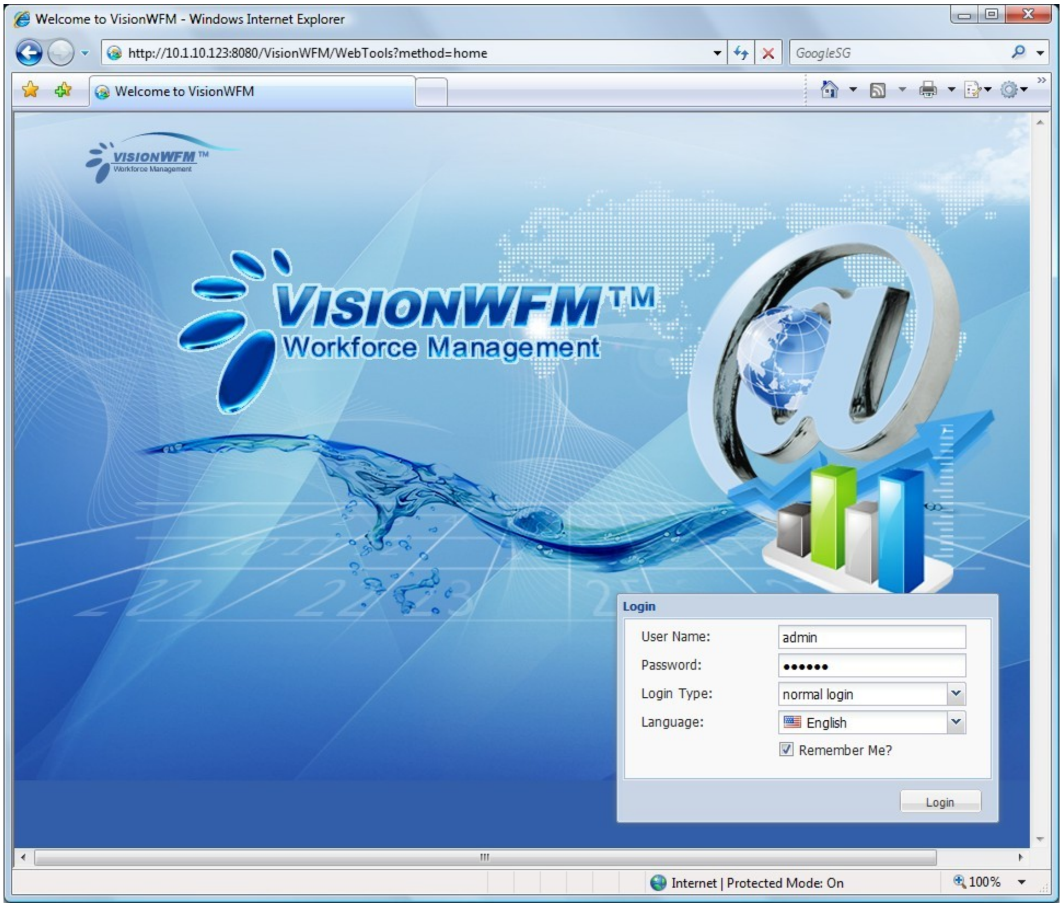
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	site1	1	Talking	Thu Apr 14 15:57:14 2011	Online	16	8	123	181	30
○	4	site4	1	Switch Down	Fri Feb 18 12:33:54 2011	Online	16	0	0	0	30
○	6	site6	1	Talking	Wed Apr 13 16:14:27 2011	Online	15	0	15	15	30

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

8.1 Verify VXI China VisionWFM

Using Internet Explorer, browse to http://<ip_addr>:8080/VisionWFM/, where ip_addr is the IP address of the VisionWFM server. Log in using an account with administrative privileges.



Welcome to VisionWFM - Windows Internet Explorer

http://10.1.10.123:8080/VisionWFM/WebTools?method=home

Login

User Name: admin

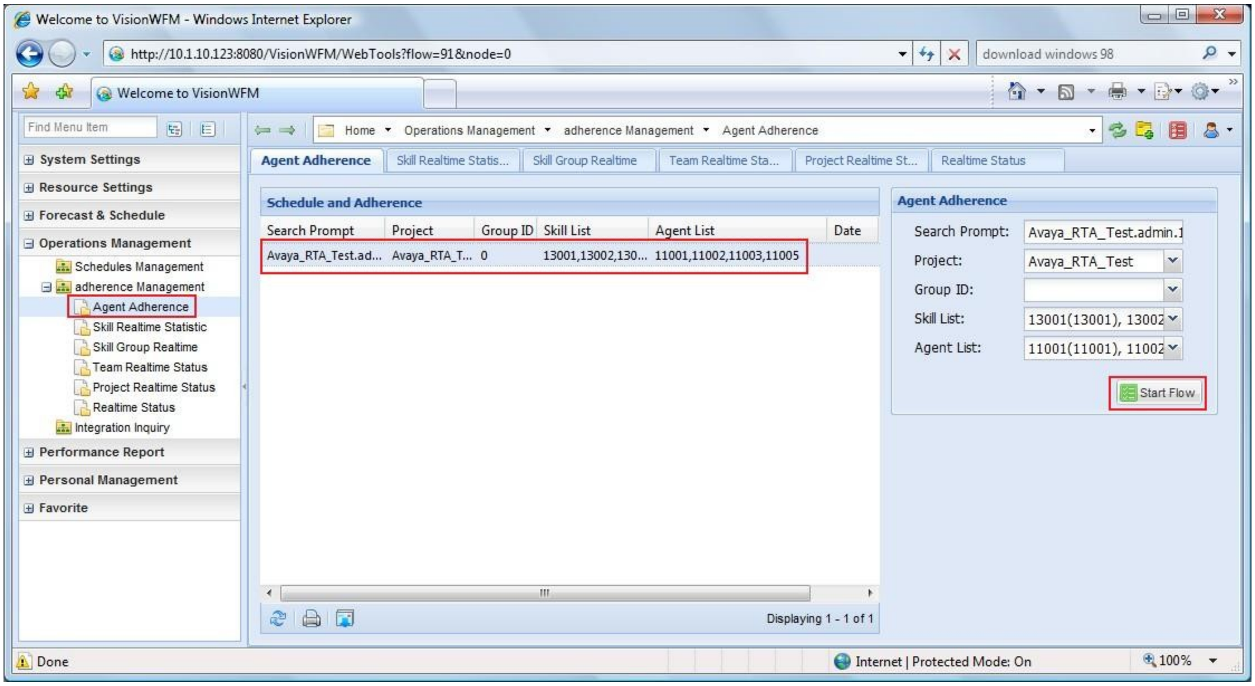
Password: ••••••

Login Type: normal login

Language: English

☑ Remember Me?

Select **Adherence Management > Agent Adherence** from the left, then click the appropriate row in Schedule and Adherence (e.g. for the hunt groups and agent-IDs used in the testing) and click **Start Flow**.



Schedule and Adherence

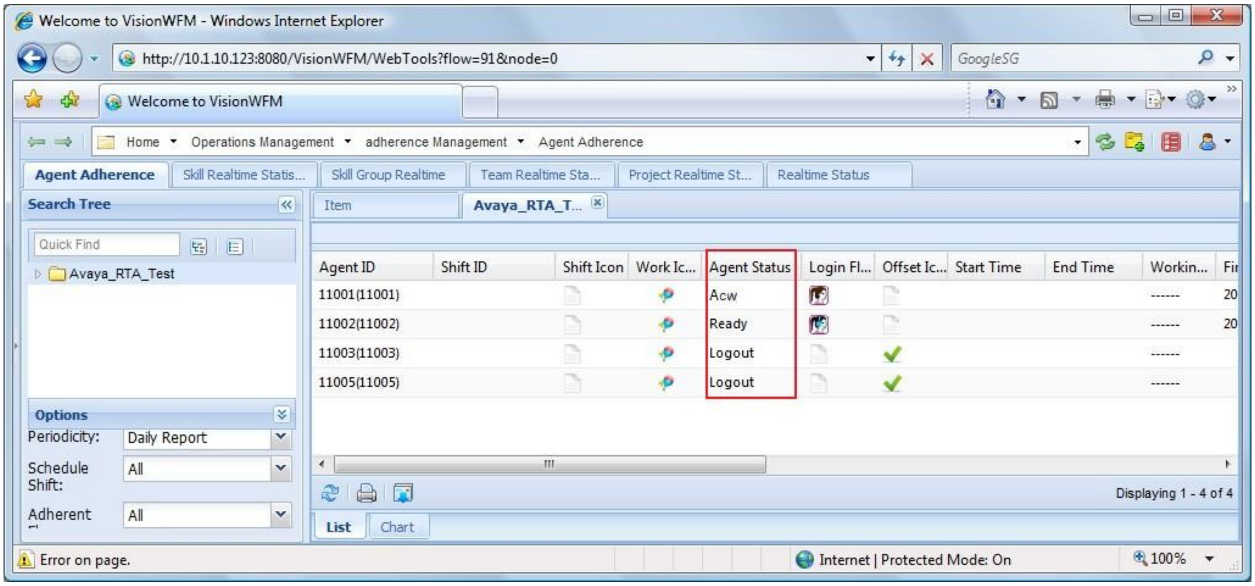
Search Prompt	Project	Group ID	Skill List	Agent List	Date
Avaya_RTA_Test.ad...	Avaya_RTA_T...	0	13001,13002,130...	11001,11002,11003,11005	

Displaying 1 - 1 of 1

Agent Adherence

Search Prompt: Avaya_RTA_Test.admin.1
Project: Avaya_RTA_Test
Group ID:
Skill List: 13001(13001), 13002
Agent List: 11001(11001), 11002

In the **Agent Adherence** tab, verify that the **Agent Status** field correctly indicates the agent state by comparing with the real-time report in Avaya CMS.

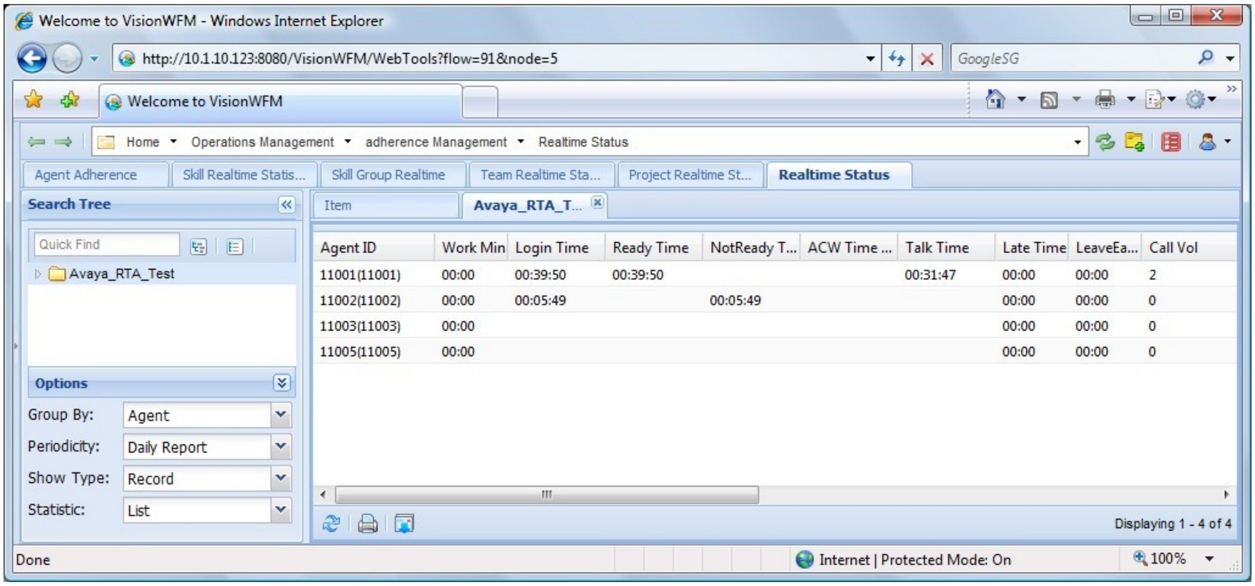


Options
Periodicity: Daily Report
Schedule Shift: All
Adherent: All

Agent ID	Shift ID	Shift Icon	Work Ic...	Agent Status	Login Fl...	Offset Ic...	Start Time	End Time	Workin...	Fi
11001(11001)				Acw					------	20
11002(11002)				Ready					------	20
11003(11003)				Logout		✓			------	
11005(11005)				Logout		✓			------	

Displaying 1 - 4 of 4

In the **Realtime Status** tab, verify that the call details such as **Talk Time** and **Call Vol** are updated correctly by placing a call to the agents.



Group By: Agent
Periodicity: Daily Report
Show Type: Record
Statistic: List

Agent ID	Work Min	Login Time	Ready Time	NotReady T...	ACW Time ...	Talk Time	Late Time	LeaveEa...	Call Vol
11001(11001)	00:00	00:39:50	00:39:50			00:31:47	00:00	00:00	2
11002(11002)	00:00	00:05:49		00:05:49			00:00	00:00	0
11003(11003)	00:00						00:00	00:00	0
11005(11005)	00:00						00:00	00:00	0

10. Conclusion

These Application Notes describe the configuration steps required for VXI China VisionWFM 3.0 to successfully interoperate with Avaya Call Management System Release 16 and Avaya Aura® Application Enablement Services 5.2. All feature and serviceability test cases were completed successfully.

11. Additional References

The following documents are available at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager*, Release 6.0, Document No. 03-300509, August 2010.

[2] *Avaya Call Management System Release 16 Switch Connections, Administration, and Troubleshooting*, November 2009.

[3] *Avaya Call Management System Release 16 Database Items and Calculations*, November 2009.

[4] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Document ID 02-300357, Issue 11, November 2009.

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.