

#### Avaya Solution & Interoperability Test Lab

# Application Notes for ITNAVIGATOR A-NAV with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

#### **Abstract**

These Application Notes describe the configuration steps required for IT NAVIGATOR A-NAV to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES).

These Application Notes describe how to configure the A-NAV real time monitoring system with Avaya Communication Manager and Avaya AES to monitor, in real time, agents and call activities in the contact center.

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

#### 1. Introduction

These Application Notes describe the configuration steps required for IT NAVIGATOR A-NAV to successfully interoperate with Avaya Communication Manager and Avaya AES.

The A-NAV system is comprised of a Java Telephony Application Programmer Interface (JTAPI) Probe server and an A-NAV State Machine server. The JTAPI Probe server uses the Avaya AES JTAPI service to receive the status and events of all calls, agents, hunt groups and vector directory numbers (VDNs) in the contact centre.

The information is then analyzed in real time by the A-NAV State Machine and is displayed in the A-NAV user interface. The user interface can be used to monitor the current status and actions of all contact centre devices as well as to allow a supervisor to invoke service observing, whisper page, and remote logout features using the A-NAV JTAPI Functional server. The user interface also allows a supervisor to add/change an agent and to change an agent's skills via the Avaya AES Systems Management Service (SMS)

**Figure 1** shows the compliance tested configuration.

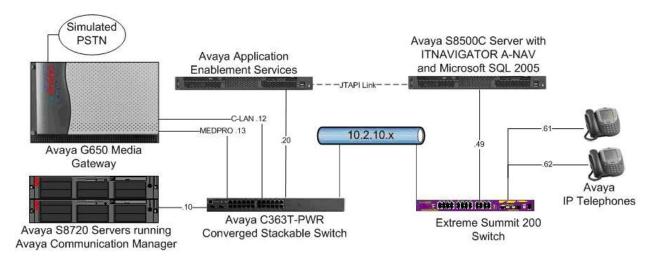


Figure 1: Network Diagram of the Compliance Tested Configuration.

Please note that the Avaya configuration sections refer to the CTI link as the Telephony Service Application Programmer Interface (TSAPI), as JTAPI is mapped to TSAPI on the Avaya AES.

# 2. Equipment and Software Validated

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

Equipment	Software
Avaya S8720 Servers	Avaya Communication Manager 5.0
	Build 5.0.00.852.7
Avaya S8500C Server	Avaya AES 4.1 (Build 4.1.0.31.2)
Avaya G650 Media Gateway	
C-LAN TN799DP	HW01 FW024
MEDPRO TN2602AP	HW08 FW031
Avaya S8500C Server	ITNAVIGATOR A-NAV:
	A-NAV JTAPI Probe 1.3.003.2
	A-NAV State Machine 1.3.003
	A-NAV JTAPI Functional Server 1.2
	Microsoft Windows Server 2003 - Service
	Pack 2.
	Microsoft SQL 2005

## 3. Configure Avaya Communication Manager

This section provides the procedures for configuring Avaya Communication Manager. The procedures fall into the following areas.

- Configure the CTI link.
- Configure feature access codes.
- Configure an administrator login.

Please note that it is expected that the installer is familiar with configuring stations, agents, vectors, VDNs, etc. on Avaya Communication Manager as the focus of these Application Notes is on the configuration of the JTAPI interface only. For all other provisioning information, such as software installation, installation of optional components, basic configuration of Avaya Communication Manager, etc., refer to the Avaya Communication Manager product documentation in reference [1].

Unless otherwise stated, the System Administration Terminal (SAT) interface was used for all Avaya Communication Manager configurations.

#### 3.1. Configure the CTI Link

This section assumes that the Internet Protocol (IP) service to the Avaya AES was previously administered. Information on how to do this is available in the Avaya AES product documentation in reference [2].

Use the "add cti-link x" command, where "x" is an available CTI link number, to add a new CTI link. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field. The remaining fields may be left at their default values. Submit these changes.

add cti-link 3 Page 1 of 2

CTI Link: 3
Extension: 13300

Type: ADJ-IP

Name: TSAPI CTI Link 3

COR: 1

#### 3.2. Configure Feature Access Codes

Use the "change feature-access-codes" command. On Page 1 of the feature access code form enter a valid feature access code in the **Auto Route Selection (ARS) - Access Code 1** field.

```
change feature-access-codes
                                                                      1 of
                                                                Page
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *01
        Abbreviated Dialing List2 Access Code: *02
        Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                      Answer Back Access Code: *06
                        Attendant Access Code:
     Auto Alternate Routing (AAR) Access Code: *08
   Auto Route Selection (ARS) - Access Code 1: 9
                                                      Access Code 2:
                Automatic Callback Activation: *10
                                                      Deactivation: #10
                                          All: *12
Call Forwarding Activation Busy/DA: *11
                                                      Deactivation: #12
                        Call Park Access Code: *13
                      Call Pickup Access Code: *14
CAS Remote Hold/Answer Hold-Unhold Access Code: *15
                 CDR Account Code Access Code: *16
                       Change COR Access Code:
                   Change Coverage Access Code: *18
                                                         Close Code: #19
                   Contact Closure Open Code: *19
```

On Page 5 of the feature access code form enter a valid feature access code in the **Whisper Page Access Code** field.

```
change feature-access-codes
                                                                         4 of 8
                                                                 Page
                           FEATURE ACCESS CODE (FAC)
                       Station Lock Activation: *58
                                                        Deactivation: #58
      Station Security Code Change Access Code: *59
              Station User Admin of FBI Assign:
                                                                   Remove:
  Station User Button Ring Control Access Code:
             Terminal Dial-Up Test Access Code: *62
Terminal Translation Initialization Merge Code:
                                                          Separation Code:
            Transfer to Voice Mail Access Code: *64
          Trunk Answer Any Station Access Code: *65
              User Control Restrict Activation: *66
                                                        Deactivation: #66
 Voice Coverage Message Retrieval Access Code: *67
 Voice Principal Message Retrieval Access Code: *68
           Whisper Page Activation Access Code: *78
```

On Page 5 of the feature access code form enter valid feature access codes in the **Service Observing Listen Only Access Code** and **Remote Logout of Agent Access Code** fields.

```
change feature-access-codes

FEATURE ACCESS CODE (FAC)

Automatic Call Distribution Features

After Call Work Access Code: *70

Assist Access Code: *71

Auto-In Access Code: *72

Aux Work Access Code: *73
```

Login Access Code: \*74

Logout Access Code: \*75

Manual-in Access Code: \*76

Service Observing Listen Only Access Code: \*77

Service Observing Listen/Talk Access Code: \*78

Service Observing No Talk Access Code: \*79

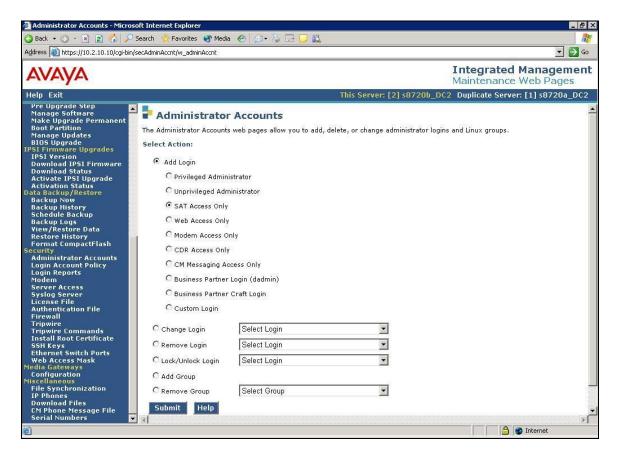
Add Agent Skill Access Code: \*80

Remove Agent Skill Access Code: \*81

Remote Logout of Agent Access Code: \*82

#### 3.3. Configure an Administrator Login

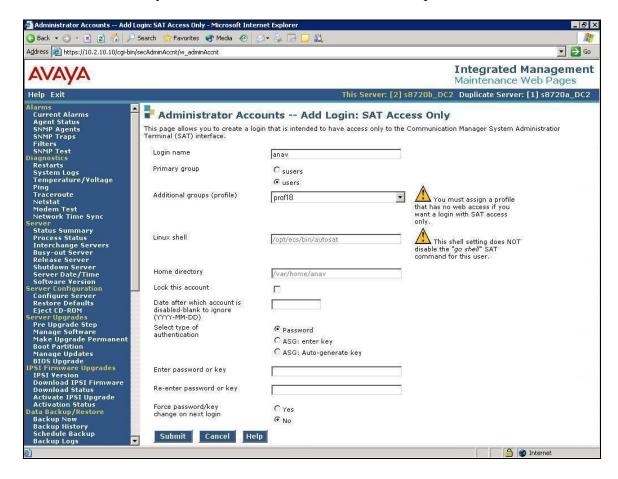
Initialize the Avaya Communication Manager web interface by browsing to "https://x.x.x.x/cgi-bin/login/webLogin", where "x.x.x.x" is the IP address of the Avaya Communication Manager server, and log in using the proper credentials (not shown). On the Standard Management Solutions screen, select **Launch Maintenance Web Interface** (not shown). From the left hand menu of the Maintenance web page, select **Security > Administrator Accounts**. On the Administrator Accounts page select the **Add Login** and **SAT Access Only** radio buttons and select **Submit**.



On the Add Login page, configure the fields as follows.

- **Login name:** Enter a unique username.
- **Primary group:** Select the **users** radio button.
- **Select type of authentication:** Select the **password** radio button.
- Enter password or key: Enter a password of at least six characters
- **Re-enter password or key:** Re-enter the password entered above.

The rest of the fields may be left at their default values. Once completed, select **Submit**.



### 4. Configure Avaya AES

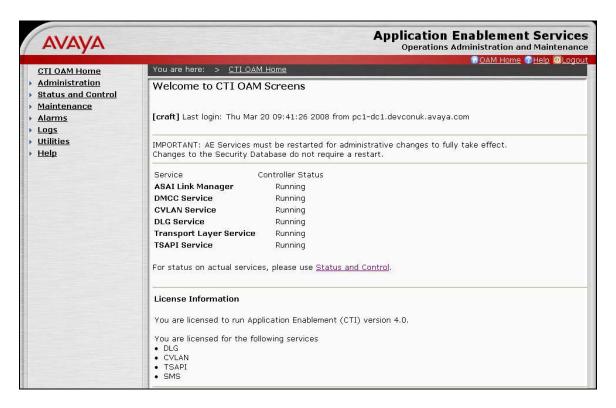
This section provides the procedures for configuring Avaya AES. The procedures fall into the following areas.

- Verify Avaya AES licensing.
- Administer TSAPI link.
- Configure CTI User
- Configure SMS

Basic configuration related to the switch connection between Avaya Communication Manager and Avaya Application Enablement Services is assumed to have been established.

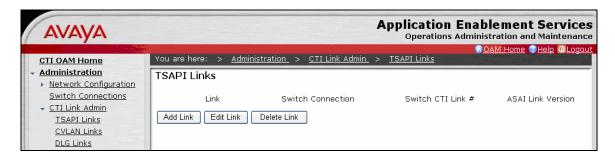
#### 4.1. Verify Avaya AES Licensing

Initialize the AES OAM web interface by browsing to "https://x.x.x.x/MVAP/index.jsp", where "x.x.x.x" is the IP address of the AES, and log in using the proper credentials (not shown). From the OAM Home screen, select **CTI OAM Administration** (not shown) to bring up the CTI OAM Home menu. Verify the TSAPI and SMS services are licensed at the Welcome to CTI OAM Screens screen by ensuring that "TSAPI" and "SMS" are in the list of services in the License Information section.



#### 4.2. Administer TSAPI link

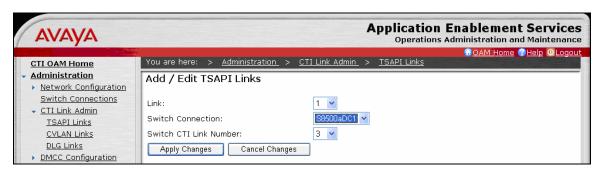
From the CTI OAM Home menu, select **Administration > CTI Link Admin > TSAPI Links**. On the TSAPI Links screen, click **Add Link** 



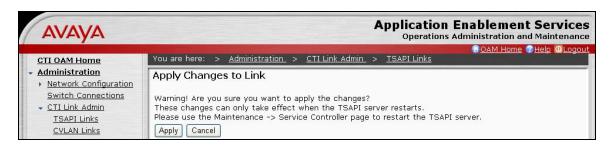
On the Add/Edit TSAPI Links screen, enter the following values.

- Link: Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection being used from the drop-down list.
- Switch CTI Link Number: Corresponding CTI link number configured in Section 3.1.

Once completed, click **Apply Changes**.



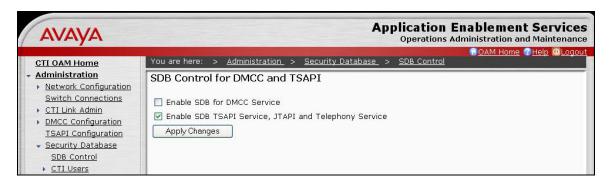
On the Apply Changes to Link screen, click **Apply**.



#### 4.3. Configure the Security Database

This section assumes that a CTI user was previously administered. Information on how to do this is available in the Avaya AES product documentation in reference [2].

From the CTI OAM Home menu, select **Administration > Security Database > SDB Control**. On the SDB Control for DMCC and TSAPI screen check the **Enable SDB TSAPI Service**, **JTAPI and Telephony Service** checkbox. Select **Apply Changes**.



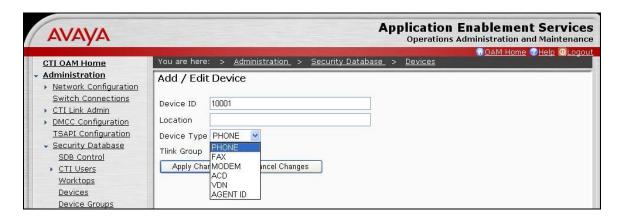
From the CTI OAM Home menu, select **Administration > Security Database > Devices**. On the Devices screen enter the Avaya Communication Manager extension number for a physical station, agent-id, hunt group or VDN and select **Add Device**.



On the Add / Edit Device screen, select from the **Device Type** drop down box as follows:

- Select **PHONE** if the device being added is a physical station.
- Select **AGENT ID** if the device being added is an agent id.
- Select **ACD** if the device being added is a hunt group.
- Select **VDN** if the device being added is a VDN.

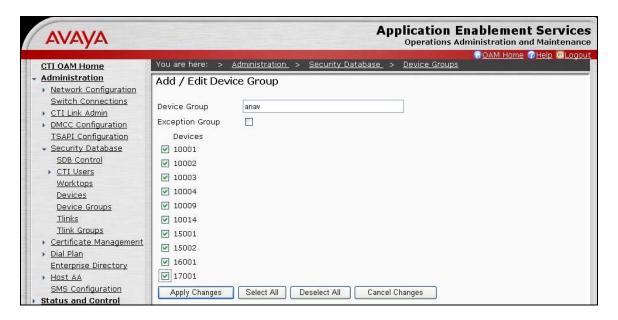
When complete, select **Apply Changes**. Repeat this procedure for every device in the contact centre.



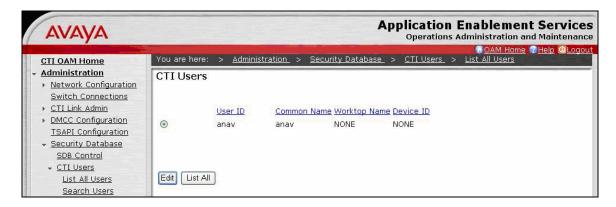
From the CTI OAM Home menu, select **Administration > Security Database > Device Groups**. On the Device Groups screen enter descriptive name for the group and select **Add Device Group**.



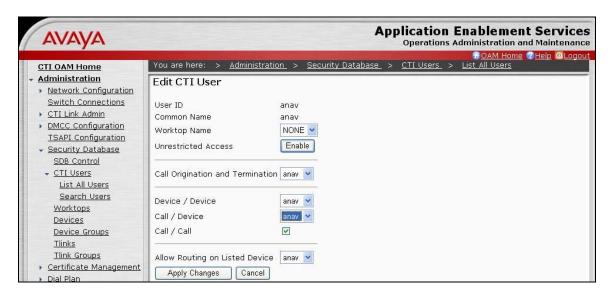
On the Add / Edit Device screen, check each device that is required to be monitored by A-NAV. When completed, select **Apply Changes**.



From the CTI OAM Home menu, select **Administration > Security Database > CTI Users > List All Users**. Select the radio button next to the user created for A-NAV, then select **Edit**.



On the **Edit CTI User** screen, check the **Call / Call** checkbox and select the device group create above in the **Call Origination and Termination**, **Device / Device**, **Call / Device** and **allow Routing on Listed Device** drop down boxes. When completed, select **Apply Changes**.

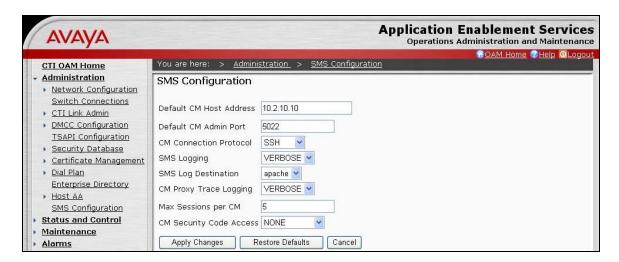


### 4.4. Configure SMS

From the CTI OAM Home menu, select **Administration > SMS Configuration**. On the **SMS Configuration** screen, configure the fields as follows.

- **Default CM Host Address:** Enter the IP address of the Avaya Communication Manager server.
- Default CM Admin Port: "5022"
- CM Connection Protocol: "SSH"

The rest of the fields may be left at their defaults. When completed, select **Apply Changes**.



# 5. Configure ITNAVIGATOR A-NAV

This section provides the procedures for configuring ITNAVIGATOR A-NAV. The procedures fall into the following areas.

- Configure the JTAPI Probe.
- Configure the JTAPI Functional server.
- Configure SMS settings.

Please note that it is expected that the installer is familiar with configuring agents, skills and VDNs, etc. on ITNAVIGATOR A-NAV as the focus of these Application Notes is on the configuration of the JTAPI and SMS interfaces only. For all other provisioning information, such as software installation, installation of optional components, basic configuration of ITNAVIGATOR A-NAV, etc., refer to the ITNAVIGATOR A-NAV product documentation in reference [3].

#### 5.1. Configure the JTAPI Probe

On the server where A-NAV is installed, open the "TSAPI.PRO" file for editing. The "TSAPI.PRO" file is located by default in the "\$DRIVE:\NAVPlatform\JTapiProbe\bin" folder, where "\$DRIVE" is the hard drive on which A-NAV is installed. In the "TSAPI.PRO" file under [Telephony Servers], enter a line that reads "x.x.x.x=450", where "x.x.x.x" is the IP address of the Avaya AES. When completed, save and close the file.

```
File Edit Format View Help

# tsapi.pro - Telephony Services API Properties File for JTAPI

# This file must be located in one of the directories found in CLASSPATH.

# This is a list of the servers offering Telephony Services via TCP/IP.

# Either domain name or IP address may be used; the default port number is 450.

# The form is: host_name=port_number For example:

# tserver.mydomain.com=450

# 127.0.0.1=450

# (Remove the '#' when creating actual server entries.)

[Telephony Servers]

10.2.10.20=450
```

In the same folder, open the "config.xml" file for editing. In the **loginID** and **password** lines, enter the login ID and password of the Avaya AES CTI user. In the **hostname** line, enter the hostname of the server hosting A-NAV. When completed, save and close the file.

#### 5.2. Configure the Functional Server

The JTAPI Functional Server is configured in the same way as the JTAPI Probe Server. The "TSAPI.PRO" and "config.xml" files are located by default in the

"\$DRIVE:\NAVPlatform\JTapiProbe\bin" folder, where "\$DRIVE" is the hard drive on which A-NAV is installed. The "TSAPI.PRO" file should be configured exactly the same as for the JTAPI Probe Server in **Section 5.1**. Configure the lines in the "config.xml" file as follows.

- **login:** Enter the login ID of the Avaya AES CTI user.
- password: Enter the password of the Avaya AES CTI user.
- **DialingPrefix:** Enter the Avaya Communication Manger feature access code for "Service Observ Listen Only" created in **Section 3.2**.
- **DialingPrefixws:** Enter the Avaya Communication Manger feature access code for "Whisper Page" created in **Section 3.2**.
- OutsideDialingPrefix: Enter the Avaya Communication Manger feature access code for "Automatic Route Selection (ARS) created in Section 3.2.
- **RemoteLogout:** Enter the Avaya Communication Manger feature access code for "Remote Logout of Agent" created in **Section 3.2**.

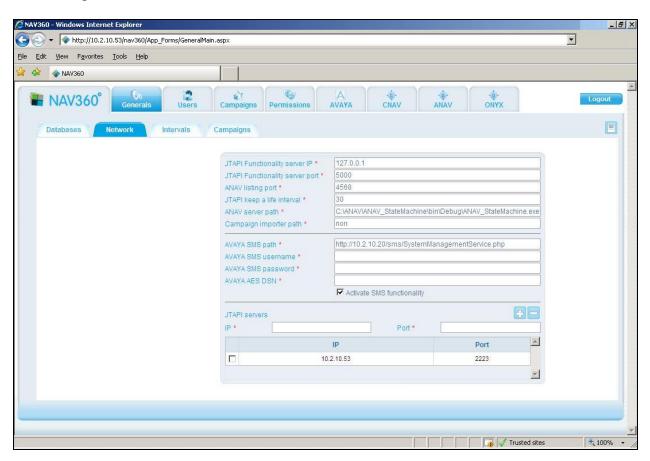
When completed, save and close the file.

#### 5.3. Configure SMS Settings

From any PC on the same network as the A-NAV server, using a web browser, enter "<a href="http://x.x.x.x./nav360">http://x.x.x.x./nav360</a>", where "x.x.x.x" is the IP address of the A-NAV server, and log in when prompted (not shown). Select the **Generals** tab, then select the **Network** tab. Configure the fields as follows.

- **AVAYA SMS path:** Enter "<u>http://x.x.x.x/sms/SystemManagement/Service.php</u>", where "x.x.x.x" is the IP address of the AES.
- **AVAYA SMS username:** Enter the Avaya Communication Manager administrator login ID created in **Section 3.3**.
- **AVAYA SMS password:** Enter the password for the Avaya Communication Manager login ID.

When completed, select the button.



### 6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying A-NAV's handling of the JTAPI and SMS protocols to request and respond to Avaya Communication Manager features.

The serviceability testing focused on verifying A-NAV's ability to recover from an outage condition, such as busying out the CTI link and disconnecting the Ethernet cable for the CTI link.

#### 6.1. General Test Approach

All feature and serviceability test cases were performed manually. The verification included checking proper states at the telephone sets, and viewing the states shown on the A-NAV user interface.

#### 6.2. Test Results

All test cases were executed and passed.

# 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, AES, and ITNAVIGATOR A-NAV.

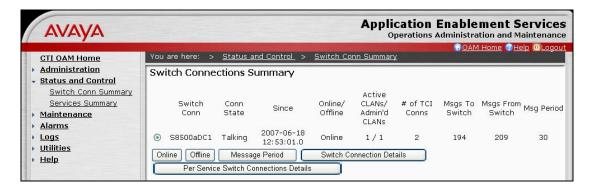
### 7.1. Verify Avaya Communication Manager

Verify the status of the administered CTI link by using the "status aesvcs cti-link" command. The **Service State** should show as "established".

3	4	no	AEServer	established	216	210		
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd		
			AE SERVICES	CTI LINK STAT	US			
status aesvcs cti-link								

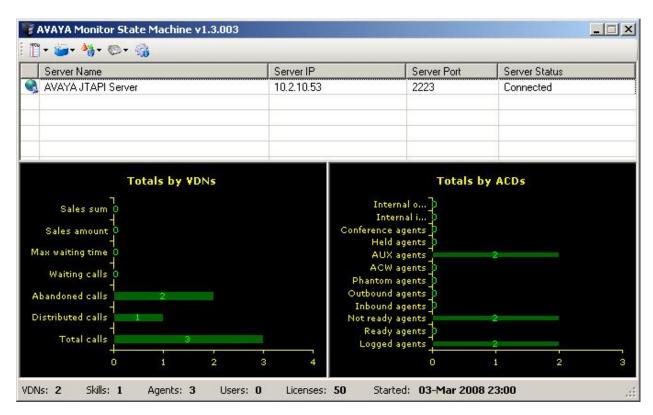
#### 7.2. Verify Avaya Application Enablement Services

From the CTI OAM Home menu, verify the status of the administered CTI link by selecting **Status and Control > Switch Conn Summary**. The **Conn State** should show "Talking".



### 7.3. Verify ITNAVIGATOR A-NAV

On the A-NAV server double-click the icon in the notification area of the taskbar. On the AVAYA Monitor State Machine screen, verify the **Server Status** column reads "Connected"



#### 8. Conclusion

These Application Notes describe the configuration steps required for IT NAVIGATOR A-NAV to successfully interoperate with Avaya Communication Manager and Avaya AES. ITNAVIGATOR A-NAV receives real-time information about agent, hunt-group and VDN status from Avaya AES using JTAPI and presents this data to the user via a web interface. ITNAVIGATOR A-NAV also has the ability to add/change agent IDs to Avaya Communication Manager using the SMS interface of Avaya AES. During compliance testing ITNAVIGATOR A-NAV used JTAPI information to accurate reflect the status of the call center devices and also used the SMS interface to make additions and changes to the Avaya Communication Manager agent ID.

#### 9. Additional References

This section is optional. Other Application Notes or references to product documentation may be listed here.

- [1] Administrator Guide for Avaya Communication Manager, Doc ID: 03-300509, Issue 4, January 2008, available at: <a href="http://support.avaya.com">http://support.avaya.com</a>.
- [2] Avaya Application Enablement Services 4.1 Administration and Maintenance Guide, Doc ID: 02-300357, Issue 9, February 2008, available at: <a href="http://support.avaya.com">http://support.avaya.com</a>.
- [3] A-NAV product documentation is available on request from ITNAVIGATOR. <a href="http://itnv.com">http://itnv.com</a>

#### ©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 <a href="mailto:devconnect@avaya.com">devconnect@avaya.com</a>.