Application Notes for PlantCML Sentinel CM with Avaya Communication Manager with Local Survivable Processor and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the PlantCML Sentinel CM 911 incident management solution to successfully interoperate with Avaya Application Enablement Services. The PlantCML Sentinel CM is an integral part of the Avaya Public Safety Communication Solution. These Application Notes describe the configuration needed to provision Avaya Application Enablement Services in a Local Survivable Processors (LSP) configuration with Avaya Communication Manager. An Avaya Application Enablement Services (AES) server is required at each local site with associated application. This configuration ensures the most seamless survivability during a failover to LSP servers. The sample configuration includes an Avaya S8720 Media Server pair at the main site, and Avaya G350 Media Gateway with S8300 Media Server LSP at the remote site.

Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab at the request of the Solutions Marketing Team.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the configuration steps required for the PlantCML Sentinel CM 911 incident management solution to successfully interoperate with Avaya Application Enablement Services. The PlantCML Sentinel CM is an integral part of the Avaya Public Safety Communication Solution. These Application Notes describe the configuration needed to provision Avaya Application Enablement Services in a Local Survivable Processors (LSP) configuration with Avaya Communication Manager. An Avaya Application Enablement Services (AES) server is required at each local site with associated application. This configuration ensures the most seamless survivability during a failover to LSP servers. The sample configuration includes an Avaya S8720 Media Server pair at the main site, and Avaya G350 Media Gateway with S8300 Media Server LSP at the remote site.

1.1. Public Safety Communication Solution Overview

The Avaya Public Safety Solution is designed to help government and private agencies responsible for the delivery of public safety services to enterprises and civilian populations. This includes:

- **Avaya Contact Center** applications such as expert agent selection to ensure the most qualified and most available resource rapidly attends to the case.

- **PlantCML Sentinel CM and Intelligent Work Station** integration which provides the public safety community with call-center solutions designed to streamline emergency call-taking. Sentinel CM is a 911 incident management solution, and integration with Avaya Communication Manager is achieved through the Avaya Application Enablement Services (AES) Telephony Services Application Programming Interface (TSAPI) & Device, Media and Call Control Interface (DMCC) services.

- **Raytheon JPS ACU-2000IP Intelligent Interconnect System** integration which provides seamless communication across traditionally disparate communications such as Land-based Mobile Radio (LMR). The ACU-2000IP is a radio IP/SIP gateway that allows IP-PBX stations to interface with radios. Multiple interface cards allow all radios to be a part of the IP-PBX system. Integration with Avaya Communication Manager is achieved through the SIP Enablement Services (SES).

- **NICE CLS/VoIP Logger** integration for secure recording of audio on the entire chain of service delivery from the conversations with the citizen, to command and control and dispatch, to resolution.

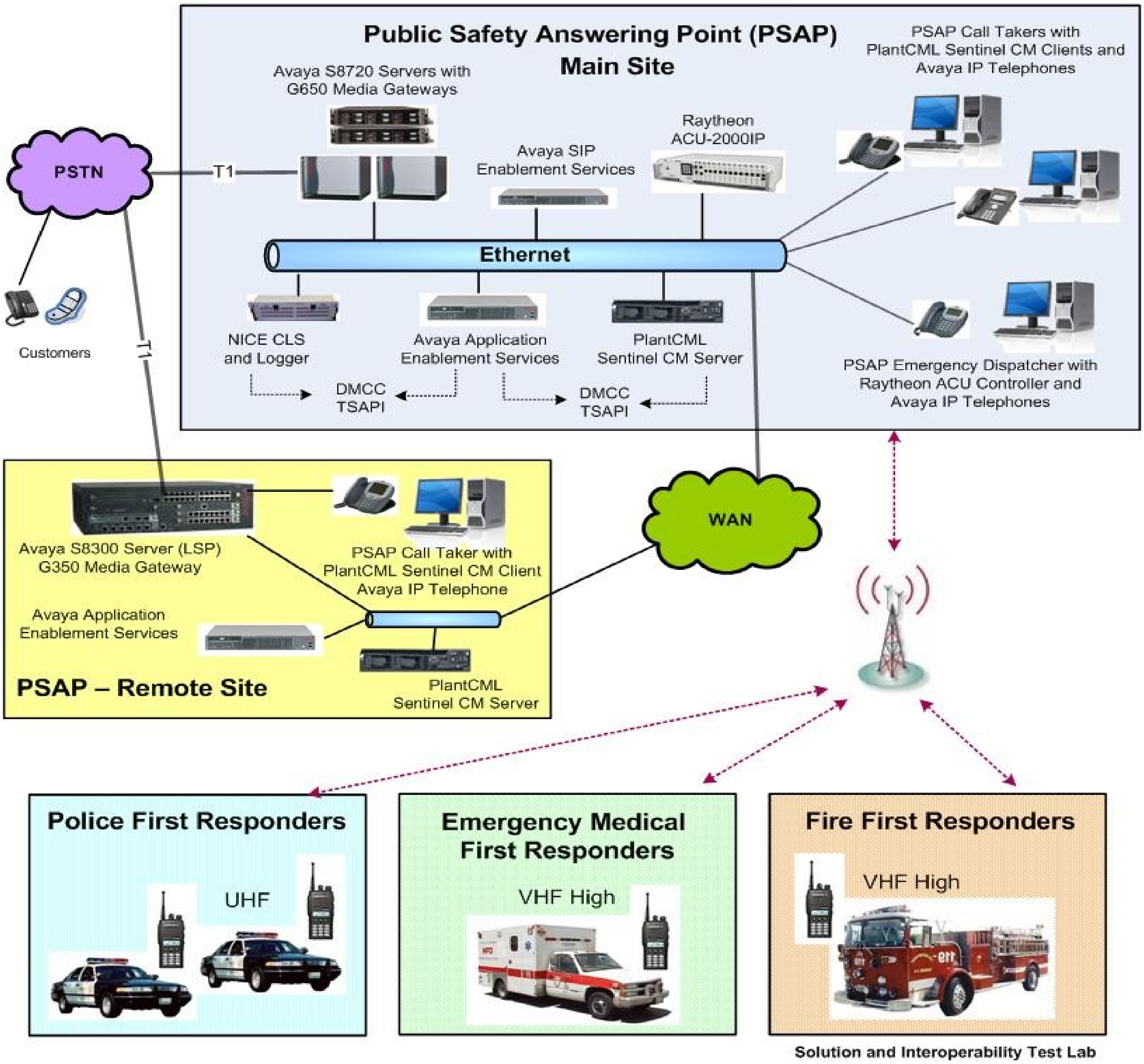


Figure 1: Avaya Public Safety Solution Reference Configuration

1.2. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing scenarios focused on the integration of PlantCML Sentinel CM with Avaya Communication Manager via Avaya AES Release 4.2.1. The specific tests include the following areas:

- Queue 911 incoming calls
- Answer, hold, transfer, conference calls to PSAP agents.
- Monitor / Barge-in / Service Observing / Whisper-page interactions
- Call park, and call pickup interactions

The serviceability testing focused on verifying the ability of Sentinel to recover from adverse conditions, such as:

- S8720 Server interchanges / Reset
- WAN failure
- Busyout C-LANs and CTI links

1.3. Support

Technical support on PlantCML Sentinel can be obtained through the following:

- **Temecula:** (800) 491-1734
- **Gatineau:** (800) 265-8325

1.4. PlantCML Sentinel CM Overview

PlantCML Sentinel CM is an IP based incident response system that:

- receives 911 emergency and administrative calls
- automatically looks up the caller's location based on the caller's telephone number and other information
- presents the call to a call taker at a Sentinel 9-1-1 workstation
- enables call takers to transfer call or data to outside agencies (e.g., fire, police, ambulance, Sheriff's office)

National Emergency Number Association (NENA) recommends critical reliability of the IP-PBX, duplicate AES servers and redundant PlantCML Sentinel CM servers. The PlantCML Sentinel CM servers function as an active/standby, with the standby ready to take over from the active server upon failure. The redundant PlantCML Sentinel CM servers use the CTI link to communicate with each AES server. Telephony Services Application Programming Interface (TSAPI) is used within Sentinel CM Server to automatically retrieve relevant provisioning information from Avaya Communication Manager and to monitor the call queue, etc.

PlantCML Sentinel CM solution consists of:

- A pair of Sentinel CM Servers
- Sentinel 9-1-1 Intelligent Workstations.

The 911 call answering agents have Sentinel 9-1-1 Intelligent Workstations (IWS) as their desktops and are equipped with an Avaya IP Telephone. Sentinel 9-1-1 IWS are Windows XP machines with the Sentinel 9-1-1 client application. This application provides visual incoming call alerts, and Automatic Location Information (ALI) call information to the 911 call answering agents. Each Sentinel 9-1-1 client has both a TSAPI connection and a Device, Media and Call Control (DMCC) API connection to Avaya AES. The TSAPI call control services are utilized by the Sentinel 9-1-1 clients to support call related actions initiated from the agent desktops, such as log in, answer, and transfer calls. The Device Media and Call Control API services are utilized by the Sentinel 9-1-1 clients to support single button activation of features, such as call park and call pickup from the agent desktops.

When an incoming 911 call is routed by Avaya Communication Manager and delivered to an available agent, the Sentinel active server utilizes the Automatic Numbering Identification (ANI) in the TSAPI event reports to look up the associated Automatic Location Identification (ALI) information, and populates the answering agent screen with both ANI and ALI. The ALI information is typically provided by an external ALI provider. The Sentinel active server will interface with this ALI provider. For the compliance testing, the Sentinel server utilized an internal database to obtain the ALI information.

1.4.1. Sentinel 9-1-1 Intelligent Workstations (IWS)

The Sentinel 9-1-1 Intelligent Workstation enables the 911 call answering personnel to easily manage and handle 911 calls. The Sentinel 9-1-1 Application provides one-button transfers for voice and data, audio and visual incoming call alerts, dynamic call status indicators, and intelligent call prompting. TTY and instant recall recorder functionalities are integrated in the Sentinel 9-1-1 application.

1.4.2. Sentinel GUI

The Sentinel GUI provides a Windows interface to all features of the 9-1-1 CTI application. The navigation of the application is through a PC keyboard and the mouse pointing device. The GUI is designed around a Microsoft Windows standard user interface.

1.4.3. Patriot Communications Server (PCS) API

The communication with Sentinel Server is realized via the PCS API software layer. Sentinel communicates with Sentinel Server through the CallP Manager module. The transport protocol is TCP over IP.

1.4.4. TSAPI

Telephony Server Application Interface (TSAPI) is an Avaya API to communicate with an Avaya Telephony Server AES.

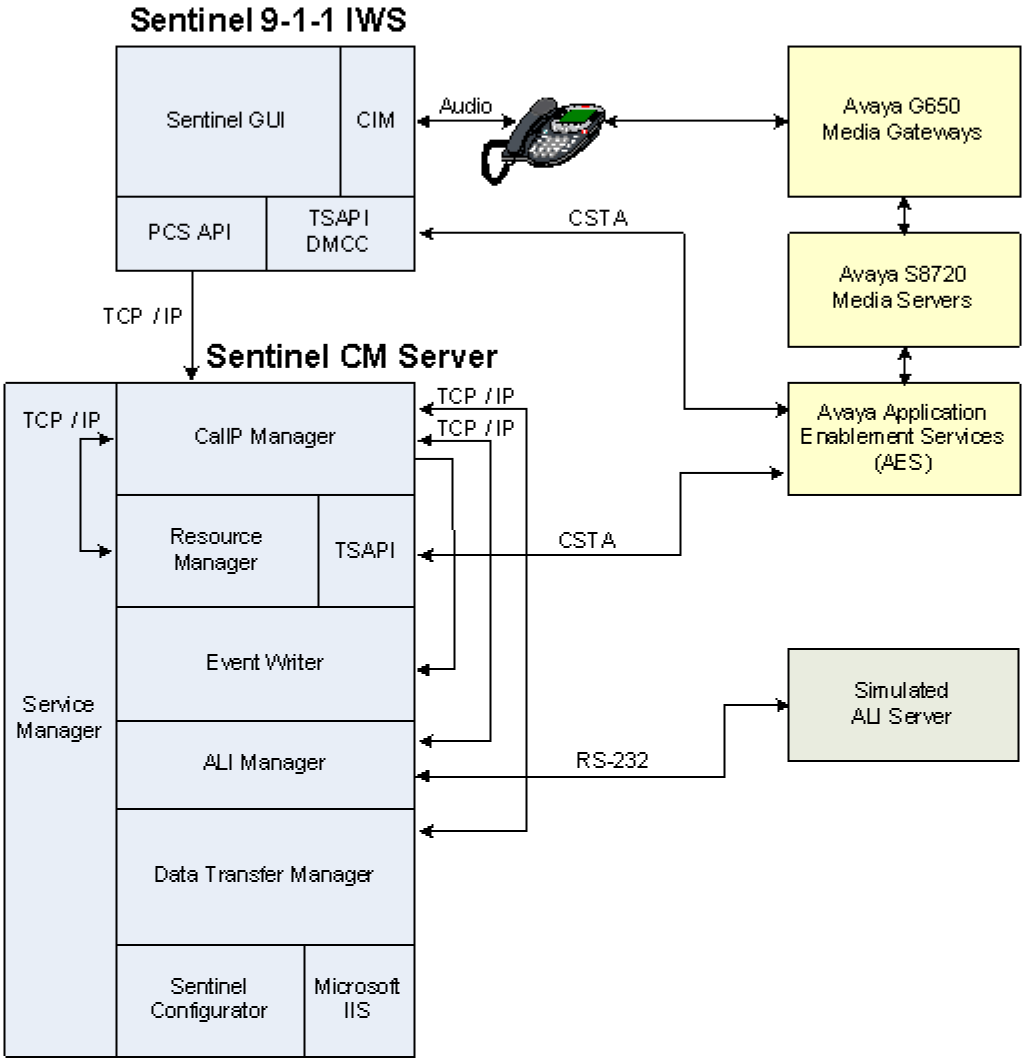
1.4.5. DMCC

DMCC is a Telephony Server API that supports Computer-Supported Telecommunications Applications (CSTA) standard CTI interface. This interface is used to implement features that are not supported by TSAPI (Call Park, Call Pickup).

1.4.6. Computer Interface Module (CIM)

The audio card facilitates voice communication from the telephone set to operator’s headset.

1.4.7. Sentinel CM Server Components



Sentinel Server Service Manager

The Sentinel Server Service Manager starts up all Sentinel Server Services and makes sure they remain operational.

CallP Manager

- Manages the data transactions associated with all the calls of the system.
- Sends system activities to the Event Writer.
- Receives all local PBX activities from the Sentinel and system wide activities from the Resource Manager.
- Provides call detail information (ALI, ESN, STI, etc.) to the Sentinel via TCP/IP.
- Connects to Remote CallP Manager to maintain hot standby duplication.

Resource Manager

- Monitors the activity events in Avaya Application Enablement Server (AES) and forwards the info to the CallP Manager.
- Provides COM interface for the Sentinel Server Configurator.

Event Writer

- Receives the system activity events from the CallP Manager.
- Writes all activity events into the relational database.

ALI Manager

- Provides ALI for 911 and admin calls (manual request).
- ALI is interfaced with an external ALI provider via an RS-232 serial port. For testing purposes, a simulated ALI database will be used.

Data Transfer Manager

This module is responsible for transferring the information given by the CallP Manager to the RS-232 data ports.

Following are supported by PlantCML Sentinel CM Data Transfer Manager, however these were not tested as part of the Solution Validation.

- Communication with CAD systems
- Fax/Modem dial-out
- Dedicated data port
- Interface to DLR logging systems to provide Call Details

1.5. Operational Scenarios

1.5.1. Normal Operation

During normal operation, all the C-LANs in the G650 Media Gateways will register with the active S8720 Media Servers. The G650 Media Gateways and the G350 Media Gateway will register with the Main PSAP Site S8720 Media Server.

The AES communicates with Avaya Media Servers via C-LANs. These C-LANs are administered on the Communication Manager **ip-services** form. These C-LANs are also administered on all the AES servers, on the **Switch Connection Edit CLAN** form.

The AES server at the Main PSAP Site and the Remote PSAP Site will have active links to the C-LANs located in G650 Media Gateways. The AES server at the Main Site and the Remote Site will also have link to the S8300 Media Server located at the Remote Site. In the normal operations, this connection state for this link will be "idle".

The PlantCML Sentinel clients at all locations (Main and Remote Site) will use the AES located at the Main Site to provide CTI functionality.

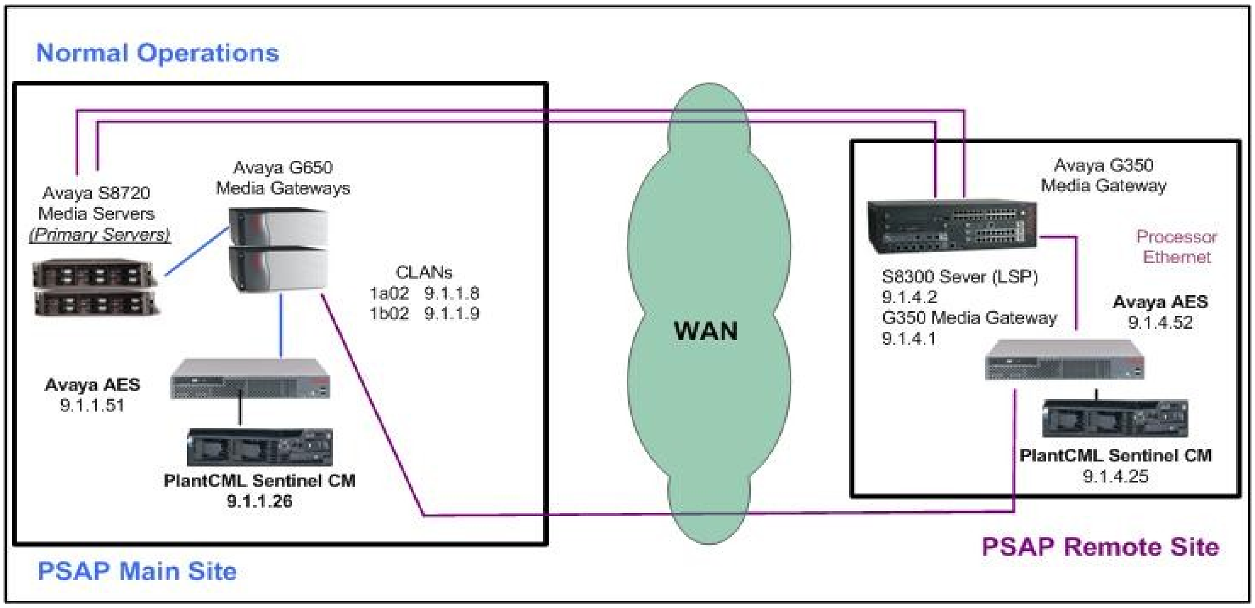


Figure 2

1.5.2. WAN Outage

During WAN outage, the G650 Media Gateways at the Main Site will continue to register to the Main Servers – S8720 Media Servers. The AES at the Main Site will have active links to all the administered C-LANs on the Main Site G650 Media Gateways. The PlantCML Sentinel clients at Main Site will use the AES located at the Main Site to provide CTI functionality.

The G350 Media Gateway at Remote PSAP Site will register to the LSP server – S8300 Media Server located at the local site and will use the local Processor Ethernet. The AES server at the site will lose all its connections to the C-LANs. The PlantCML Sentinel clients at the Remote Site will use this AES server to provide CTI functionality.

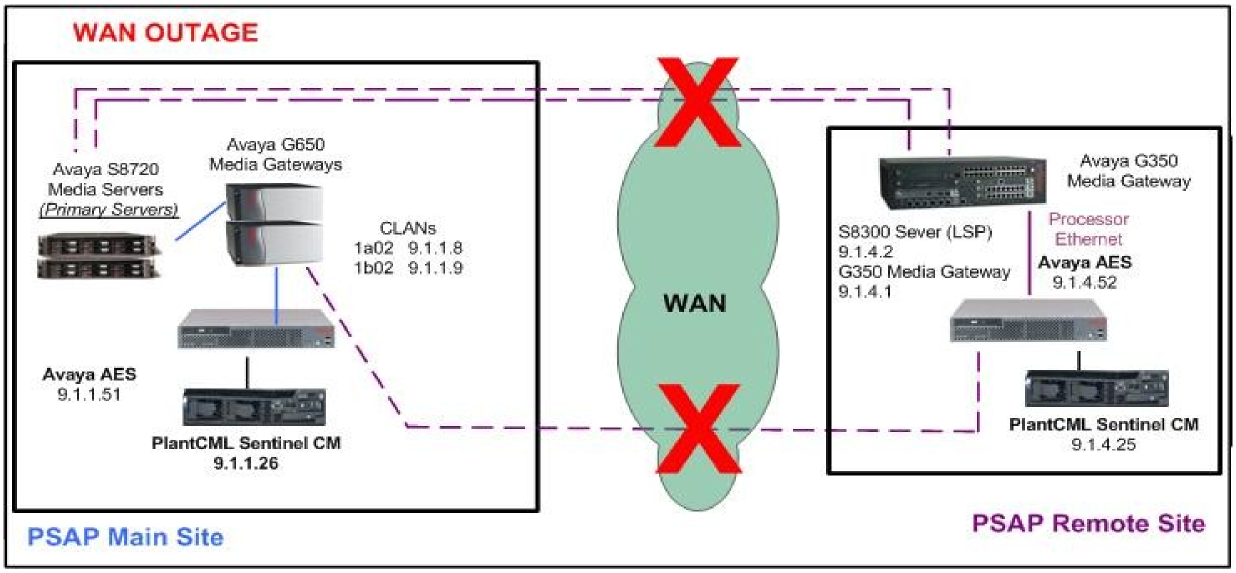


Figure 3

When the connectivity to the main servers is back up, the Remote Site AES server will switch back to the administered C-LANs on the Main Site G650 Media Gateways.

2. Network Topology

The network implemented for the reference configuration is shown in **Figure 4**. The Public Safety Answering Point location consists of Avaya S8720 Servers controlling G650 Media Gateways. The PSAP location is also equipped with a pair of Avaya Application Enablement Services (AES) servers, Avaya IP phones, a pair of PlantCML Sentinel CM servers and multiple Sentinel 9-1-1 clients.

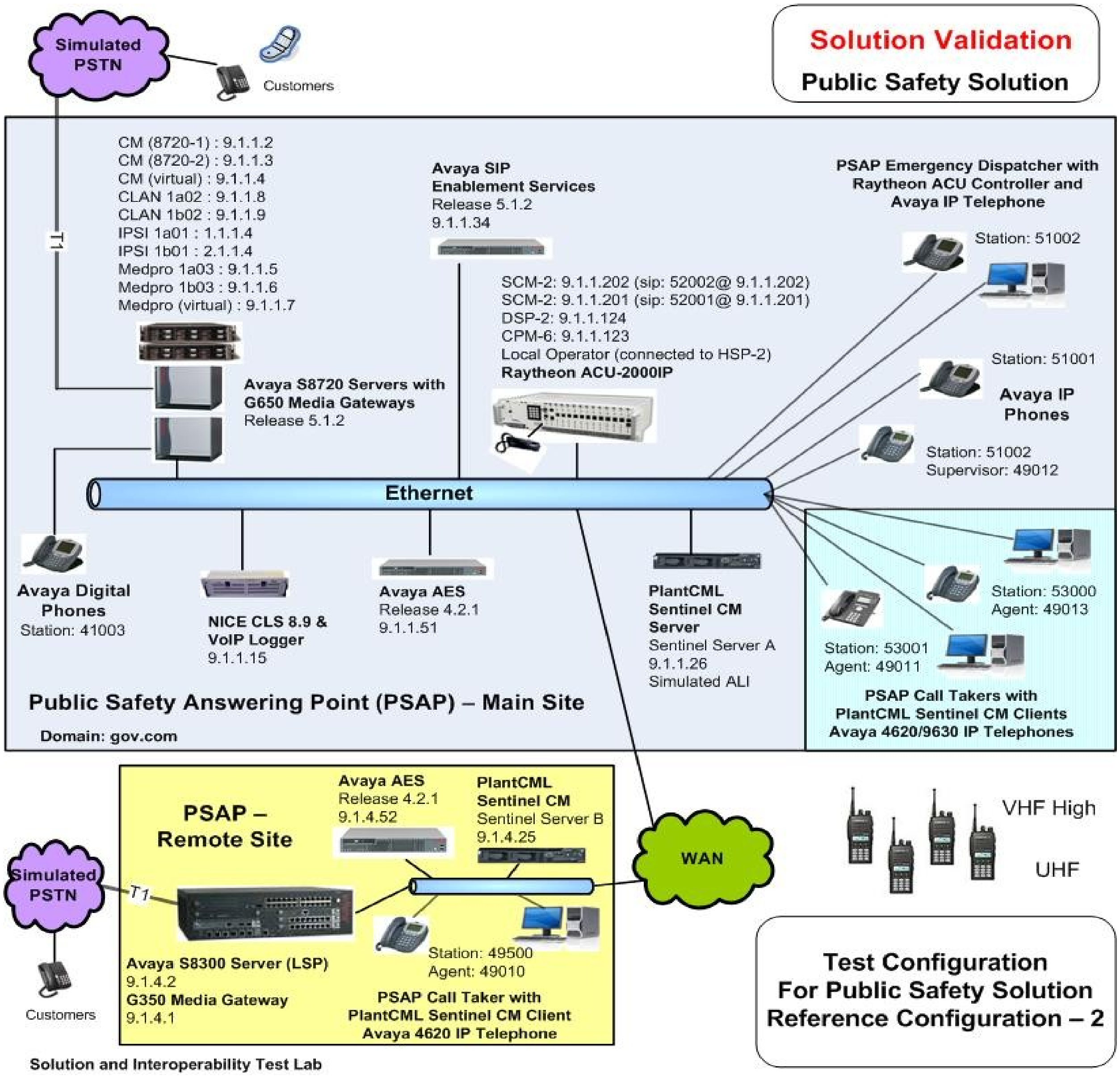


Figure 4: PlantCML Sentinel CM with Avaya Communication Manager and Avaya AES

Note: These Application Notes assume that the reference configuration depicted in Figure 4 is already in place including Avaya Communication Manager, Avaya Media Gateways and Avaya Media Servers at the Main and Remote PSAP Sites. Please consult the appropriate documentation listed in the Reference section of this document for more information on how to set up these components.

Name	IP Address	Location	Network Region
CLAN-01A02	9.1.1.8	PSAP Main Site	1
CLAN-01B02	9.1.1.9	PSAP Main Site	1
govaes2	9.1.1.51	PSAP Main Site	
Server-A	9.1.1.26	PSAP Main Site	
GVT-S8300-LSP	9.1.4.2	PSAP Remote Site	4
govaes1	9.1.4.52	PSAP Remote Site	
Server-B	9.1.4.25	PSAP Remote Site	

IP Address Table

3. Equipment and Software Validated

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

Device Description	Versions Tested
Avaya Communication Manager - S8720 Servers - S8300 Server	Release 5.1.2 (R015x.01.2.416.4)
Avaya G350 Media Gateway	FW Version 27 .26 .0
Avaya G650 Media Gateway - IPSI (TN2312BP) - CLAN (TN799DP) - MedPro (TN2602AP)	 - HW15 FW055 - HW01 FW026 - HW02 FW044
Avaya AES	Release 4.2.1 (Build 20-5)
Avaya 4600 Series H.323 Telephones	R2.9
Avaya 9600 Series H.323 Telephones	R2.0
Avaya 6211 Analog Telephones	N/A
Avaya 2420 Digital Telephones	N/A
PlantCML Sentinel - Sentinel CM Server - Sentinel Intelligent Workstation	 Release 2.0 Build 33 Release 2.0 Build 33 OS for the IWS is Windows XP Professional (Service Pack 2)

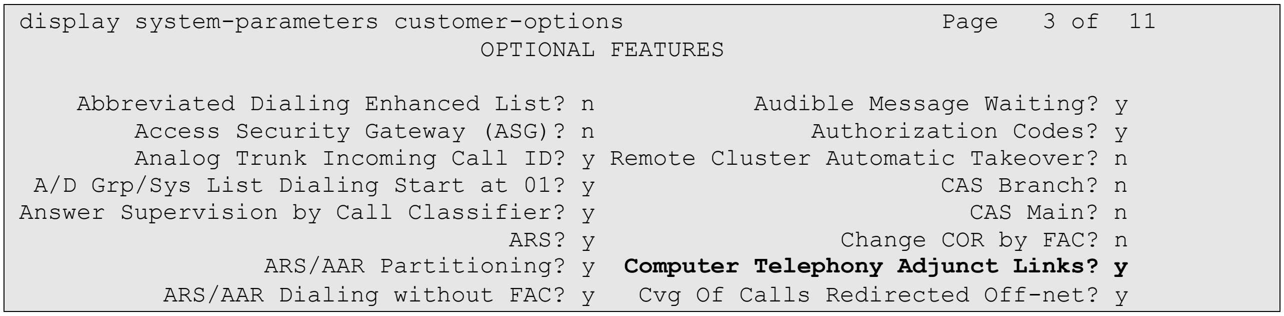
4. Configure Avaya Communication Manager

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

- Verify Avaya Communication Manager License
- Administer IP services for AES transport link
- Administer CTI link for TSAPI service
- Administer Physical Stations
- Administer System Parameters
- Administer Feature Access Codes
- Administer Hunt Group and Skill group
- Administer Agent LoginIDs
- Administer Vector and VDNs
- Administer Survivable Processor ip-services for LSP
- Create Login for PlantCML

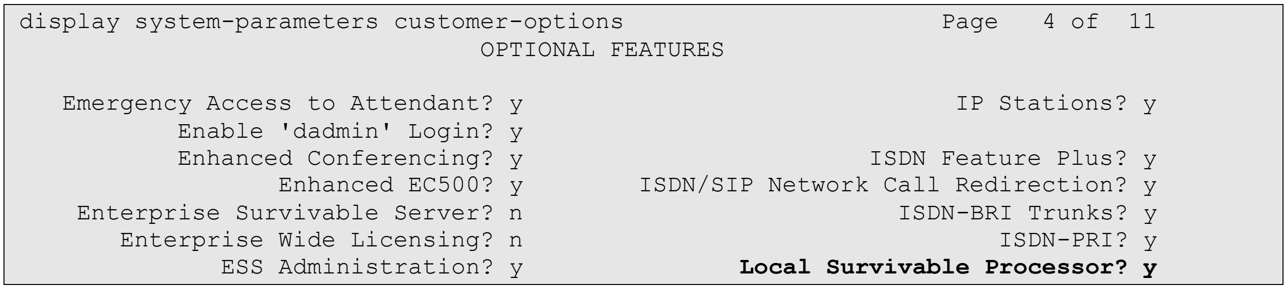
4.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.



```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y Remote Cluster Automatic Takeover? n
 A/D Grp/Sys List Dialing Start at 01? y                      CAS Branch? n
Answer Supervision by Call Classifier? y                        CAS Main? n
                                  ARS? y               Change COR by FAC? n
                 ARS/AAR Partitioning? y  Computer Telephony Adjunct Links? y
          ARS/AAR Dialing without FAC? y   Cvg Of Calls Redirected Off-net? y
```

Navigate to **Page 4**, and verify that the **Local Survivable Processor** customer option is set to “y”.



```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                            IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                     ISDN Feature Plus? y
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                       ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                              ISDN-PRI? y
              ESS Administration? y             Local Survivable Processor? y
```

Navigate to **Page 6**, and verify that the **Expert Agent Selection (EAS)** and **Vectoring (Basic)** customer options are set to “y”.

```
display system-parameters customer-options                      Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 5.0

                                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? y                    Service Observing (VDNs)? y
                    Call Work Codes? y                                  Timed ACW? y
      DTMF Feedback Signals For VRU? y                           Vectoring (Basic)? y
                   Dynamic Advocate? y                       Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y                   Vectoring (G3V4 Enhanced)? Y
```

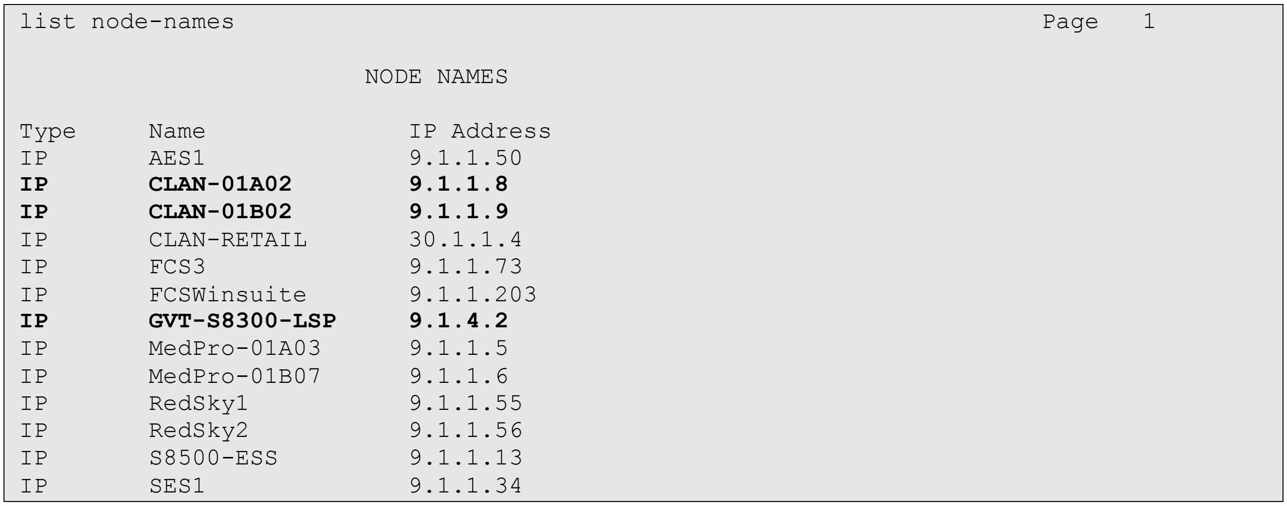
Navigate to **Page 10**, and verify that there are sufficient **IP_API_A** licenses. One such license will be required for each 911 call answering agent.

```
display system-parameters customer-options                      Page  10 of  11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
IP_API_A       : 100            4
IP_API_B       : 100            0
IP_API_C       : 100            0
IP_Agent       : 300            0
IP_IR_A        : 0              0
IP_Phone       : 12000          5
IP_ROMax       : 12000          0
IP_Soft        : 300            0
IP_eCons       : 0              0
```

4.2. Verify Node Names for C-LAN and LSP

Enter the “list node-names” command, and verify the node-names and IP addresses. For the sample configuration, following **Name** and **IP Address** were used. The actual node name and IP address may vary.

C-LAN	
Name	**IP Address**
CLAN-01A02	9.1.1.8
CLAN-01B02	9.1.1.9
LSP	
GVT-S8300-LSP	9.1.4.2

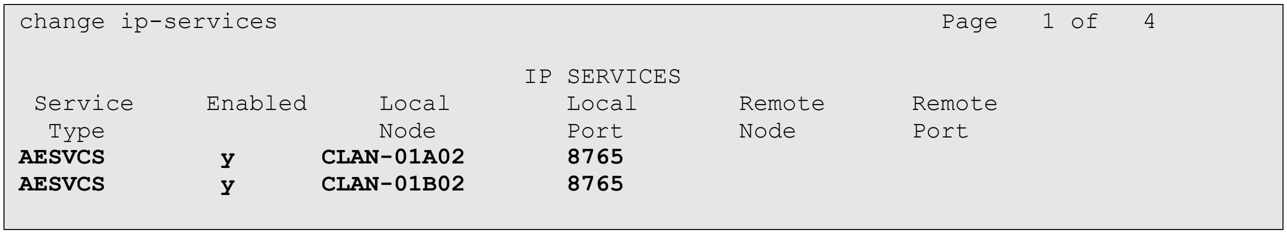


```
list node-names                                                  Page   1

                        NODE NAMES

Type     Name              IP Address
IP       AES1              9.1.1.50
IP       CLAN-01A02        9.1.1.8
IP       CLAN-01B02        9.1.1.9
IP       CLAN-RETAIL       30.1.1.4
IP       FCS3              9.1.1.73
IP       FCSWinsuite       9.1.1.203
IP       GVT-S8300-LSP     9.1.4.2
IP       MedPro-01A03      9.1.1.5
IP       MedPro-01B07      9.1.1.6
IP       RedSky1           9.1.1.55
IP       RedSky2           9.1.1.56
IP       S8500-ESS         9.1.1.13
IP       SES1              9.1.1.34
```

4.3. Administer IP Services for AES Transport Link

Administer the transport link to the AES server with the “change ip-services” command. Add an entry with the following values for fields on **Page 1**:

- **Service Type:** “AESVCS”
- **Enabled:** “y”
- **Local Node:** C-LAN node name from **Section 4.2**
- **Local Port:** Retain the default value of “8765”



```
change ip-services                                        Page   1 of   4

                                   IP SERVICES
 Service     Enabled      Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
AESVCS         y      CLAN-01A02       8765
AESVCS         y      CLAN-01B02       8765
```

Proceed to **Page 4**, and enter the following values:

- **AE Services Server:** Name obtained from the AES server.
- **Password:** Password to be administered on the AES server.
- **Enabled:** “y”

Note that the name and password entered for the **AE Services Server** and **Password** fields are case sensitive, and must match the name and password on the AES server. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing “uname –n” at the Linux command prompt. The same password entered in the screen below will need to be set on the AES server, as described in **Section 5.3.**
System will assign a Server ID to each AES server and this will be required in **Section 6.3.**

Note two AES servers need to be administered on the ip-services form.

```
change ip-services                                            Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      govaes1           *                   y
      2:      govaes2           *                   y
      3:
```

4.4. Administer CTI Link for TSAPI Service

Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields. Submit these changes.

Note two CTI-Links need to be administered, one for each AES server.

```
add cti-link 1                                                 Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 55000
     Type: ADJ-IP
                                                                   COR: 1

     Name: TSAPI GOVAES1
```

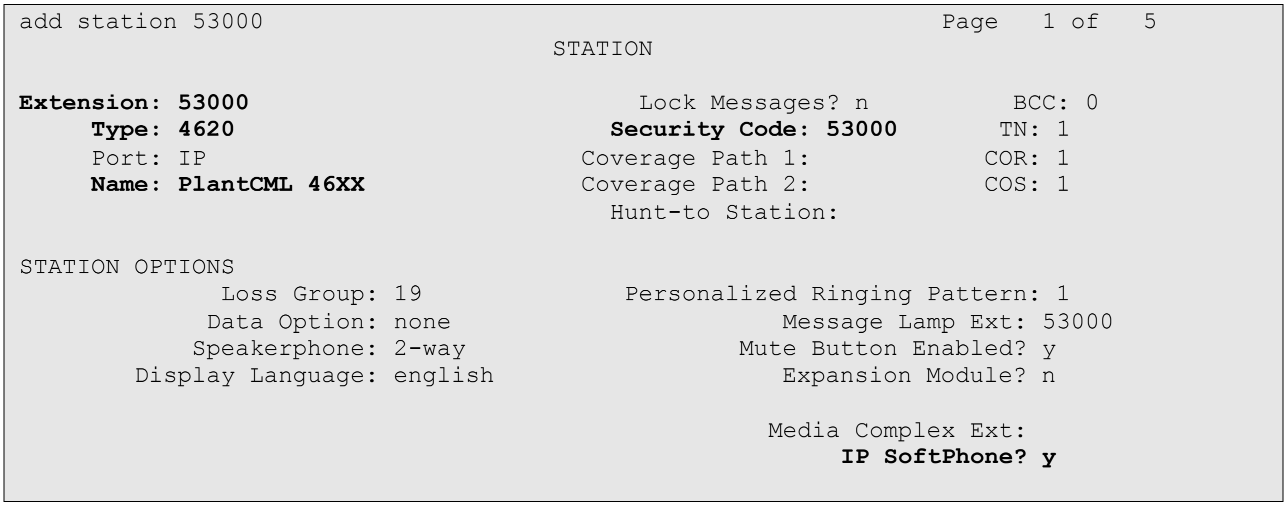
```
add cti-link 2                                                 Page   1 of   3
                                    CTI LINK
 CTI Link: 2
Extension: 55001
     Type: ADJ-IP
                                                                   COR: 1

     Name: TSAPI GOVAES2
```

4.5. Administer Physical Stations

Add a physical station for each 911 call answering agent using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

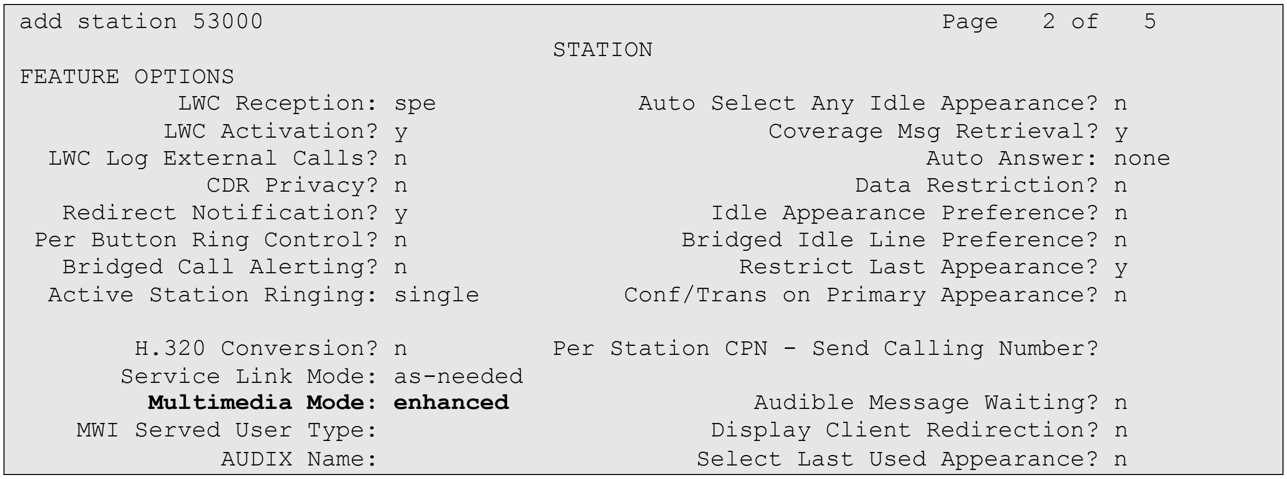
- **Type:** A valid station type. In this case, “4620” and “9630” were used.
- **Name:** A descriptive name.
- **Security Code:** Enter a valid code.
- **IP SoftPhone:** “y”

Note that enablement of **IP SoftPhone** allows the physical station to be controlled by a softphone application such as Sentinel 9-1-1.



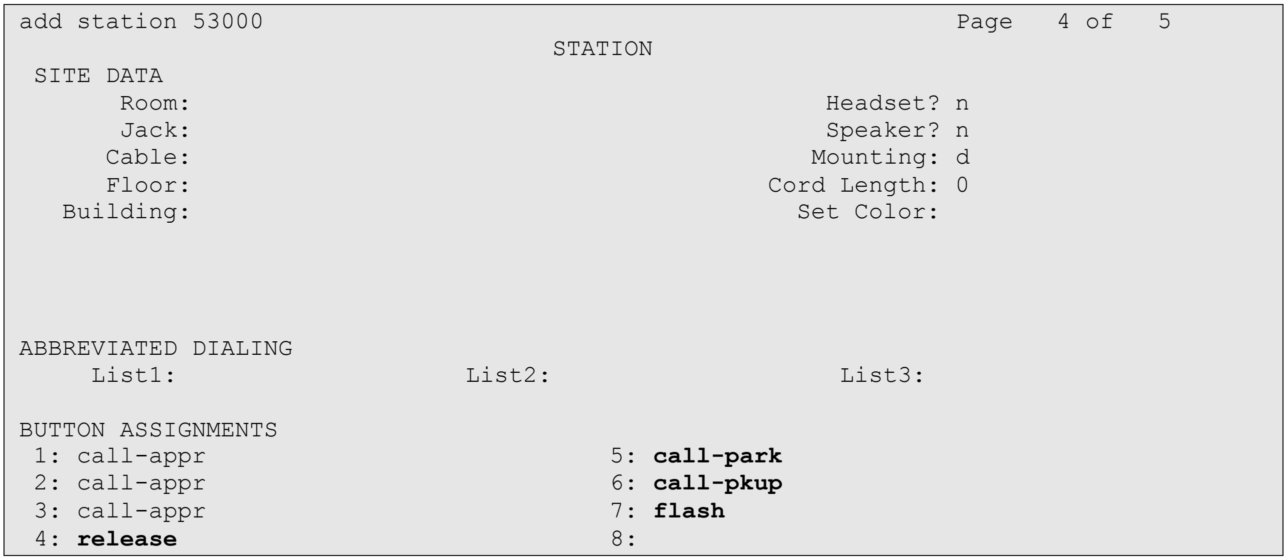
```
add station 53000                                               Page   1 of   5
                                     STATION

Extension: 53000                           Lock Messages? n          BCC: 0
     Type: 4620                          Security Code: 53000      TN: 1
     Port: IP                          Coverage Path 1:            COR: 1
     Name: PlantCML 46XX               Coverage Path 2:            COS: 1
                                         Hunt-to Station:

STATION OPTIONS
              Loss Group: 19              Personalized Ringing Pattern: 1
             Data Option: none                       Message Lamp Ext: 53000
            Speakerphone: 2-way                   Mute Button Enabled? y
        Display Language: english                    Expansion Module? n

                                                    Media Complex Ext:
                                                         IP SoftPhone? y
```

Proceed to **Page 2**, and set the **Multimedia Mode** to “enhanced”. This configuration is needed to enable Sentinel 9-1-1 clients to obtain the phone display information.



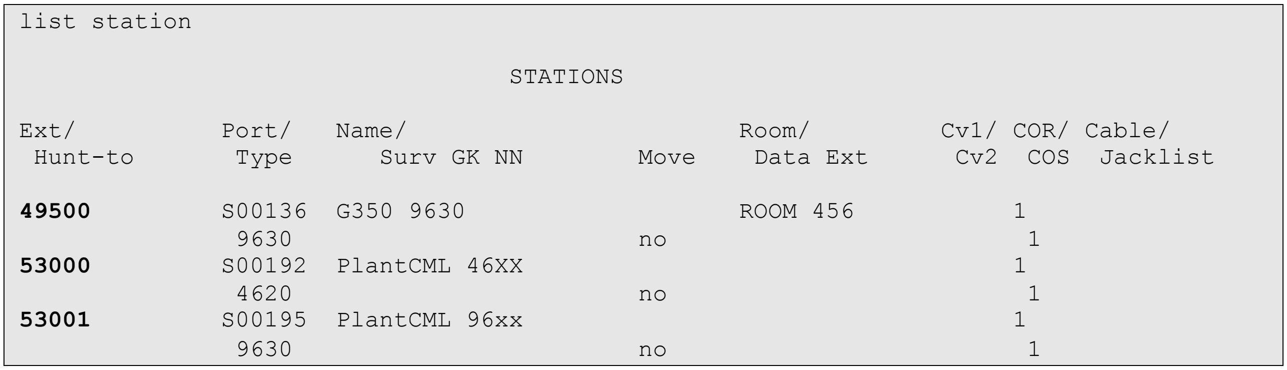
```
add station 53000                                               Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single          Conf/Trans on Primary Appearance? n

        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
```

Depending on phone type, **Page 4** or **Page 5**, assign the following features to any available buttons: “release”, “call-park”, “call-pkup”, and “flash”. Note that each station has to have these three feature buttons. The Sentinel 9-1-1 clients will pick up the correct location of the feature buttons from Avaya AES using the Device, Media and Call Control API.



```
add station 53000                                              Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                               Headset? n
       Jack:                                               Speaker? n
      Cable:                                              Mounting: d
      Floor:                                           Cord Length: 0
   Building:                                             Set Color:




ABBREVIATED DIALING
     List1:                   List2:                   List3:

BUTTON ASSIGNMENTS
 1: call-appr                           5: call-park
 2: call-appr                           6: call-pkup
 3: call-appr                           7: flash
 4: release                             8:
```

Repeat the “add station n” command to add the desired number of stations. For the compliance testing, three stations were administered as shown below.



```
list station

                                  STATIONS

Ext/          Port/   Name/                        Room/         Cv1/ COR/ Cable/
 Hunt-to       Type      Surv GK NN        Move     Data Ext      Cv2  COS  Jacklist

49500         S00136  G350 9630                    ROOM 456           1
               9630                        no                          1
53000         S00192  PlantCML 46XX                                   1
               4620                        no                          1
53001         S00195  PlantCML 96xx                                   1
               9630                        no                          1
```

4.6. Administer System Parameters

Enter the “change system-parameters features” command. Navigate to **Page 4**, and set the **Temporary Bridged Appearance on Call Pickup** to “n”.

```
change system-parameters features                               Page   4 of  17
                        FEATURE-RELATED SYSTEM PARAMETERS
          Reserved Slots for Attendant Priority Queue: 5
                           Time before Off-hook Alert: 10
               Emergency Access Redirection Extension:
 Number of Emergency Calls Allowed in Attendant Queue: 5

               Call Pickup on Intercom Calls? y         Call Pickup Alerting? n
 Temporary Bridged Appearance on Call Pickup? n         Directed Call Pickup? n
                  Extended Group Call Pickup: none
```

Proceed to **Page 6**, and set **Auto Hold** to “y”.

```
change system-parameters features                              Page   6 of  17
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5              Auto Start? n
    Conference Parties with Public Network Trunks: 6               Auto Hold? y
 Conference Parties without Public Network Trunks: 6          Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180         Bridging Tone? y
                 Short Interdigit Timer (seconds): 3         Conference Tone? n
              Unanswered DID Call Timer (seconds): 60         Intrusion Tone? n
              Line Intercept Tone Timer (seconds): 30    Mode Code Interface? y
                 Long Hold Recall Timer (seconds): 0
                      Reset Shift Timer (seconds): 0
     Station Call Transfer Recall Timer (seconds): 0
                               DID Busy Treatment: tone
```

4.7. Administer Feature Access Codes

Enter the “change feature-access-codes” command. Set the **Call Park Access Code** and **Answer Back Access Code**. These will be needed in **Section 6.3** for Park and Unpark. For the sample configuration, *41 and *42 were used.

```
change feature-access-codes                                     Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *70
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: *42

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
                         Call Park Access Code: *41
```

4.8. Administer Hunt Group and Skill group

Avaya Communication Manager needs to be administered for Automatic Call Distribution (ACD) configuration. This will include hunt groups and skill groups, Agent LoginIDs, call vectors and VDNs.

The following section briefly describes the hunt groups, skill groups and Agent LoginIDs pertinent to the sample configuration. For additional information on ACD configuration, please refer to **Avaya Communication Manager Guide to ACD Call Centers** [3].

For the 911 incoming calls, one hunt group needs to be administered on Avaya Communication Manager. Administer the hunt group by entering the “add hunt-group xxx” command, where “xxx” is the hunt group, and not a dialable extension. The hunt group number has a direct relation to skill group number. “xxx” is also the skill group number that will be defined in the agent-loginID screen and queued to in the vector.

Enter the following values for the specified fields, and retain the default values for the remaining fields.

- Group Name: **Enter a descriptive name**
- Group Extension: **Dialable extension of the hunt group**
- Group Type: **ucd-mia** (uniform call distribution – most idle agent)
- COR: **Class of restriction for hunt group**
- ACD: **y**
- Vector: **y**
- Queue: **y**
- Skill: **y**

```
add hunt-group 15                                             Page   1 of   3
                                  HUNT GROUP

            Group Number: 15                            ACD? y
              Group Name: PlantCML                    Queue? y
         Group Extension: 49015                      Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                     MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited

add hunt-group 15                                             Page   2 of   3
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
                 Measured: internal        Service Objective (sec): 20
     Supervisor Extension: 51001          Service Level Supervisor? n
```

4.9. Administer Agent LoginIDs

Administer the 911 answering agents by using the “add agent-loginID xxxxx” (where xxxxx is the extension of the agent). Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Login ID:** Will be populated automatically
- **Name:** A descriptive name
- **Password:** Must use 4 digit numeric password
- **Call Handling Preference:** Enter **“**skill-level”
- **SN** Enter the hunt group (skill) number
- **SL** Enter appropriate skill level. “1” was used for this testing.

```
add agent-loginID 49010                                         Page   1 of   2
                                 AGENT LOGINID

                Login ID: 49010                                     AAS? n
                    Name: PlantCML Agent1                         AUDIX? n
                      TN: 1                               LWC Reception: spe
                     COR: 1                      LWC Log External Calls? n
           Coverage Path:                       AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                               Password: *
                                                Password (enter again): *
                                                            Auto Answer: station
                                                      MIA Across Skills: system
                                              ACW Agent Considered Idle: system
                                              Aux Work Reason Code Type: system
                                                Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                                Forced Agent Logout Time:

     WARNING:  Agent must log in again before changes take effect


  add    agent-loginID 49010                                     Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

    SN   RL SL           SN   RL SL           SN   RL SL           SN   RL SL
 1: 15      1       16:                 31:                 46:
 2: 16      1       17:                 32:                 47:
 3:                 18:                 33:                 48:
 4:                 19:                 34:                 49:
 5:                 20:                 35:                 50:
 6:                 21:                 36:                 51:
```

Make a note of Login ID and Password for each agent administered to handle 911 calls. This will be needed in **Section 5.7** to administer users on the AES servers.

Repeat the “add agent-loginID xxxx” command to add the desired number of 911 answering agents. For the sample configuration, three 911 call answering agents and one 911 Supervisor were administered as shown below:

```
list agent-loginID 49010 count 4

                              AGENT LOGINID

Login         Name/           Dir Agt COR Ag SO Skil/Lv Skil/Lv Skil/Lv Skil/Lv
ID            Extension       AAS/AUD     Pr

49010         PlantCML Agent1         1   lvl n   15/01   16/01     /       /
              unstaffed                             /       /       /       /
49011         PlantCMl Agent2         1   lvl n   15/01     /       /       /
              unstaffed                             /       /       /       /
49012         911 Supervisor          1   lvl n   15/01   16/01     /       /
              unstaffed                             /       /       /       /
49013         Remote PlantCML         1   lvl n   15/01   16/01     /       /
              unstaffed                             /       /       /       /
```

4.10. Administer Vector and VDNs

The incoming 911 calls will use a Vector Directory Number (VDN). A VDN is a “soft” extension number that is not assigned to an equipment location. VDNs are assigned within the parameters permitted by the customer dial plan analysis table. VDNs point to a vector number. Vectors determine how a specific call should be routed and what call treatment the call should be given. For the sample configuration, the following VDN and Vector were used.

```
display vdn 53015                                                   Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 53015
                                 Name*: PlantCML HotLine
                         Vector Number: 20
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

```
display vector 20                                                Page   1 of   6
                                  CALL VECTOR

    Number: 20               Name: Bilingual 911
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    0   secs hearing silence
02 collect      1    digits after announcement 58000    for none
03 goto step    5             if digits          =      1
04 goto step    6             if digits          =      2
05 queue-to     skill 15   pri m
06 queue-to     skill 16   pri m
07 stop
```

4.11. Administer Survivable Processor

Issue the **change survivable-processor <xx>** command, where **<xx>** is the node-name for the LSP server. In the sample configuration, this is **GVT-S8300-LSP**.

Navigate to **Page 2** and enter the following value:

- Enabled: Enter "**o**" for the AES server associated with the LSP site. This will override for LSPs, and the AES server will always connect to an LSP first. In the sample configuration, this is server-id 1 as administered in **Section 4.3**.

```
change survivable-processor GVT-S8300-LSP                       Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local              Local    Remote             Remote
  Type              to dsk  Node               Port     Node               Port
  CDR1        i       n     CLAN-01A02         0        FCS3               5050
  AESVCS      o       n     procr              8765
  AESVCS      i       n     CLAN-01B02         8765
```

4.12. System-Parameter Features

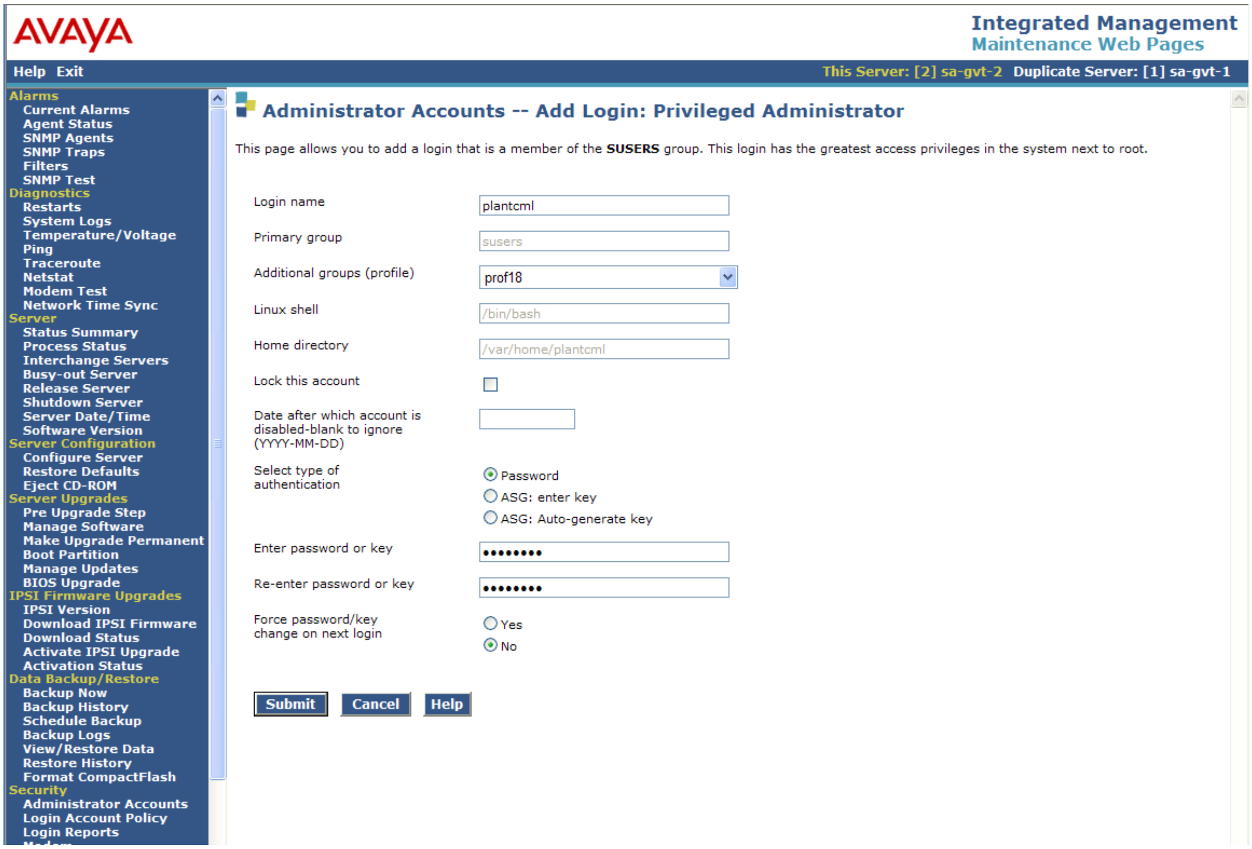
Enter **change system-parameter features** and select "silence" for Station Tone Forward Disconnect (on page 10).

```
change system-parameters features                               Page  10 of  17
                        FEATURE-RELATED SYSTEM PARAMETERS

                Pull Transfer: n            Update Transferred Ring Pattern? n
        Outpulse Without Tone? y              Wait Answer Supervision Timer? n
        Misoperation Alerting? n               Repetitive Call Waiting Tone? n
   Allow Conference via Flash? y
 Vector Disconnect Timer (min):        Network Feedback During Tone Detection? y
   Hear Zip Tone Following VOA? y    System Updates Time On Station Displays? n

                    Station Tone Forward Disconnect: silence
                            Level Of Tone Detection: precise
         Charge Display Update Frequency (seconds): 30
                            Date Format on Terminals: mm/dd/yy
                         Onhook Dialing on Terminals? n
```

4.13. Create Login for PlantCML

Launch the Maintenance web interface from Avaya Communication Manager. Click the **Administrator Accounts** option under Security on the left half of the screen. On the screen that appears, select the **Add Login** action and the **Privileged Administrator** radio button (not shown).

On the **Administrator Accounts – Add Login screen**, enter the **Login name** and **password** that will be used by the PlantCML Sentinel Application to log into Avaya Communication Manager. The Login and password will be used in **Section 6.3**. Click **Submit**.



Administrator Accounts -- Add Login: Privileged Administrator

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

Login name	plantcml
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/plantcml
Lock this account	□
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	● Password ○ ASG: enter key ○ ASG: Auto-generate key
Enter password or key	••••••••
Re-enter password or key	••••••••
Force password/key change on next login	○ Yes ● No

5. Configure Avaya Application Enablement Services

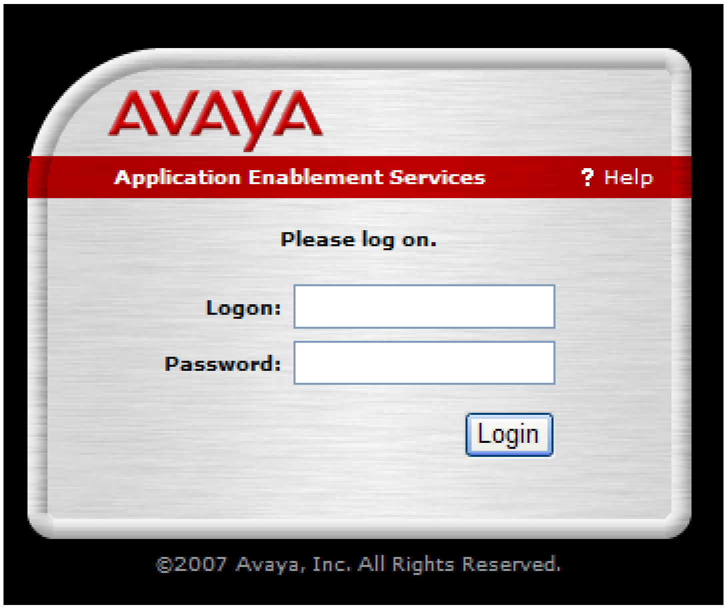
This section provides the procedures for configuring Avaya Application Enablement Services. The procedures include the following areas:

- Verify Avaya Application Enablement Services License
- Administer local IP
- Administer switch connection
- Administer TSAPI link
- Administer security database
- Obtain Tlink name
- Administer Sentinel users
- Administer device groups
- Restart TSAPI service

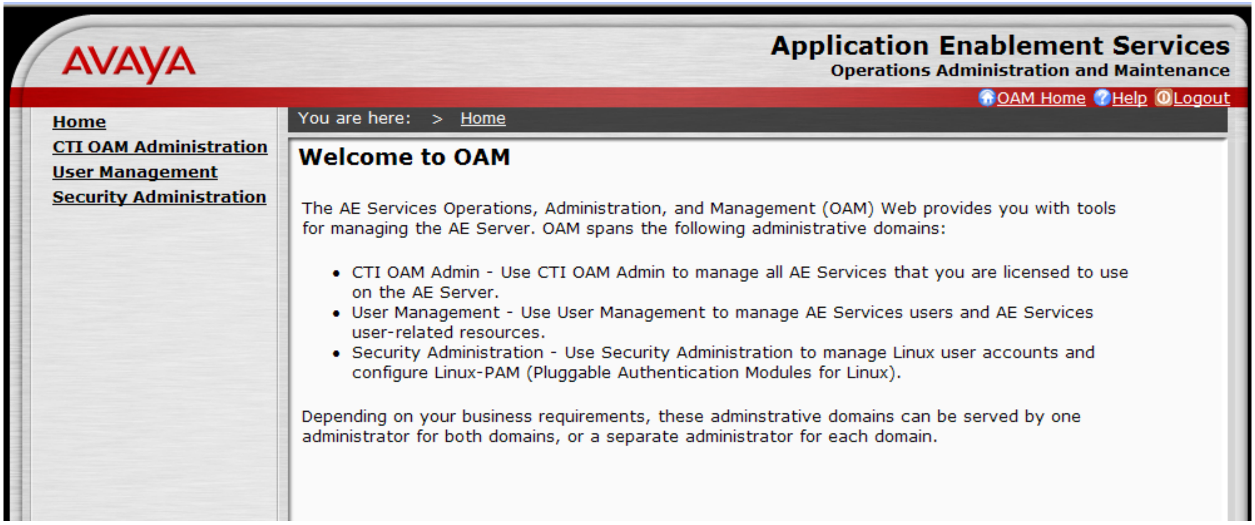
As described in **Section 1.2** and shown in **Figure 2**, two AES servers need to be administered. Administration Steps described in **Section 5.1 to Section 5.9** should be followed for both AES servers. Additional steps will be required for the AES located at the PSAP Remote Site and these will be described in Section 5.10.

5.1. Verify Avaya Application Enablement Services License

Access the AES OAM web based interface by using the URL "https://ip-address:8443/MVAP" in an Internet browser window, where "ip-address" is the IP address of the AES server. The **Login** screen is displayed as shown below. Note that the AES OAM includes two separate administrative accounts, one to access CTI OAM Admin and a separate one to access User Management. Log in using the CTI OAM Admin user name and password.


AVAYA
Application Enablement Services
? Help
Please log on.
Logon:
Password:
Login
©2007 Avaya, Inc. All Rights Reserved.

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



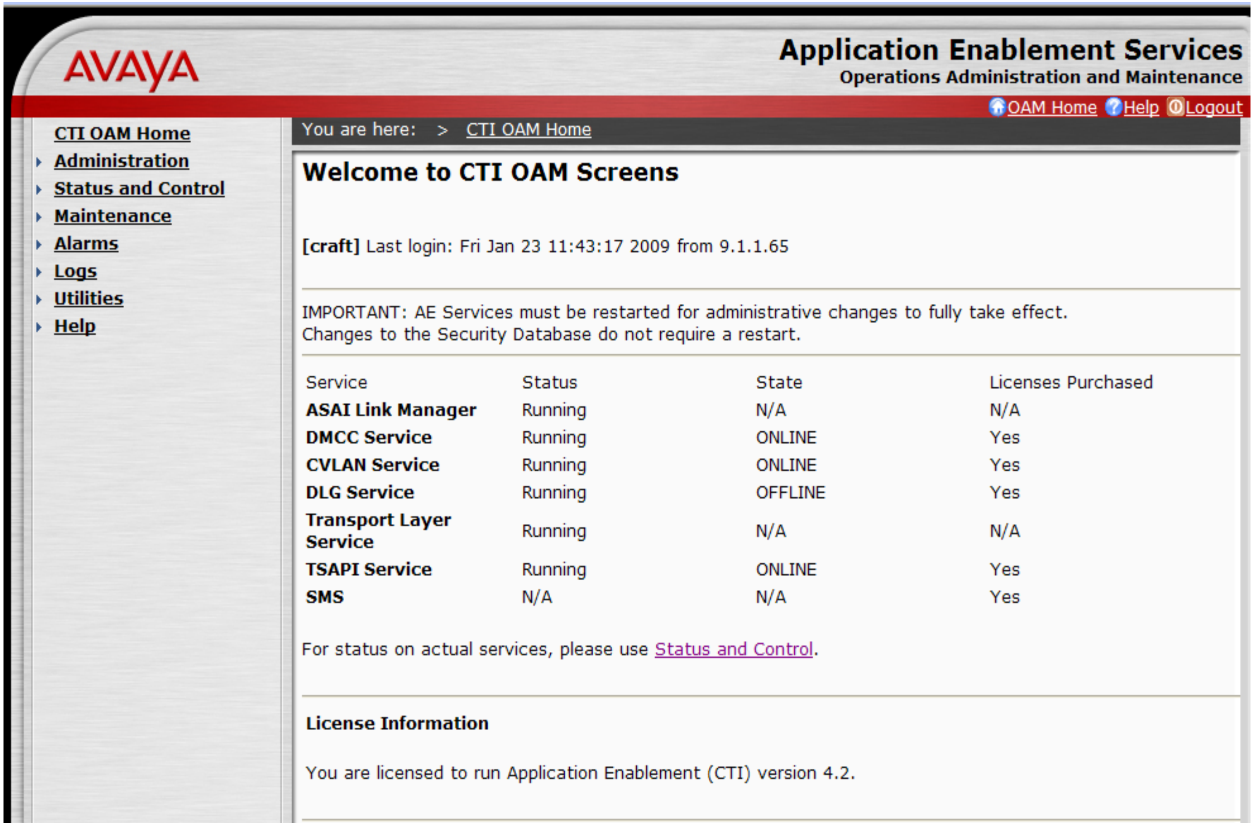
Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Security Administration - Use Security Administration to manage Linux user accounts and configure Linux-PAM (Pluggable Authentication Modules for Linux).

Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

The **Welcome to CTI OAM Screens** is displayed. Verify that AES is licensed for the TSAPI service, as shown below. If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.



Welcome to CTI OAM Screens

[craft] Last login: Fri Jan 23 11:43:17 2009 from 9.1.1.65

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	Licenses Purchased
ASAI Link Manager	Running	N/A	N/A
DMCC Service	Running	ONLINE	Yes
CVLAN Service	Running	ONLINE	Yes
DLG Service	Running	OFFLINE	Yes
Transport Layer Service	Running	N/A	N/A
TSAPI Service	Running	ONLINE	Yes
SMS	N/A	N/A	Yes

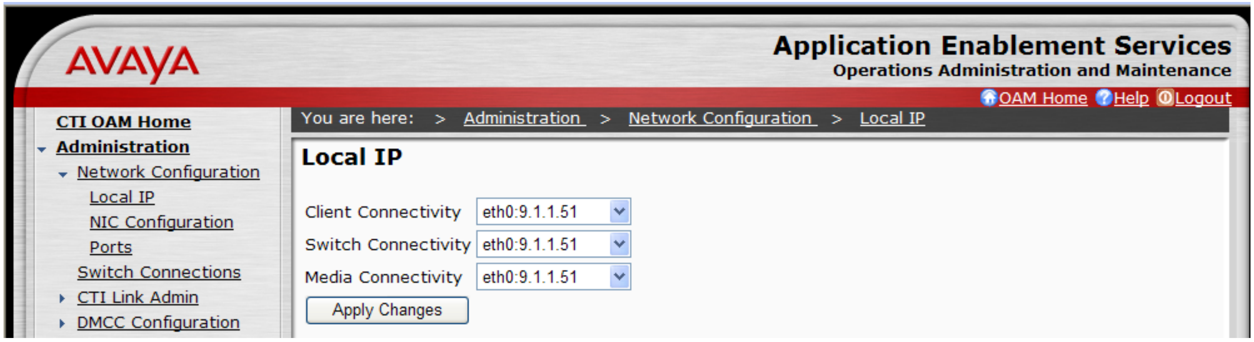
For status on actual services, please use Status and Control.

License Information

You are licensed to run Application Enablement (CTI) version 4.2.

5.2. Administer Local IP

Select **Administration > Network Configuration > Local IP** from the left pane. The **Local IP** screen is displayed into the right pane, as shown below. In the **Client Connectivity** field, select the AES server IP address that will be used to interface to Sentinel server and Sentinel 9-1-1 clients. In the **Switch Connectivity** field, select the AES server IP address that will be used to connect to Avaya Communication Manager. In the sample configuration, the same NIC interface is used for the Client Connectivity and Switch Connectivity. Note that in some cases, they might be different. Click on **Apply Changes**.

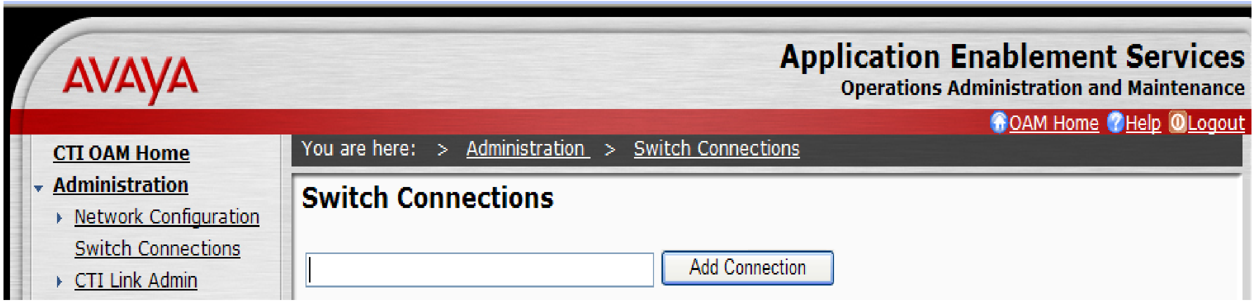


Local IP

Client Connectivity: eth0:9.1.1.51
Switch Connectivity: eth0:9.1.1.51
Media Connectivity: eth0:9.1.1.51

5.3. Administer Switch Connection

Select **Administration > Switch Connections** from the left pane. The **Switch Connections** screen is displayed, as shown below. Enter a descriptive name for the switch connection and click on **Add Connection**. In this case, "govaes2" is used. Note that the actual switch connection name may vary.

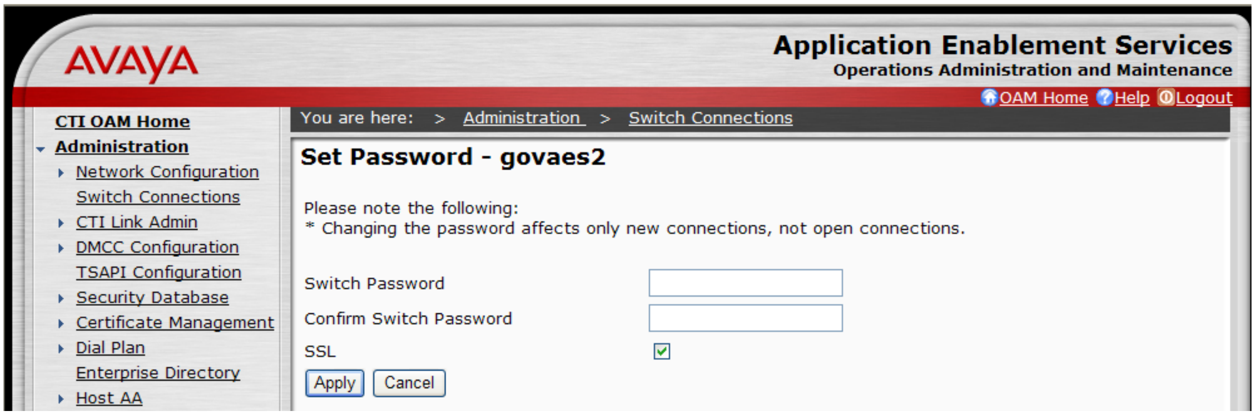

AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
CTI OAM Home
Administration
Network Configuration
Switch Connections
CTI Link Admin
You are here: > Administration > Switch Connections
Add Connection

Switch Connections

Next, the **Set Password – govaes2** screen is displayed. Enter the following values for the specified fields:

- **Switch Password:** Same password from **Section 4.3**.
- **Confirm Switch Password:** Re-enter the same password from **Section 4.3**.
- **SSL:** Retain the check.

Click on **Apply**.



Set Password - govaes2

Please note the following:
* Changing the password affects only new connections, not open connections.

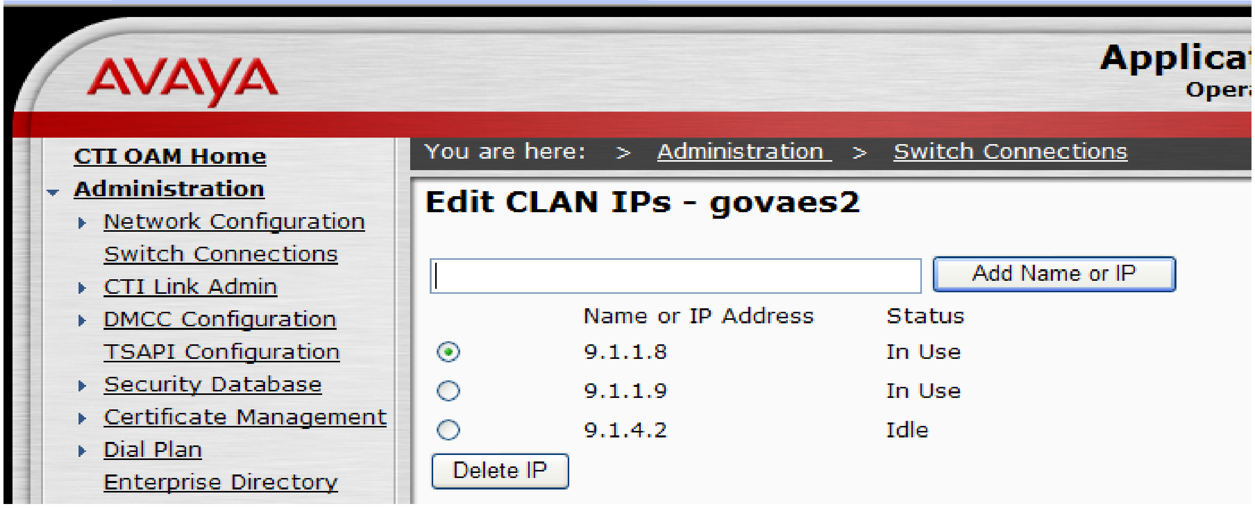
Switch Password	
Confirm Switch Password	
SSL	☑

The **Switch Connections** screen is displayed next (not shown). Select the newly added switch connection name from the listing, and click on **Edit CLAN IPs**.

The **Edit CLAN IPs – govaes2** screen is displayed next.

- Enter the host name or IP address of the C-LAN used for AES connectivity from **Section 4.2**. Click on **Add Name or IP**.
- Enter the host name or IP address of the S8300 Media Server from **Section 4.2**. Click on **Add Name or IP**.

The updated screen with administered CLANs is shown below.

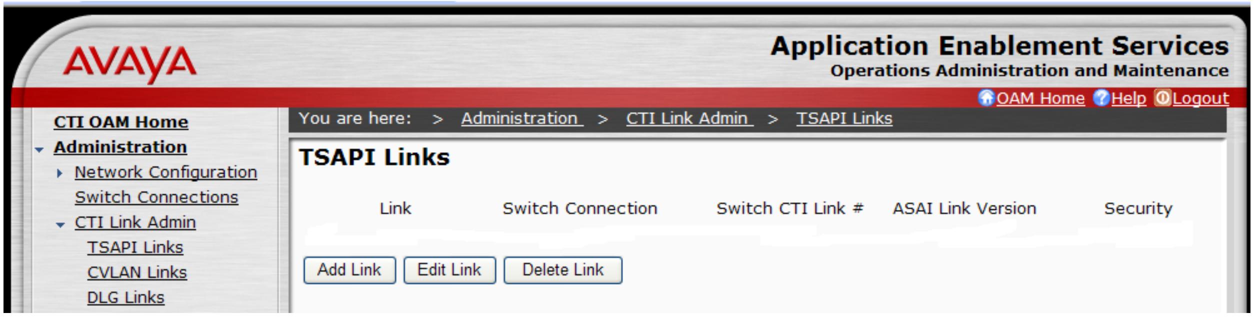


Edit CLAN IPs - govaes2

	Name or IP Address	Status
●	9.1.1.8	In Use
○	9.1.1.9	In Use
○	9.1.4.2	Idle

5.4. Administer TSAPI Link

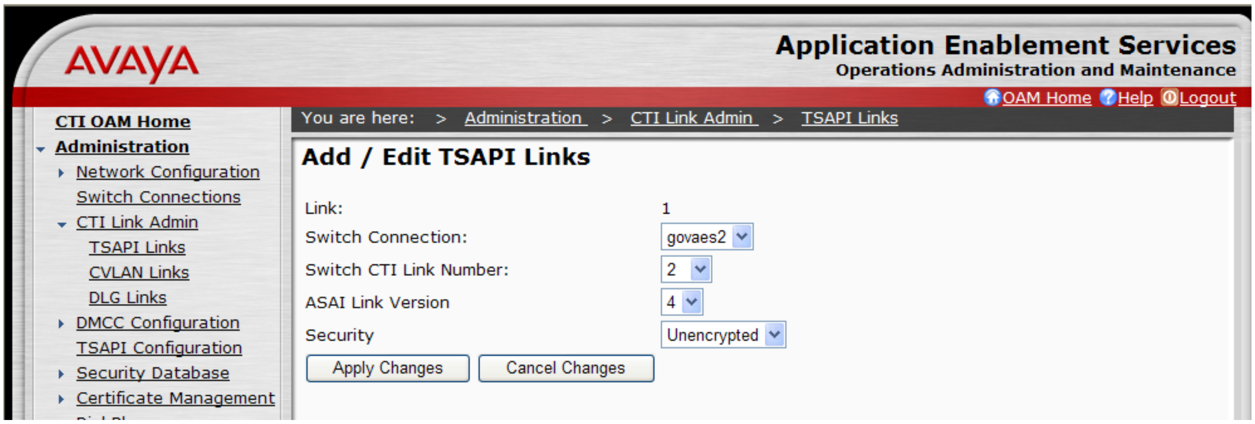
To administer a TSAPI link, select **Administration > CTI Link Admin > TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click on **Add Link**.



TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add / Edit 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 name of the switch connection from **Section 5.3**. For **Switch CTI Link Number**, select the CTI link number from **Section 4.4**. Accept the default values for **ASAI Link Version** and **Security**. Click on **Apply Changes**.



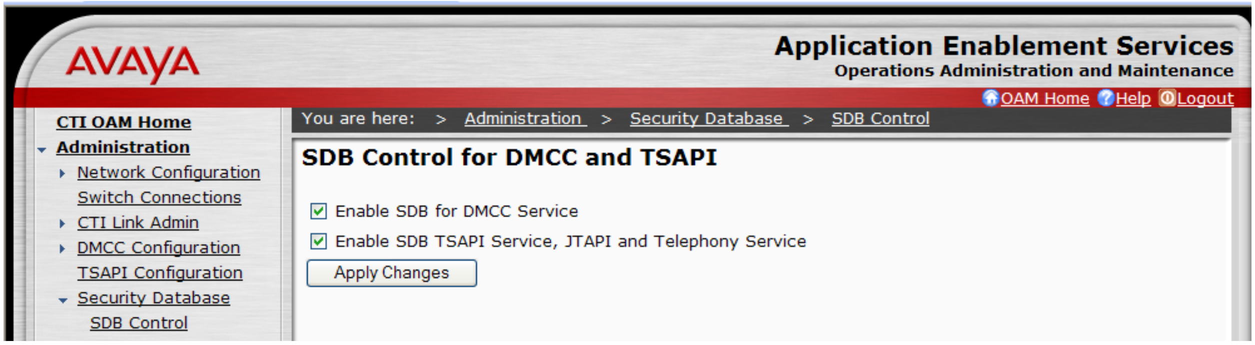
Add / Edit TSAPI Links

Link:	1
Switch Connection:	govaes2
Switch CTI Link Number:	2
ASAI Link Version	4
Security	Unencrypted

The **Apply Changes to Link** screen is displayed (not shown). Click on **Apply**.

5.5. Administer Security Database

Enable the security database on AES, as this functionality is utilized by Sentinel. Select **Administration > Security Database > SDB Control** to display the **SDB Control for DMCC and TSAPI** screen shown below. Click on **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony Service**. Click on **Apply Changes**.



SDB Control for DMCC and TSAPI

☑ Enable SDB for DMCC Service

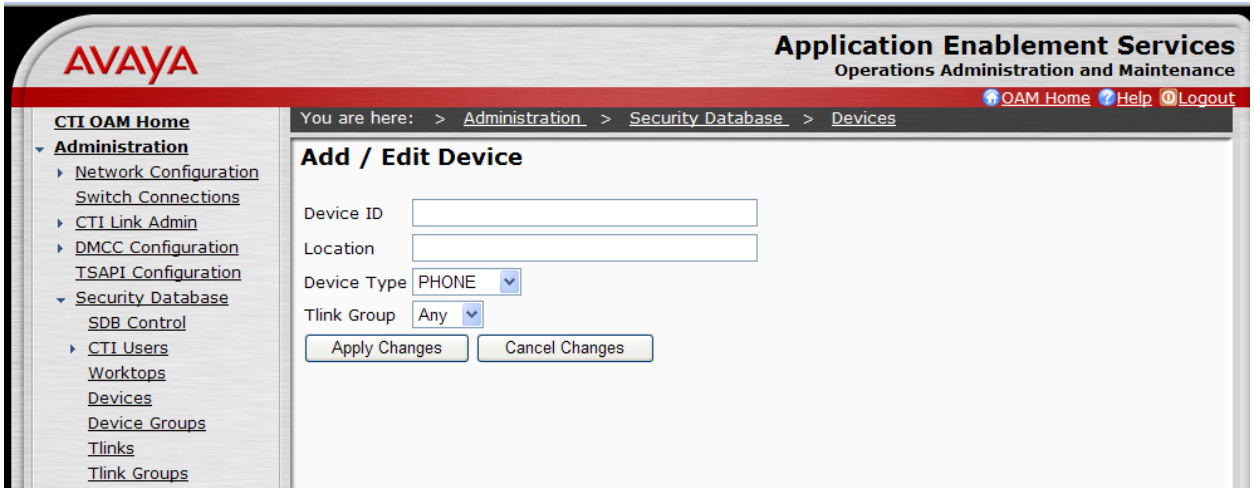
☑ Enable SDB TSAPI Service, JTAPI and Telephony Service

Apply Changes

All devices that are monitored and controlled by Sentinel need to be configured in the AES security database. Select **Administration > Security Database > Devices**, and add each device by entering the device extension and clicking on **Add Device** (not shown).

The **Add / Edit Device** screen is used to enter the associated field values for each device, as shown below. The following is a description of the device types that are monitored by Sentinel:

- **PHONE:** Station extensions.
- **VDN:** Vector Directory Number extensions.
- **AGENT ID:** Logical agent extensions.



Add / Edit Device

Device ID

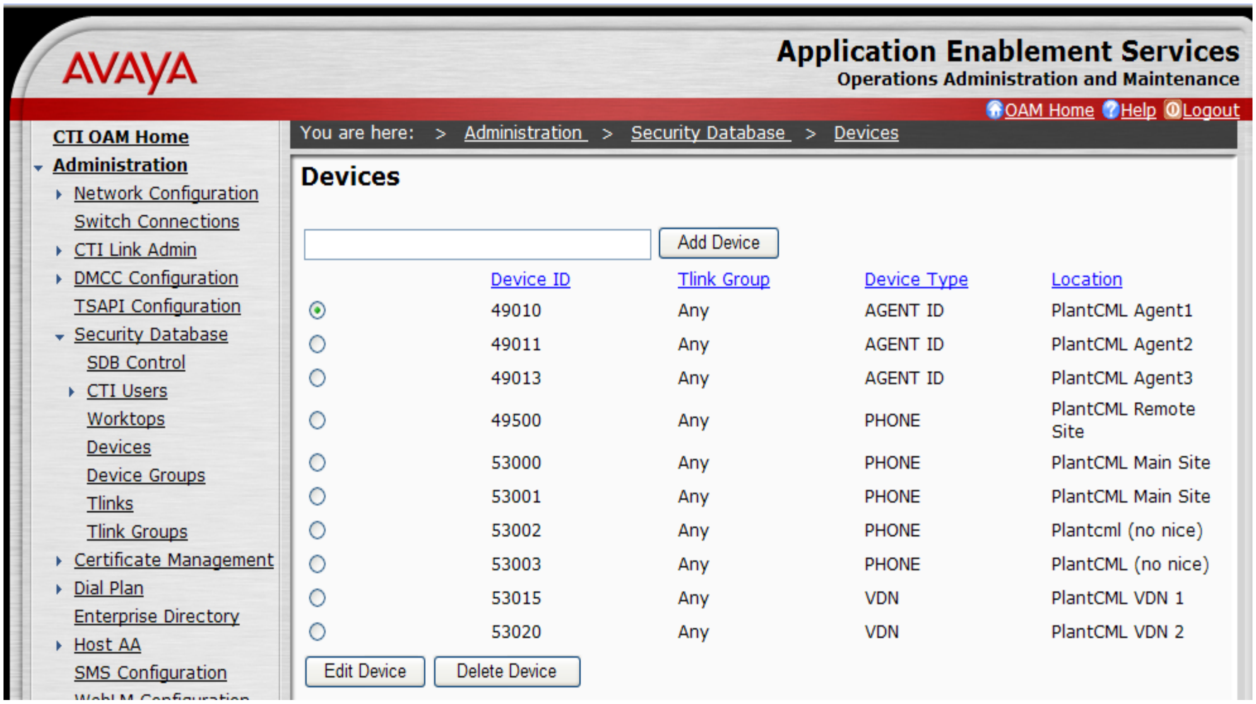
Location

Device Type PHONE

Tlink Group Any

Apply Changes Cancel Changes

A sample listing of the configured devices used for the compliance testing is shown below. Note that the total number of devices may vary, as this depends on the number of extensions to be monitored and controlled.

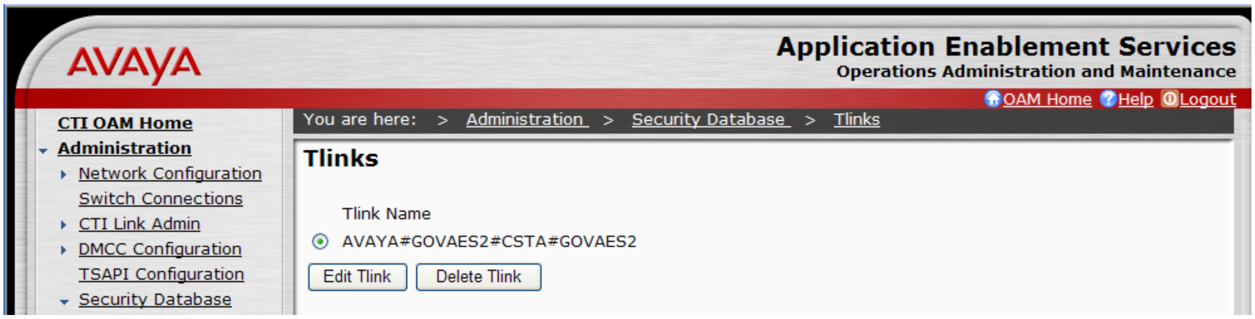


Devices

	Device ID	Tlink Group	Device Type	Location
●	49010	Any	AGENT ID	PlantCML Agent1
○	49011	Any	AGENT ID	PlantCML Agent2
○	49013	Any	AGENT ID	PlantCML Agent3
○	49500	Any	PHONE	PlantCML Remote Site
○	53000	Any	PHONE	PlantCML Main Site
○	53001	Any	PHONE	PlantCML Main Site
○	53002	Any	PHONE	Plantcml (no nice)
○	53003	Any	PHONE	PlantCML (no nice)
○	53015	Any	VDN	PlantCML VDN 1
○	53020	Any	VDN	PlantCML VDN 2

5.6. Obtain Tlink Name

Select **Administration > Security Database > Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated by the AES server, upon creation of a new switch connection. Locate the Tlink Name associated with the newly created switch connection, which would utilize the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring the Sentinel server.



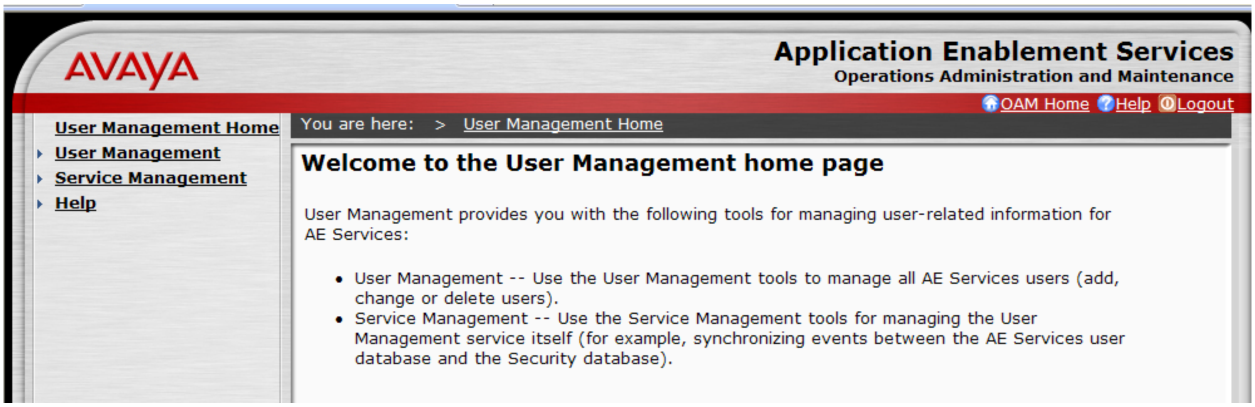
Tlinks

Tlink Name

● AVAYA#GOVAES2#CSTA#GOVAES2

5.7. Administer Sentinel Users

Administer a user account for the Sentinel servers and a user account for each Sentinel 9-1-1 client/agent. Follow the login procedures in **Section 5.1**, and log in with the User Management user name and password. The **Welcome to the User Management home page** screen is displayed, as shown below.


AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
User Management Home
User Management
Service Management
Help
You are here: > User Management Home

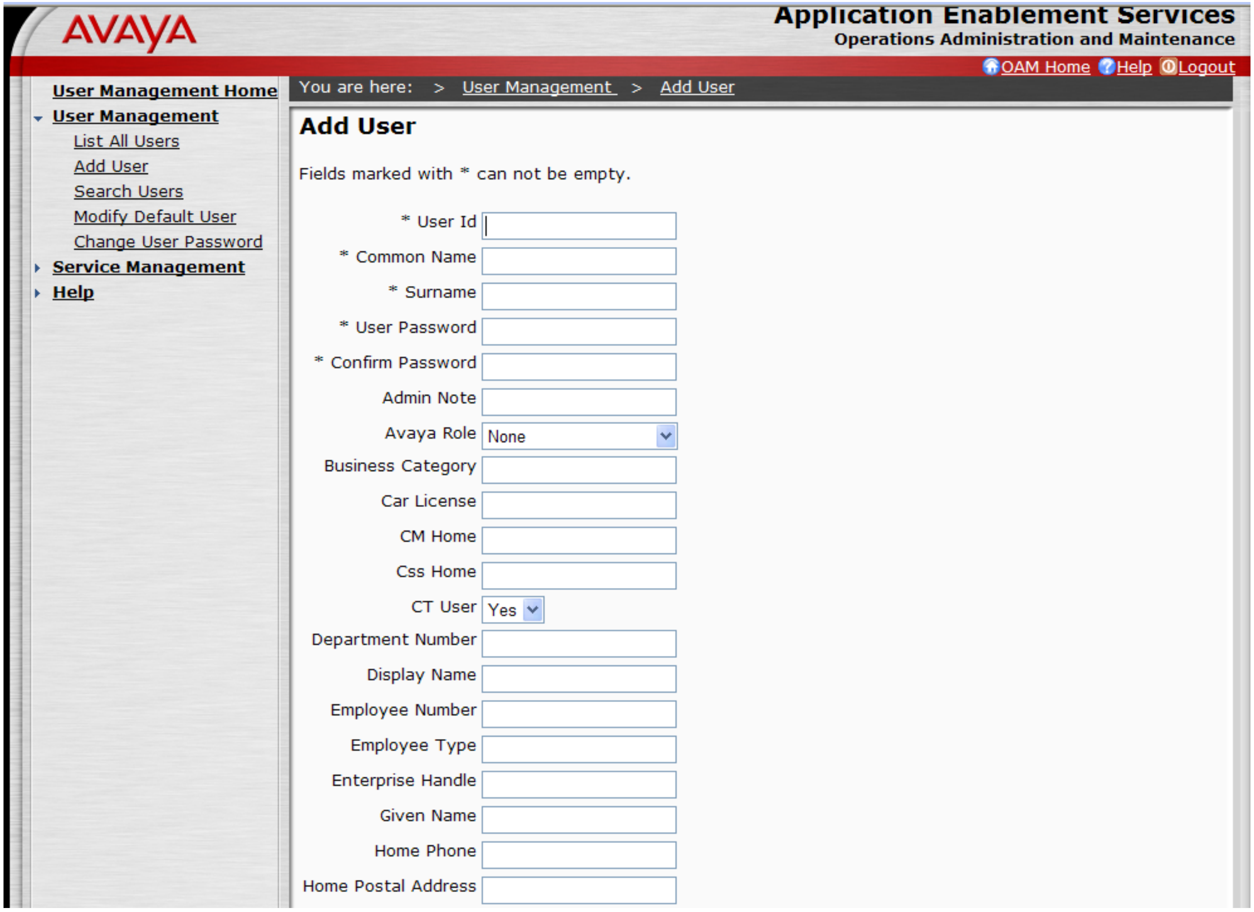
Welcome to the User Management home page

User Management provides you with the following tools for managing user-related information for AE Services:

- User Management -- Use the User Management tools to manage all AE Services users (add, change or delete users).
- Service Management -- Use the Service Management tools for managing the User Management service itself (for example, synchronizing events between the AE Services user database and the Security database).

Select **User Management > Add User** from the left pane. In the **Add User** screen shown below, enter values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields to create a user account for the Sentinel server. 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).

Note: The User Password must be a superset of the Agent ID password to meet the new AES requirements for password. For example, if the Agent ID password is "1234" then the AES User password could be “1234!QZA"



Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role None

Business Category

Car License

CM Home

Css Home

CT User Yes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

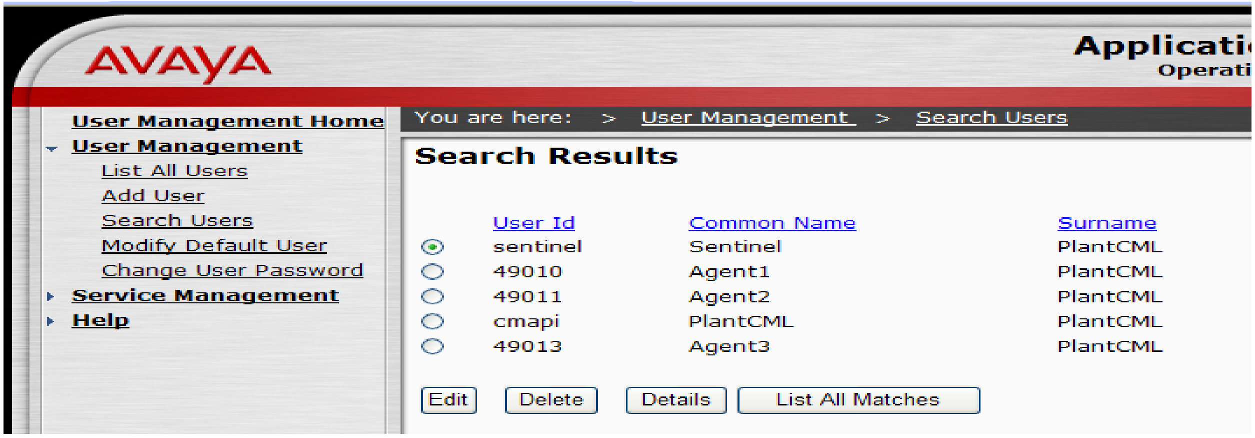
Given Name

Home Phone

Home Postal Address

Repeat this procedure to create a user account for each Sentinel 9-1-1 client/agent, using the Agent-ID and Password from **Section 4.11** as **User Id** and **User Password**. For the sample configuration, two user accounts will be created.

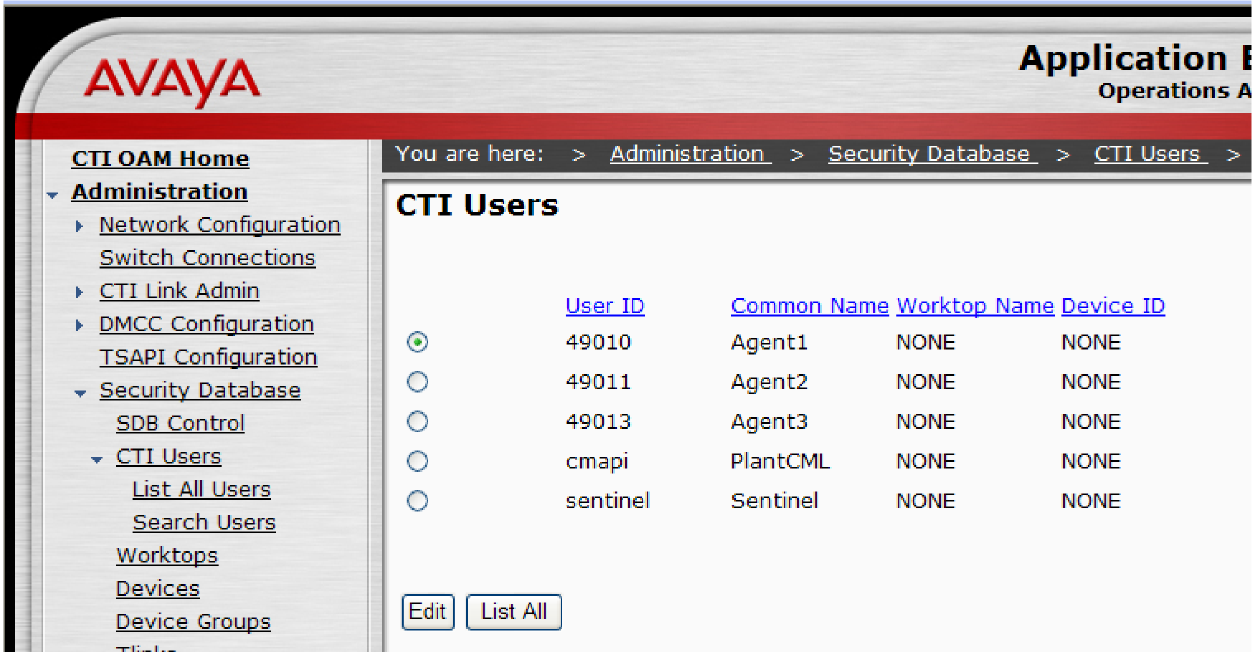
In addition to Sentinel 9-1-1 clients/agents, two additional user accounts need to be created. These are **cmapi** and **sentinel.** These user accounts will be used in **Section 6.3.** All the administered user accounts created for PlantCML Sentinel application are shown below:



Search Results

	User Id	Common Name	Surname
●	sentinel	Sentinel	PlantCML
○	49010	Agent1	PlantCML
○	49011	Agent2	PlantCML
○	cmapi	PlantCML	PlantCML
○	49013	Agent3	PlantCML

Follow the login procedures in **Section 5.1**, and log in with the CTI OAM Admin user name and password. Select **Administration > Security Database > CTI Users > List All Users** to get a listing of all CTI users, as shown below.

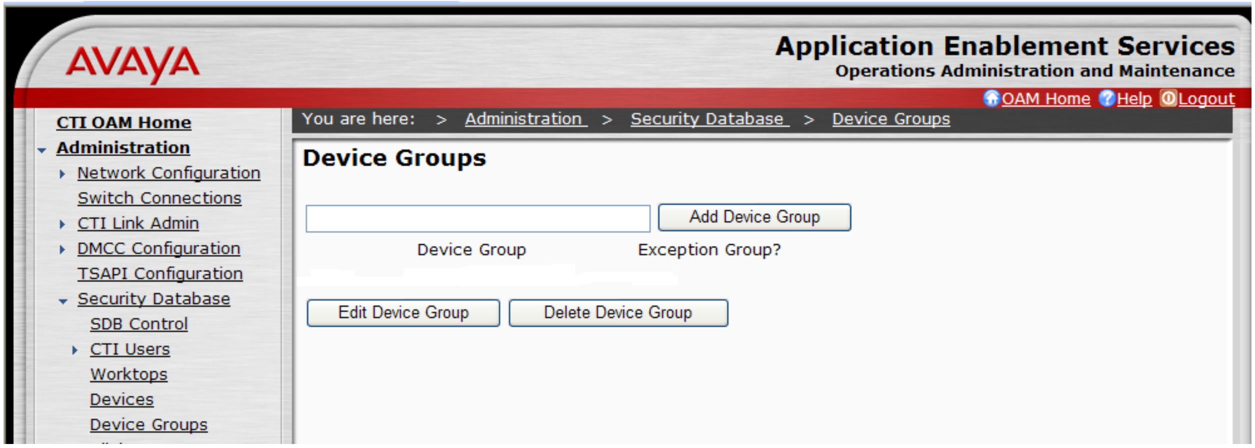


CTI Users

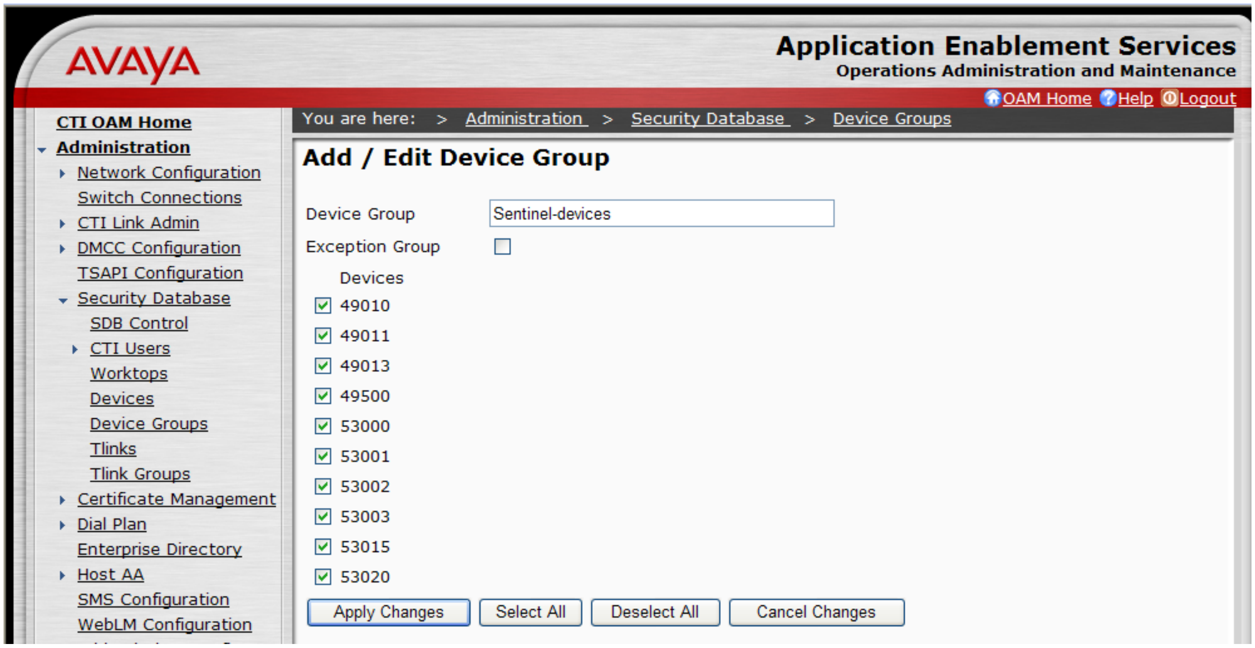
	User ID	Common Name	Worktop Name	Device ID
●	49010	Agent1	NONE	NONE
○	49011	Agent2	NONE	NONE
○	49013	Agent3	NONE	NONE
○	cmapi	PlantCML	NONE	NONE
○	sentinel	Sentinel	NONE	NONE

5.8. Administer Device Groups

Administer a device group to be used by Sentinel, to control user access of devices. Select **Administration > Security Database > Device Groups** from the left pane. In the **Device Groups** screen shown below, enter a descriptive value, and click on **Add Device Group**.



For the sample configuration, a device group of "Sentinel-devices" was created. Click on **Edit Device Group**. The **Add / Edit Device Group** screen is displayed, as shown below. Select all devices that were created in **Section 5.5**, and click on **Apply Changes**.



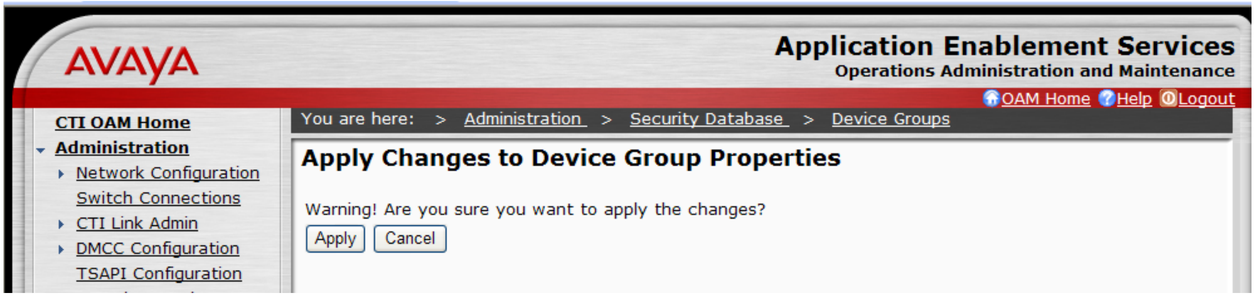
Device Group: Sentinel-devices

Exception Group ☐

Devices

☑ 49010
☑ 49011
☑ 49013
☑ 49500
☑ 53000
☑ 53001
☑ 53002
☑ 53003
☑ 53015
☑ 53020

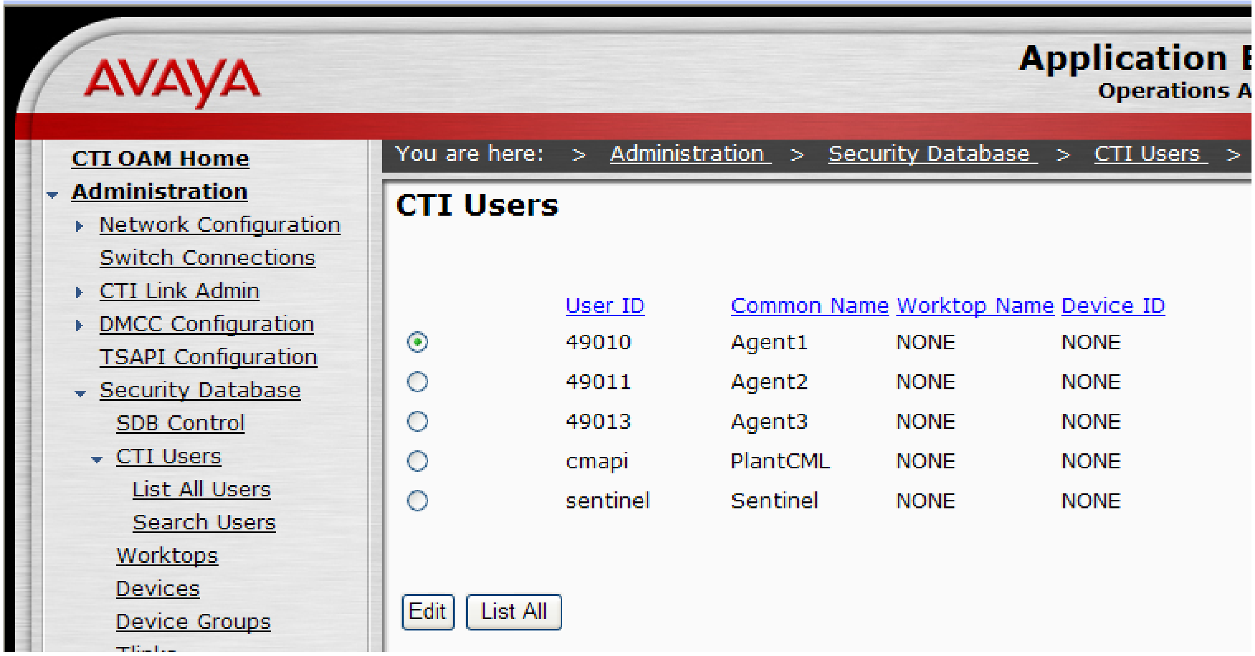
The **Apply Changes to Device Group Properties** screen is displayed next. Click on **Apply** to confirm the changes.



Apply Changes to Device Group Properties

Warning! Are you sure you want to apply the changes?

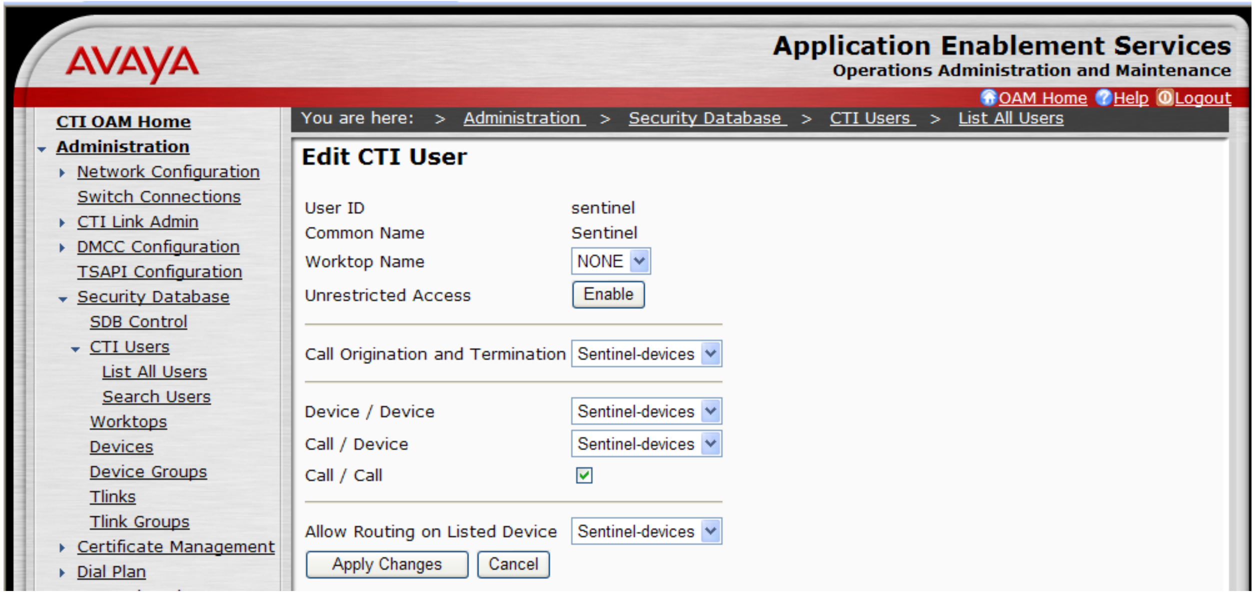
Select **Administration > Security Database > CTI Users > List All Users** to view the listing of all CTI users again, as shown below. Select the user ID created for the Sentinel server, and click on **Edit**. In this case, "sentinel".



CTI Users

	User ID	Common Name	Worktop Name	Device ID
●	49010	Agent1	NONE	NONE
○	49011	Agent2	NONE	NONE
○	49013	Agent3	NONE	NONE
○	cmapi	PlantCML	NONE	NONE
○	sentinel	Sentinel	NONE	NONE

The **Edit CTI User** screen is displayed, as shown below. Select the newly created device group for the **Call Origination and Termination**, **Device / Device**, **Call / Device**, and **Allow Routing on Listed Device** fields. Click on **Call / Call**, followed by **Apply Changes**.



Edit CTI User

User ID: sentinel
Common Name: Sentinel
Worktop Name: NONE
Unrestricted Access: Enable

Call Origination and Termination: Sentinel-devices

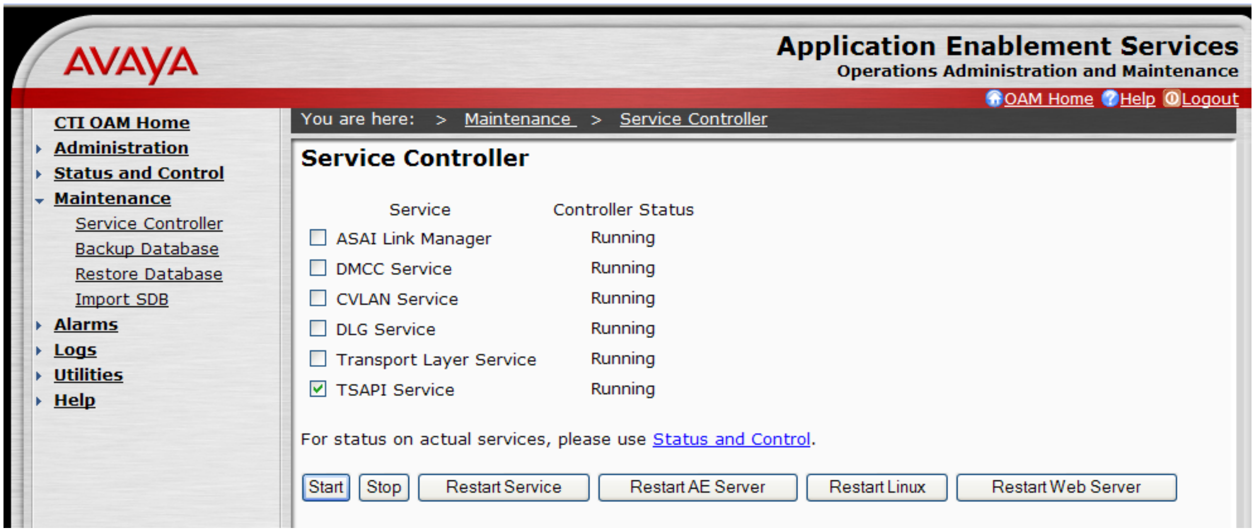
Device / Device: Sentinel-devices
Call / Device: Sentinel-devices
Call / Call: ☑

Allow Routing on Listed Device: Sentinel-devices

Repeat this procedure for all CTI users listed in the **CTI Users** screen above – “49010”, “49011” “49013” and “cmapi”.

5.9. Restart TSAPI Service

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

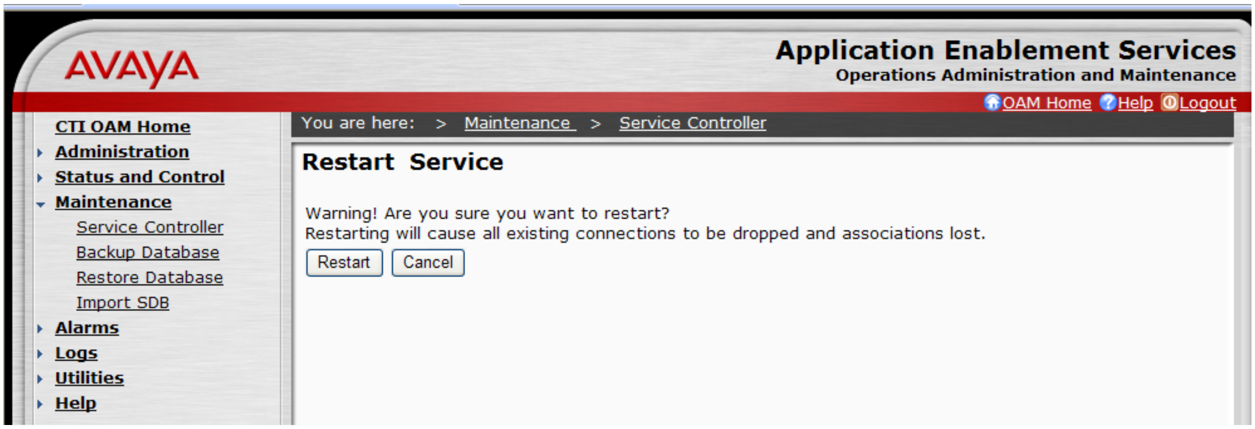


Service Controller

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.

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



Restart Service

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

5.10. Administer AES Server for the LSP Configuration

As described in **Section 1.5** and shown in **Figure 4**, two AES servers need to be administered. Repeat steps described in **Section 5.1 to Section 5.9** to configure the second AES server located at the PSAP Remote Site.

6. Configure PlantCML Sentinel Server

This section provides the procedures for configuring the PlantCML Sentinel CM servers. The procedures include the following areas:

- Administer Sentinel Server Configuration
- Launch Sentinel server configurator
- Administer global settings
- Restart CallP Manager
- Administer Sentinel clients
- Verify Sentinel Accounts
- Administer trunks

This section assumes that Sentinel CM software has already been installed on the two servers.

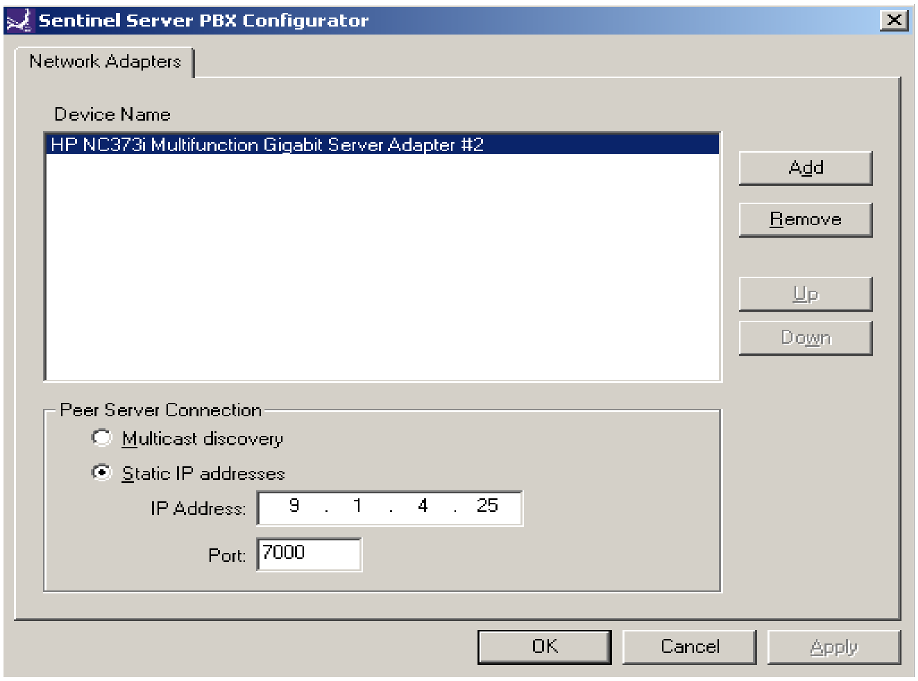
For the sample configuration, use the following in the **Name** and **IP Address**. The actual name and IP address may vary.

Sentinel CM Servers		
Name	**IP Address**	**Location**
Server-A	9.1.1.26	Main PSAP Site
Server-B	9.1.4.25	Remote PSAP Site

6.1. Administer Sentinel Server Configuration

On the sentinel server located at the Main PSAP Site (on Server-A), select **Start → Control Panel**. Double click on the **Sentinel Server** icon. The **Sentinel Server PBX Configurator** screen will appear.

- For the **Peer Server Connection**, select **Static IP addresses** and enter the IP address of the sentinel server located at the Remote PSAP Site (Server-B).
- Click on **OK** at the bottom of the screen.



Sentinel Server PBX Configurator

Network Adapters

Device Name

HP NC373i Multifunction Gigabit Server Adapter #2

Peer Server Connection

○ Multicast discovery

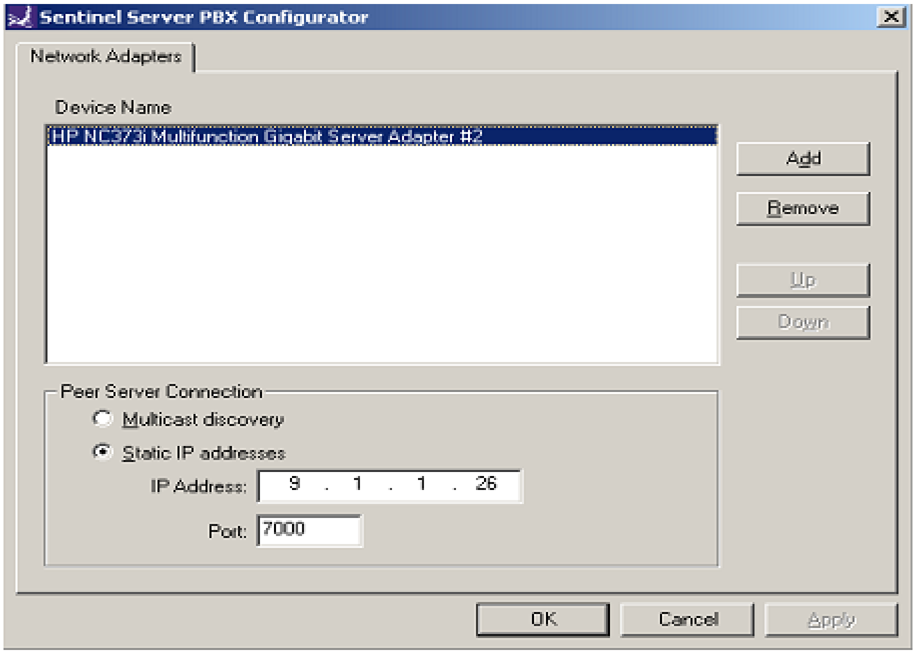
● Static IP addresses

IP Address: 9 . 1 . 4 . 25

Port: 7000

On the sentinel server located at the Remote PSAP Site (on Server-B), select **Start → Control Panel**. Double click on the **Sentinel Server** icon. The **Sentinel Server PBX Configurator** screen will appear.

- For the **Peer Server Connection**, select **Static IP addresses** and enter the IP address of the sentinel server located at the Main PSAP Site (Server-A).
- Click on **OK** at the bottom of the screen.



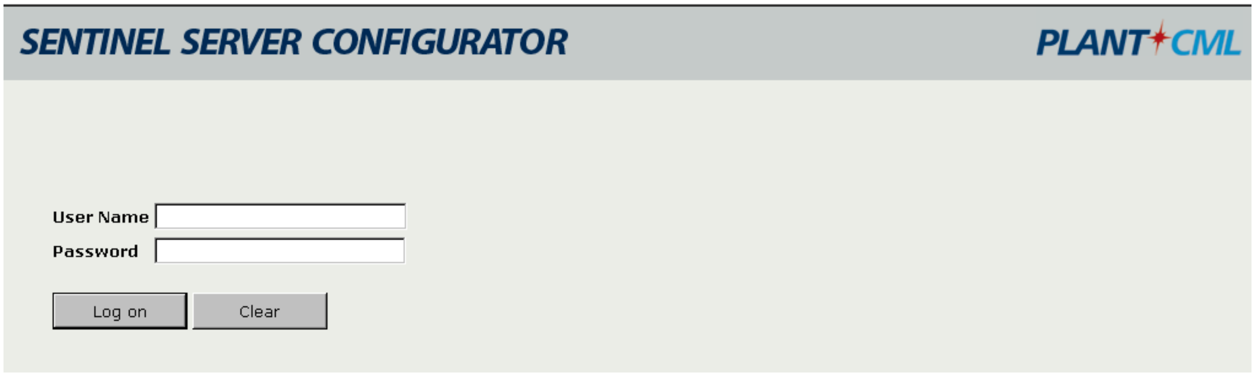
Device Name
HP NC373i Multifunction Gigabit Server Adapter #2

Peer Server Connection
○ Multicast discovery
● Static IP addresses
IP Address: 9 . 1 . 1 . 26
Port: 7000

6.2. Launch Sentinel Server Configurator

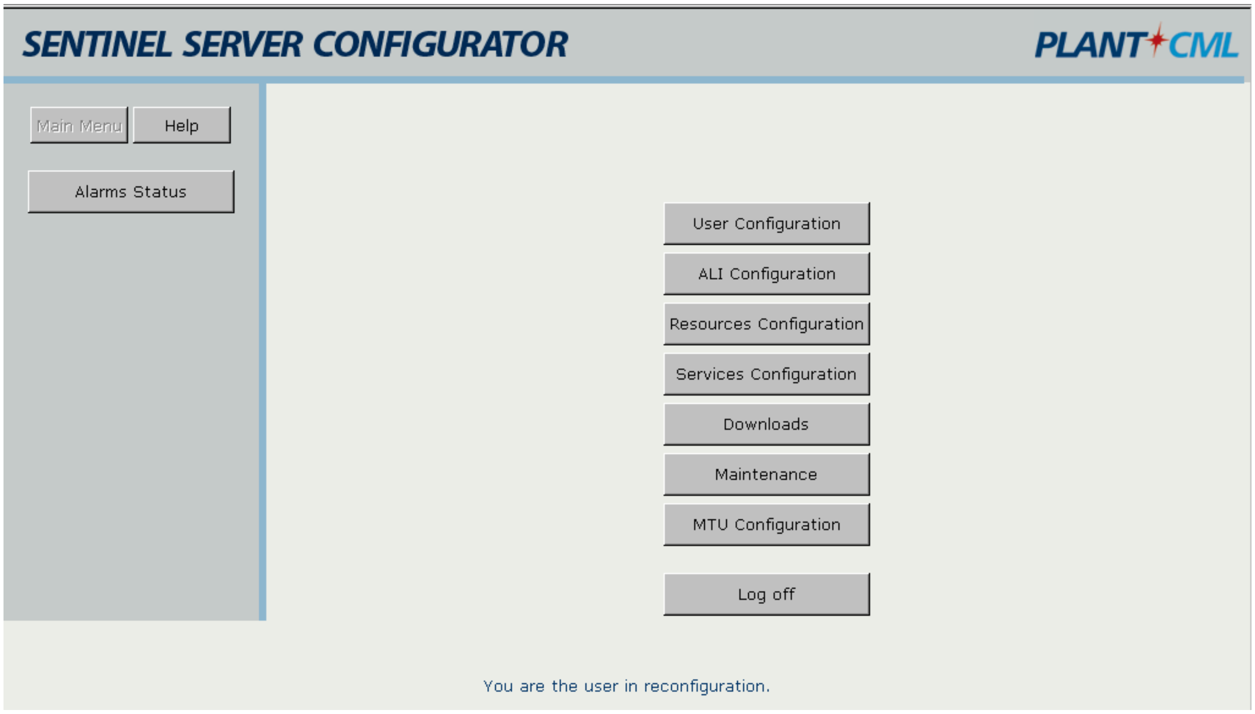
Access the Sentinel server web based interface by using the URL "http://<ip-address>/ Configurator" in an Internet browser window, where "ip-address" is the IP address of the Sentinel active server. The screen below is displayed. Log in with proper administrative credentials.

Note that the configuration steps described in **Section 6.2 to Section 6.7** are performed on the active server only. The Remote server will automatically synch up with the primary server.



6.3. Administer Global Settings

The screen below is displayed next. Click on **Resources Configuration**.



The **Global Setting Details** screen is displayed.

In the Sentinel Server section:

- Enter the **Sentinel Server A Name, Sentinel Server B Name, and Server Group**.
- Enter “0” in the Media Gateway ID field for G650 Media Gateways.
- Enter “1” in the Media Gateway ID field for G450/G350 Media Gateways.

In the Avaya Media Server section:

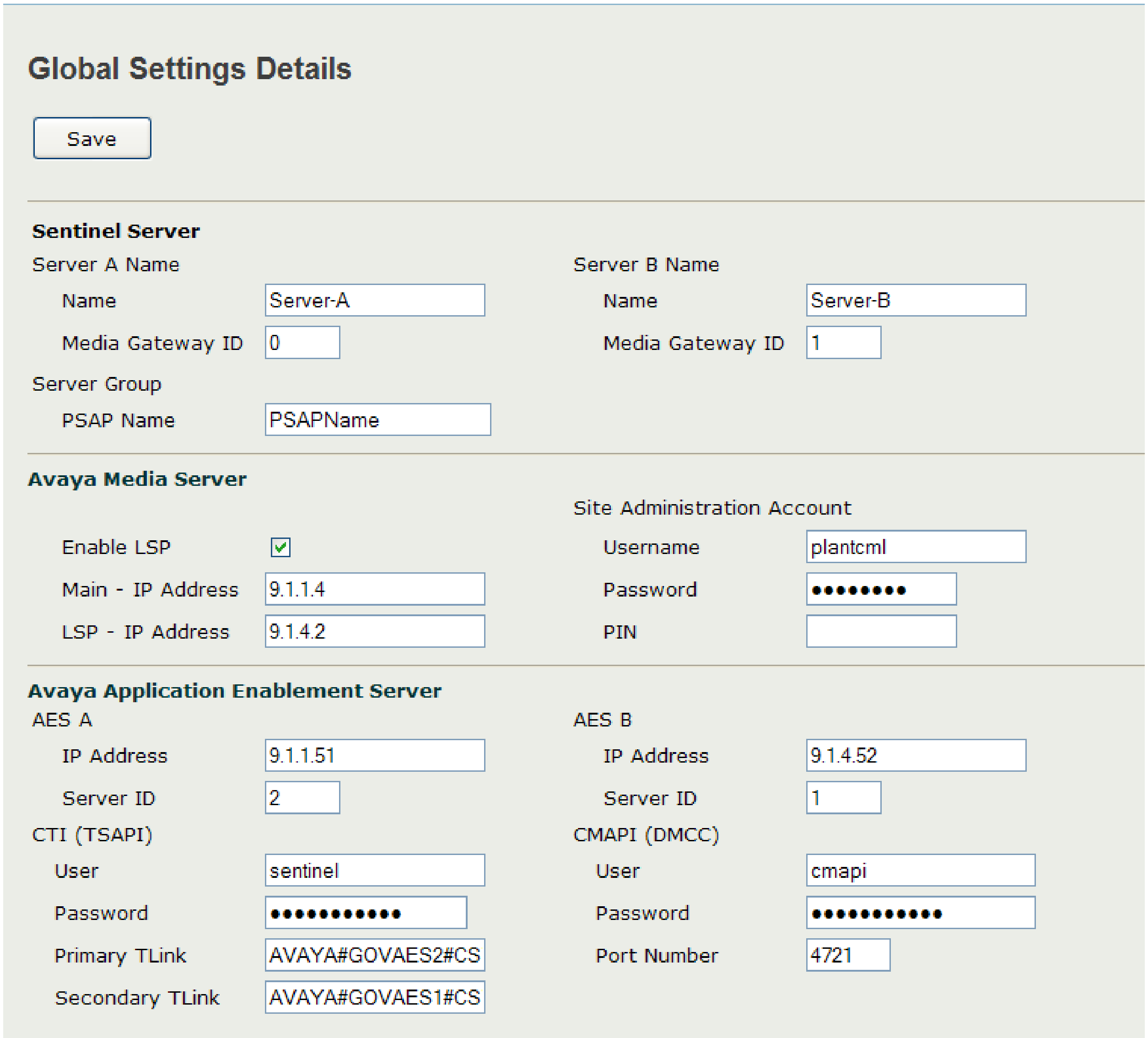
- Enter the **Avaya Communication Manager virtual IP address** in the Main – IP Address field.
- Enter the **S8300 Media Server IP address** in the LSP – IP Address field
- Check the **Enable LSP** box.
- Enter the **Username and password** created in **Section 4.13** in the Site Administration Account Username and Password fields.
- Leave PIN field blank.

In the Avaya Application Enablement Server section:

- Enter the **IP address** of the two Avaya AES servers. For the sample configuration, enter “9.1.1.51” and “9.1.1.52” (from **Section 5.2**).
- Enter the **Server ID** that corresponds to each AES server from **Section 4.5**.
- For the **CTI (TSAPI)**, enter the user ID and password created for the Sentinel servers from **Section 5.7**.
- For the **TLink** field, enter the Tlink name noted in **Section 5.6**. Two TLinks need to be entered, one for each Avaya AES server. The TLink corresponding to AES A should be listed in Primary TLink. The TLink corresponding to AES B should be listed in Secondary TLink.

- For the **CMAPI**, enter the user ID and password created in **Section 5.7**. Maintain the default value for Port Number.

The updated screen is shown below. Click on **Save** at the top of the screen to save the configuration.



Global Settings Details

Save

Sentinel Server

Server A Name		Server B Name	
Name	Server-A	Name	Server-B
Media Gateway ID	0	Media Gateway ID	1
Server Group			
PSAP Name	PSAPName		

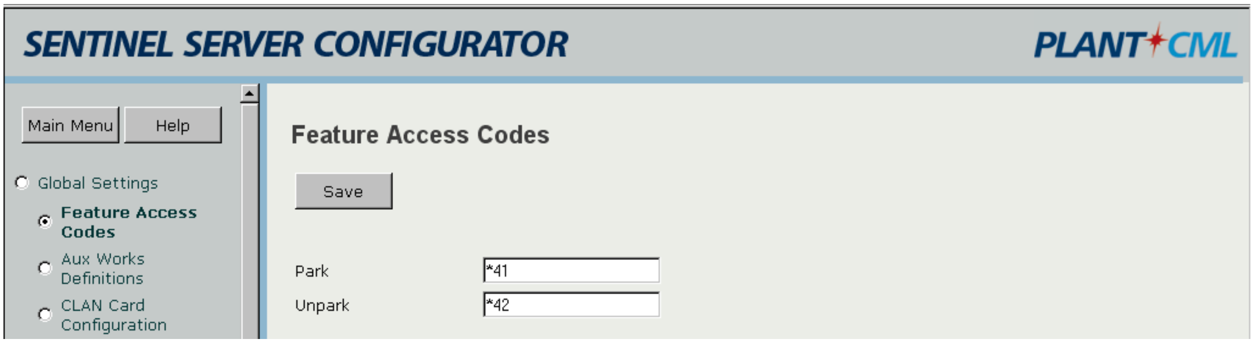
Avaya Media Server

		Site Administration Account	
Enable LSP	☑	Username	plantcml
Main - IP Address	9.1.1.4	Password	●●●●●●●●
LSP - IP Address	9.1.4.2	PIN	

Avaya Application Enablement Server

AES A		AES B	
IP Address	9.1.1.51	IP Address	9.1.4.52
Server ID	2	Server ID	1
CTI (TSAPI)		CMAPI (DMCC)	
User	sentinel	User	cmapi
Password	●●●●●●●●●●●●	Password	●●●●●●●●●●●●
Primary TLink	AVAYA#GOVAES2#CS	Port Number	4721
Secondary TLink	AVAYA#GOVAES1#CS		

Select **Feature Access Codes** in the left pane. Enter the corresponding feature access code for Call Park and Answer Back Access Code from **Section 4.7**, in **Park and Unpark** fields. Click on **Save** at the top of the screen.

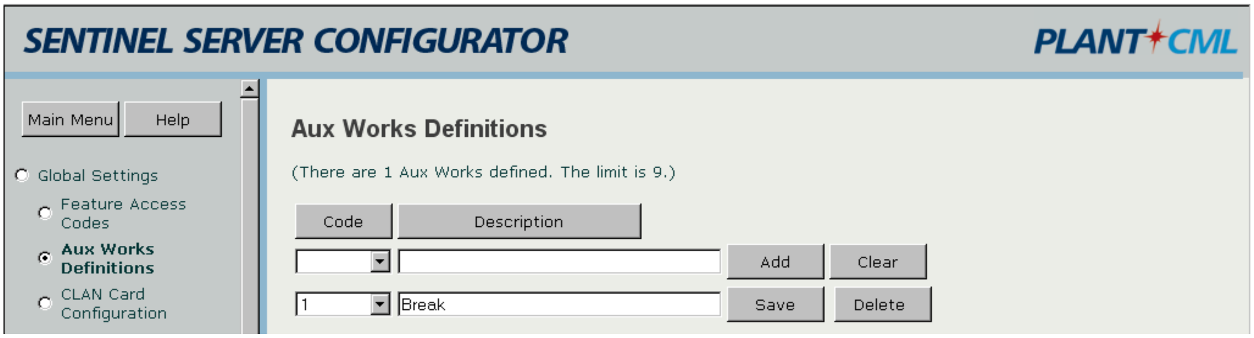


Feature Access Codes

Park: *41

Unpark: *42

Select **Aux Works Definitions** in the left pane. Enter appropriate **Code** and **Description**. Click on **Add**.



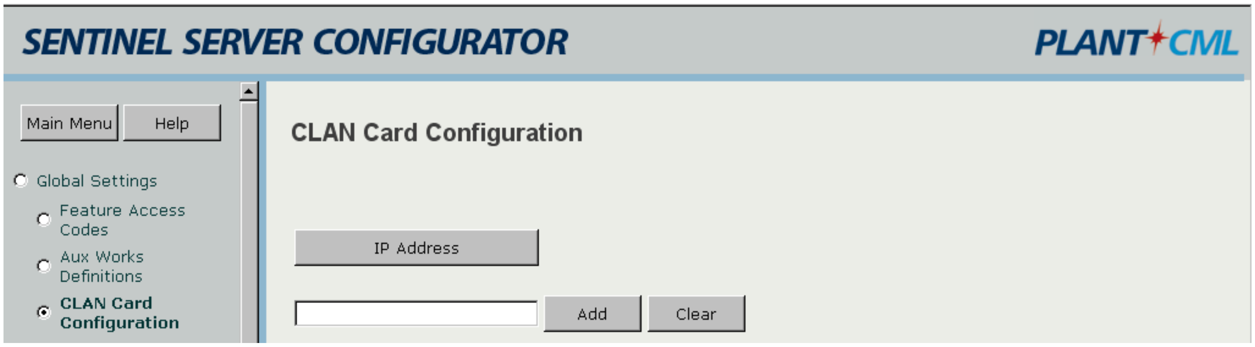
Aux Works Definitions

(There are 1 Aux Works defined. The limit is 9.)

Code	Description
1	Break

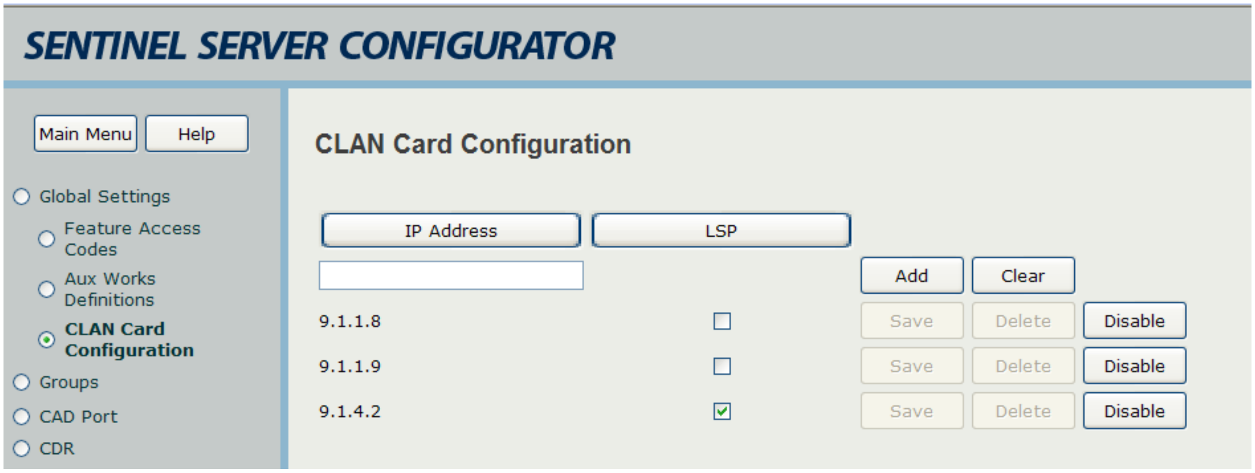
Select **CLAN Card Configuration** in the left pane.

- Enter the IP address for the C-LAN module (from **Section 4.2**). Click on **Add**.
- Enter the IP address of the S8300 Media Server (from **Section 4.2**). Click on **Add.**
- Enable LSP box for S8300 Media Server. Click on **Save.**



CLAN Card Configuration

The screen below displays the CLAN Card Configuration.

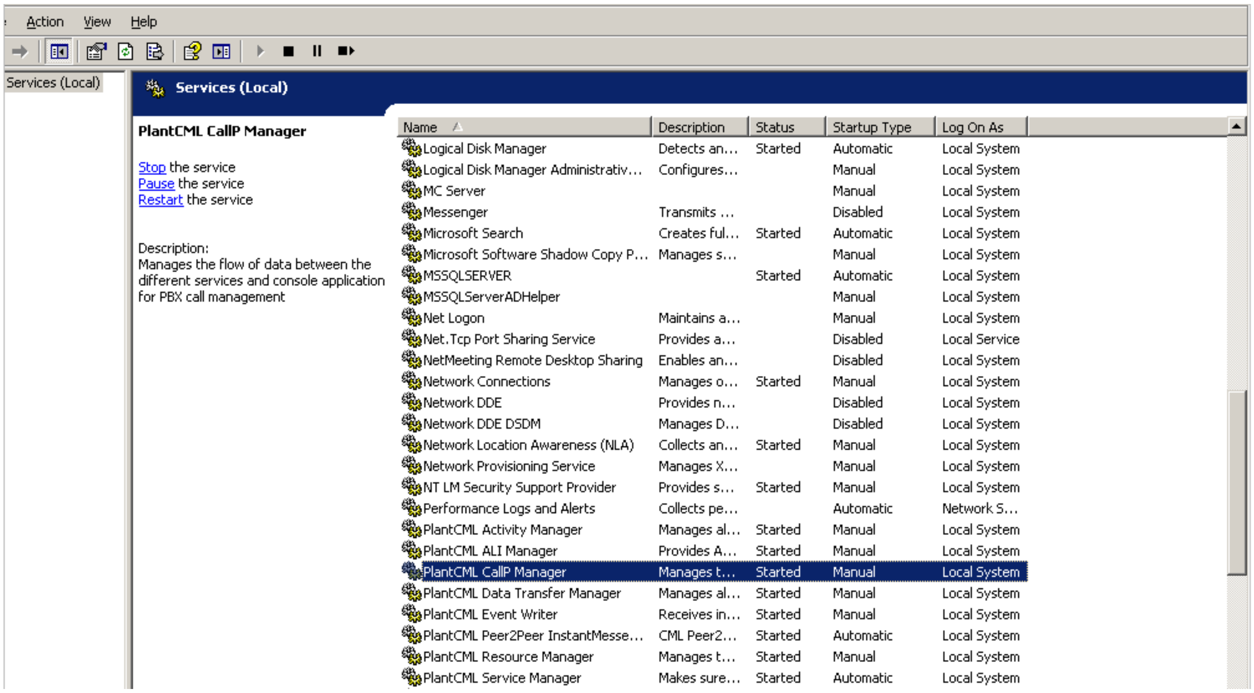


CLAN Card Configuration

IP Address	LSP
9.1.1.8	□
9.1.1.9	□
9.1.4.2	☑

6.4. Restart CallP Manager

From the Sentinel active server, restart the CallP Manager by selecting **Start** > **Control Panel** > **Administrative Tools** > **Services**. Right click on **PlantCML CallP Manager**, and select "Restart" from the drop down list. After restarting the CallP Manager, the Sentinel application will establish connectivity to Avaya AES and start querying on device information administered in the AES security database.



PlantCML CallP Manager

Stop the service
Pause the service
Restart the service

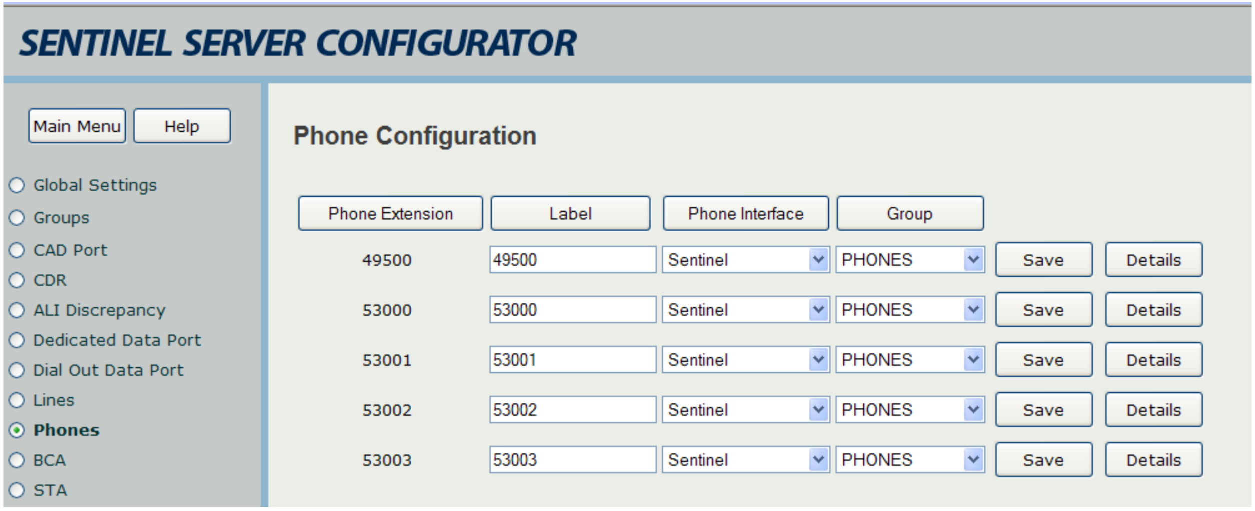
Description:
Manages the flow of data between the different services and console application for PBX call management

Name	Description	Status	Startup Type	Log On As
Logical Disk Manager	Detects an...	Started	Automatic	Local System
Logical Disk Manager Administrativ...	Configures...		Manual	Local System
MC Server			Manual	Local System
Messenger	Transmits ...		Disabled	Local System
Microsoft Search	Creates ful...	Started	Automatic	Local System
Microsoft Software Shadow Copy P...	Manages s...		Manual	Local System
MSSQLSERVER		Started	Automatic	Local System
MSSQLServerADHelper			Manual	Local System
Net Logon	Maintains a...		Manual	Local System
Net.Tcp Port Sharing Service	Provides a...		Disabled	Local Service
NetMeeting Remote Desktop Sharing	Enables an...		Disabled	Local System
Network Connections	Manages o...	Started	Manual	Local System
Network DDE	Provides n...		Disabled	Local System
Network DDE DSDM	Manages D...		Disabled	Local System
Network Location Awareness (NLA)	Collects an...	Started	Manual	Local System
Network Provisioning Service	Manages X...		Manual	Local System
NT LM Security Support Provider	Provides s...	Started	Manual	Local System
Performance Logs and Alerts	Collects pe...		Automatic	Network S...
PlantCML Activity Manager	Manages al...	Started	Manual	Local System
PlantCML ALI Manager	Provides A...	Started	Manual	Local System
PlantCML CallP Manager	Manages t...	Started	Manual	Local System
PlantCML Data Transfer Manager	Manages al...	Started	Manual	Local System
PlantCML Event Writer	Receives in...	Started	Manual	Local System
PlantCML Peer2Peer InstantMesse...	CML Peer2...	Started	Automatic	Local System
PlantCML Resource Manager	Manages t...	Started	Manual	Local System
PlantCML Service Manager	Makes sure...	Started	Automatic	Local System

6.5. Administer Sentinel Clients

Use the procedures in **Sections 6.2** to bring up an Internet browser window to log back into the Sentinel server. Select **Resources Configuration.** Select **Phones** from the left pane.

The **Phone Configuration** screen is displayed, and contains a listing of the "PHONES" device type obtained from Avaya AES. For each phone entry below, select "Sentinel" from the **Type** drop down list. This will allow the phone to be used as a Sentinel 9-1-1 client. Enter a more descriptive name into the **Label** field if desired, as shown below. Click the corresponding **Save** button after making changes for each phone entry.

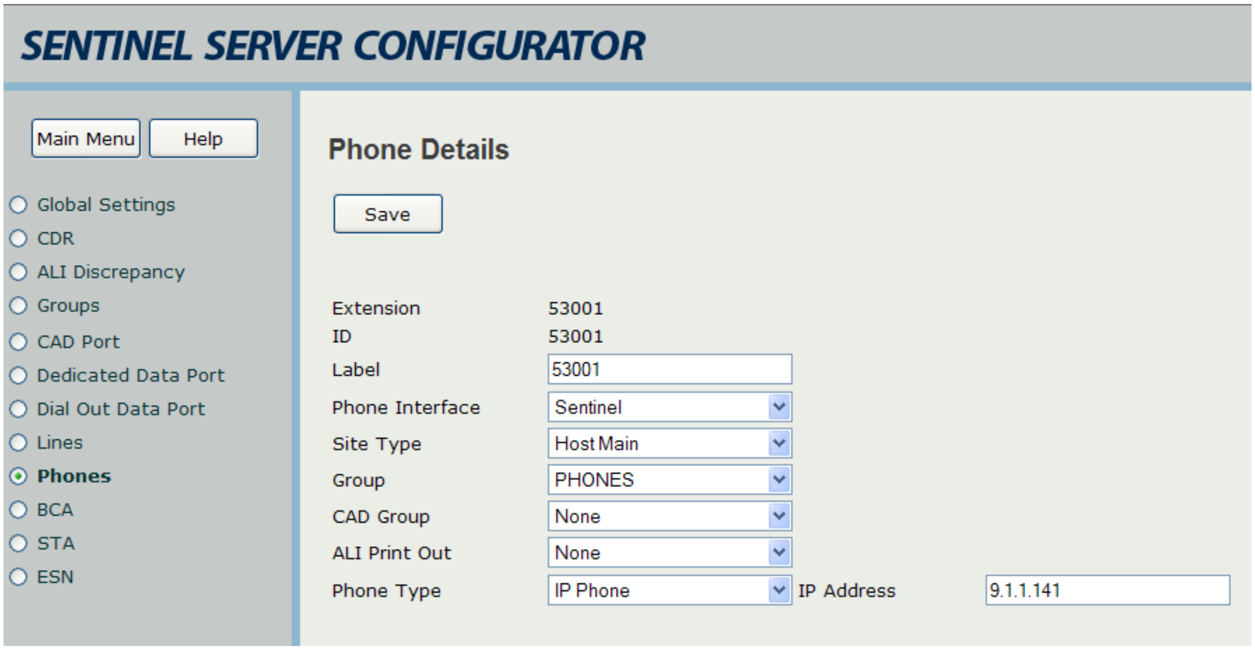


Phone Configuration

Phone Extension	Label	Phone Interface	Group		
49500	49500	Sentinel	PHONES	Save	Details
53000	53000	Sentinel	PHONES	Save	Details
53001	53001	Sentinel	PHONES	Save	Details
53002	53002	Sentinel	PHONES	Save	Details
53003	53003	Sentinel	PHONES	Save	Details

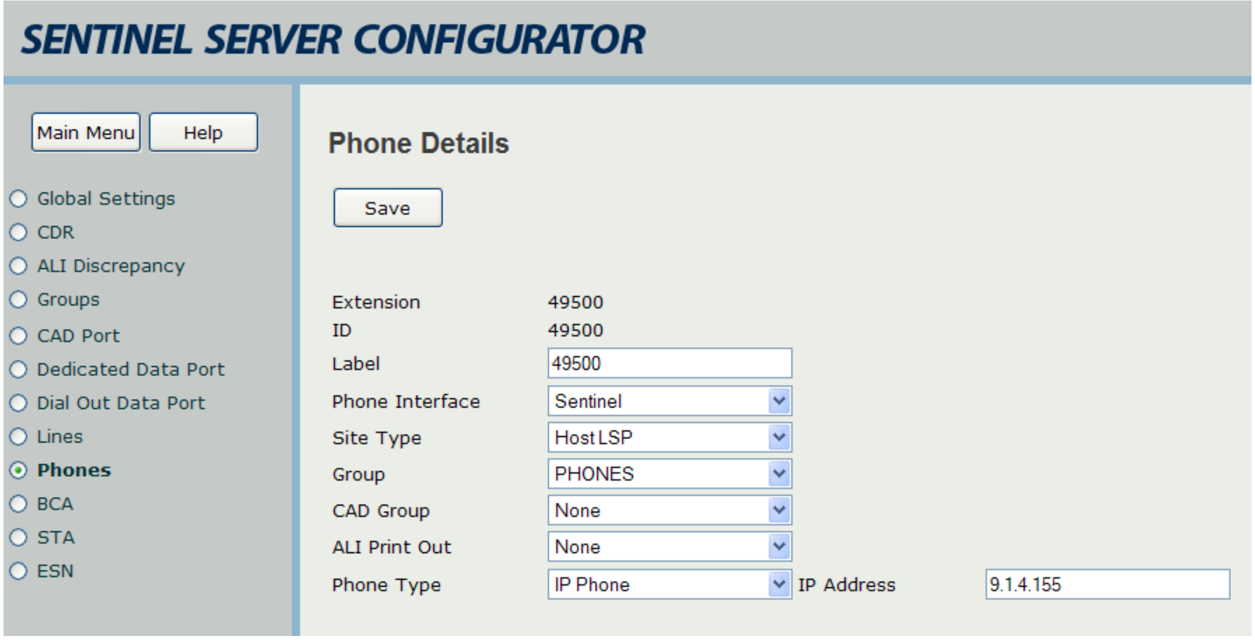
Click on Details button.

- From the pull down menu, select Site Type as **Host Main** for phones located at the Main Site.
- From the pull down menu, select Site Type as **Host LSP** for phones located at the Remote Site.
- It is recommended to populate the **Phone IP (Optional)** field if static IP addresses are used for 911 call answering agents IP Phones.
- Click the corresponding **Save** button after making changes for each phone entry.



Phone Details

Extension	53001
ID	53001
Label	53001
Phone Interface	Sentinel
Site Type	Host Main
Group	PHONES
CAD Group	None
ALI Print Out	None
Phone Type	IP Phone
IP Address	9.1.1.141

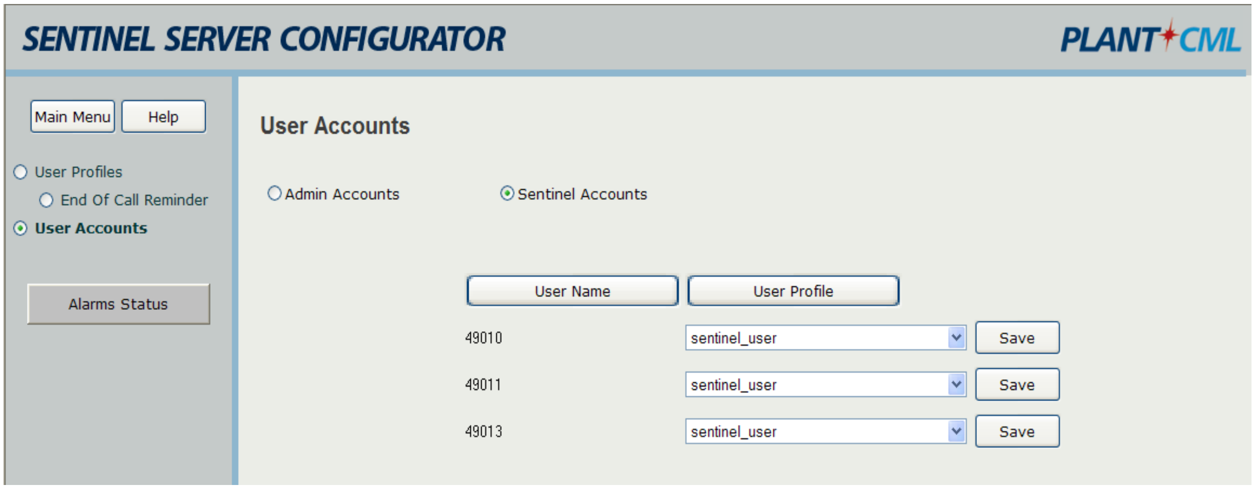


Phone Details

Extension	49500
ID	49500
Label	49500
Phone Interface	Sentinel
Site Type	Host LSP
Group	PHONES
CAD Group	None
ALI Print Out	None
Phone Type	IP Phone
IP Address	9.1.4.155

6.6. Verify Sentinel Accounts

From the main menu select **User Configuration.** Select **User Accounts** and click on **Sentinel Accounts**. Verify the Agents created in **Section 4.9** are listed here. Assign the **User Profile** "sentinel_user" for each agent from the pull down menu. Click the corresponding **Save** button after making changes for each phone entry.



User Name	User Profile
49010	sentinel_user
49011	sentinel_user
49013	sentinel_user

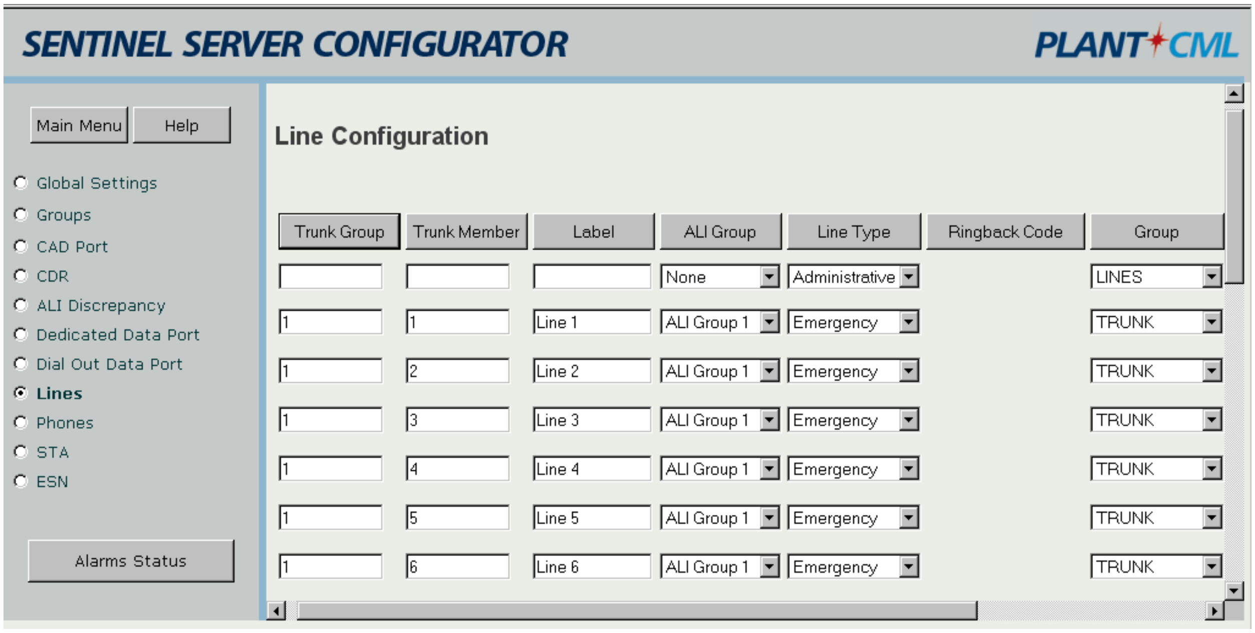
6.7. Administer Trunks

Select **Lines** from the left pane to administer information for the trunks on Avaya Communication Manager used for carrying the incoming 911 calls. An entry needs to be entered for each trunk used on Avaya Communication Manager. For the sample configuration, a trunk group number of "1" with "10" group members was created on Avaya Communication Manager for carrying the incoming 911 calls. Therefore ten such entries would need to be created. Create each entry with the following values:

- **Trunk Group:** Trunk group number for 911 calls, in this case "1".
- **Trunk Member:** A sequential number starting with "1".
- **Label:** A descriptive name.
- **ALI Group:** Select the appropriate ALI group from the drop down list.
- **Line Type:** Select "Emergency" from the drop down list.
- **Group:** Select "TRUNK" from the drop-down list.

Note that the **ALI Group** selection may vary. In the compliance testing, an internal database was used to obtain the ALI information, which corresponded to "ALI Group 1". The setting of "Emergency" in the **Line Type** field enables the Sentinel server to identify the call priority and to provide any desired call treatment, such as sending special audio alerts to the answering agents. Click the corresponding **Save** button to the right of each entry to submit the entry.

The screen below shows the first 6 trunks that were created for testing.



Line Configuration

Trunk Group	Trunk Member	Label	ALI Group	Line Type	Ringback Code	Group
			None	Administrative		LINES
1	1	Line 1	ALI Group 1	Emergency		TRUNK
1	2	Line 2	ALI Group 1	Emergency		TRUNK
1	3	Line 3	ALI Group 1	Emergency		TRUNK
1	4	Line 4	ALI Group 1	Emergency		TRUNK
1	5	Line 5	ALI Group 1	Emergency		TRUNK
1	6	Line 6	ALI Group 1	Emergency		TRUNK

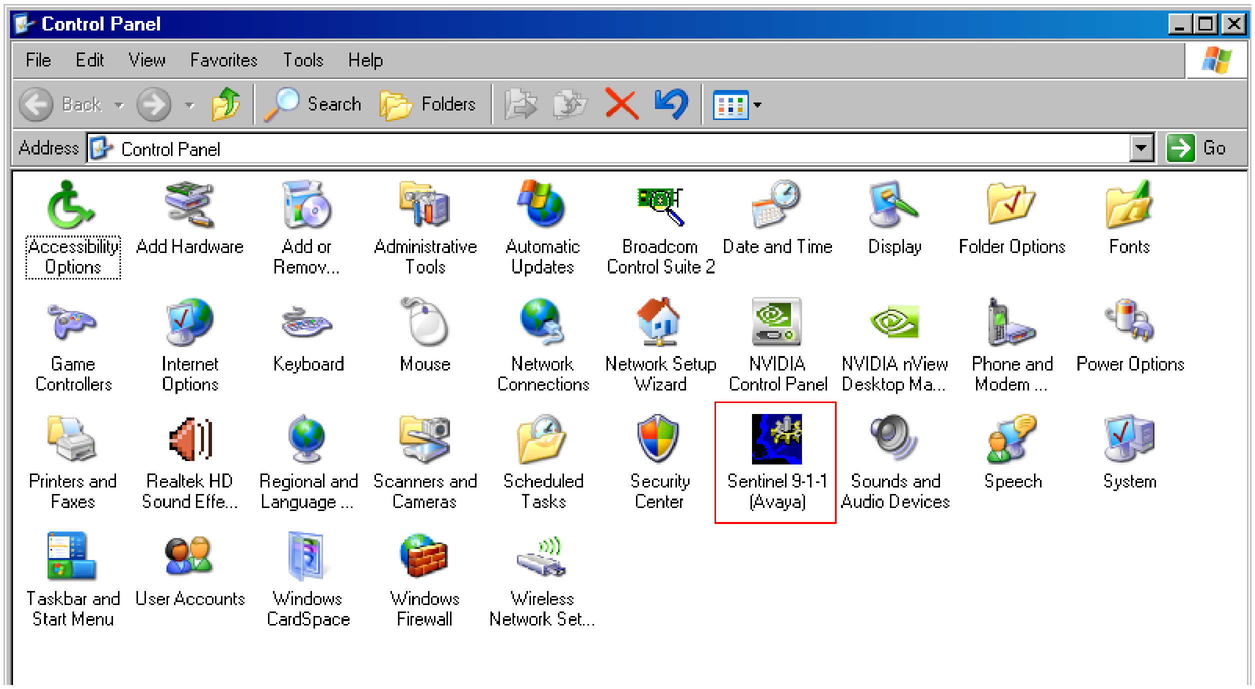
7. Configure PlantCML Sentinel 9-1-1 Clients

This section provides the procedures for configuring the PlantCML Sentinel 9-1-1 clients. The procedures include the following areas:

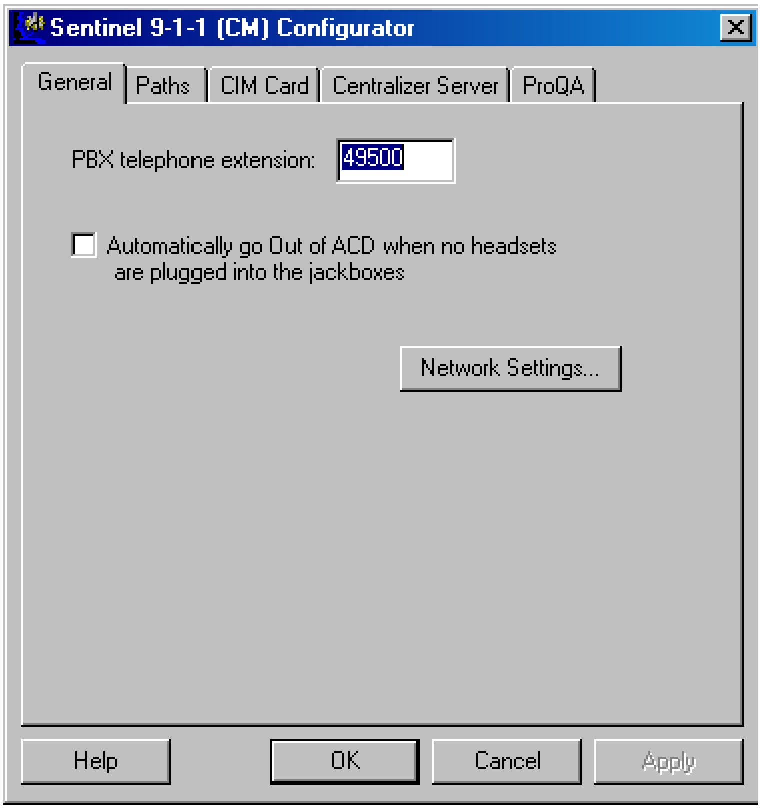
- Administer physical extension
- Log into logical extension
- Administer user configuration file

7.1. Administer Physical Extension

From each Sentinel 9-1-1 client PC, select **Start > Control Panel** to bring up the **Control Panel** screen. Double click on the **Sentinel 9-1-1 (Avaya)** icon, which was created as part of the **PlantCML Sentinel 9-1-1** installation.



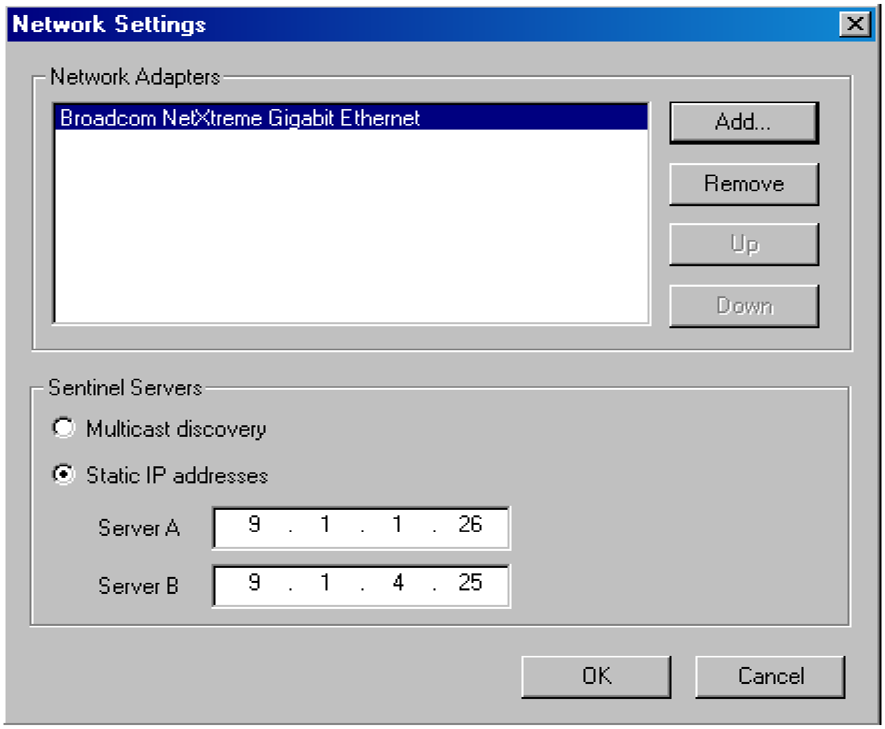
The **Sentinel 9-1-1 (Avaya) Configurator** screen is displayed. Enter the extension associated with the agent's physical telephone from **Section 4.5**, and click on **Network Settings**.



PBX telephone extension: 49500

□ Automatically go Out of ACD when no headsets are plugged into the jackboxes

The **Network Settings** screen is displayed next. Select **Static IP addresses** and enter the IP addresses for Sentinel Server A and Sentinel Server B, and click **OK**.



Network Settings

Network Adapters

Broadcom NetXtreme Gigabit Ethernet

Sentinel Servers

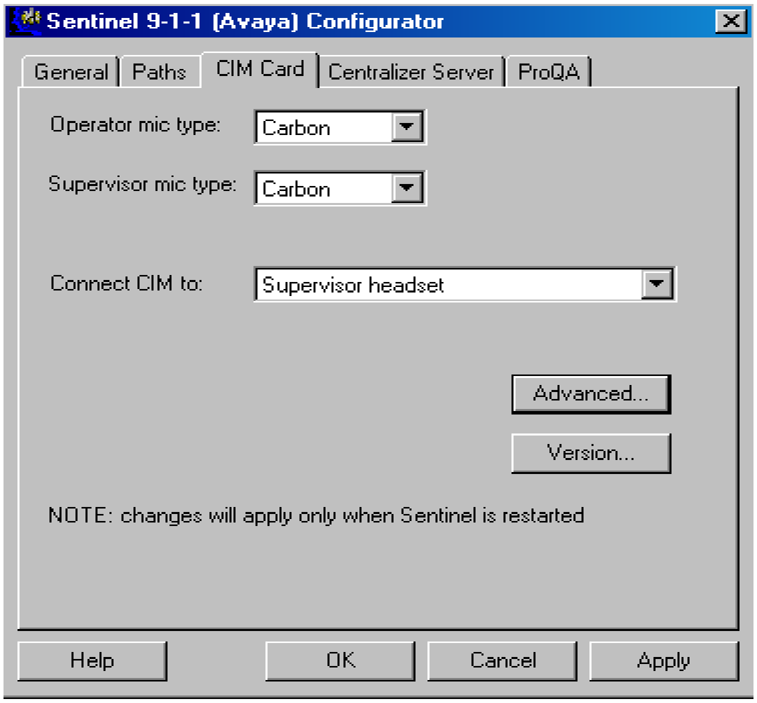
○ Multicast discovery

● Static IP addresses

Server A: 9 . 1 . 1 . 26

Server B: 9 . 1 . 4 . 25

From the **Sentinel 9-1-1 (Avaya) Configurator** screen, click on **CIM Card** tab.



Sentinel 9-1-1 (Avaya) Configurator

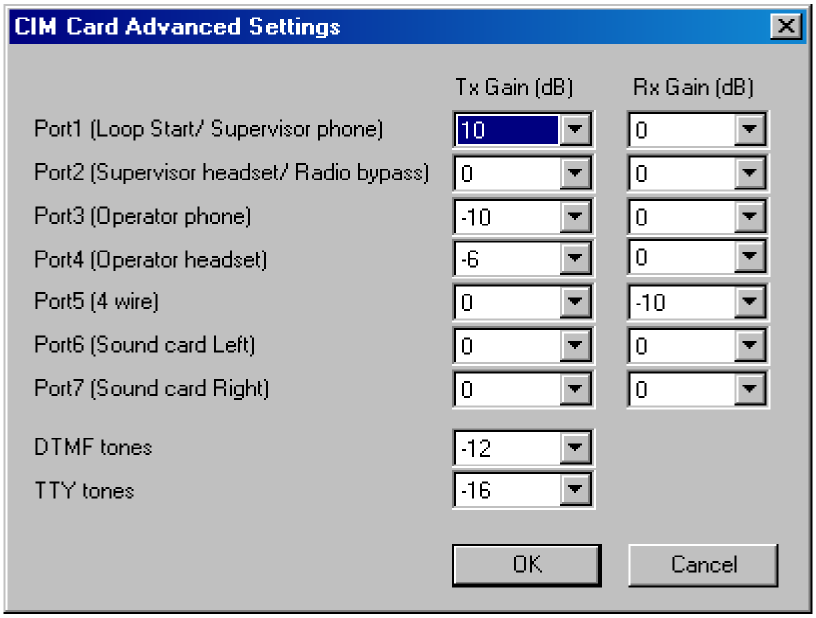
Operator mic type: Carbon

Supervisor mic type: Carbon

Connect CIM to: Supervisor headset

NOTE: changes will apply only when Sentinel is restarted

Click the **Advanced …** button. Set the parameters as shown below and click **OK**.



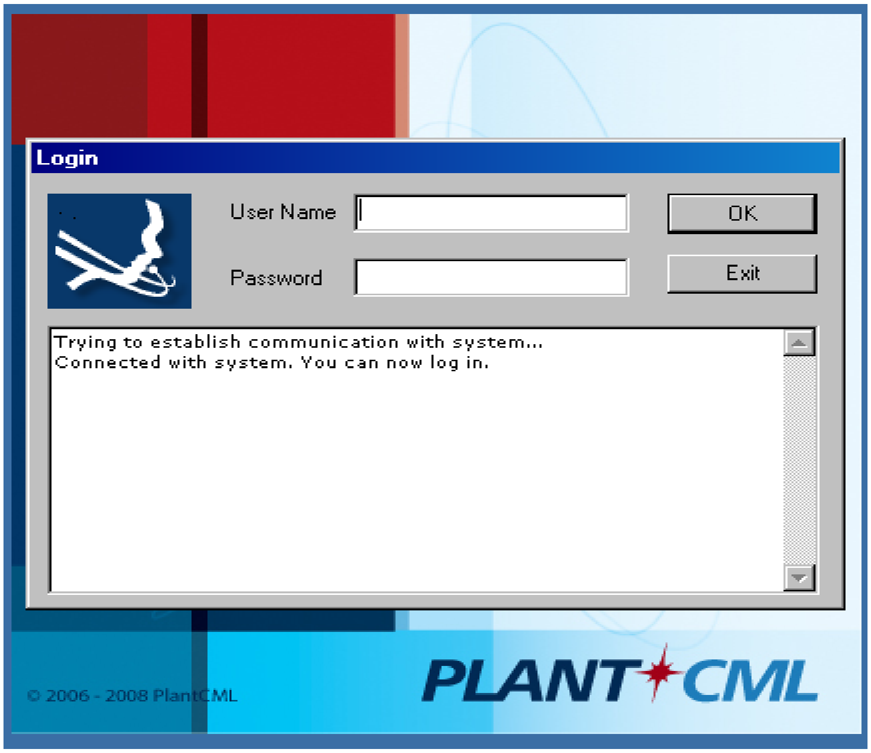
CIM Card Advanced Settings

	Tx Gain (dB)	Rx Gain (dB)
Port1 (Loop Start/ Supervisor phone)	10	0
Port2 (Supervisor headset/ Radio bypass)	0	0
Port3 (Operator phone)	-10	0
Port4 (Operator headset)	-6	0
Port5 (4 wire)	0	-10
Port6 (Sound card Left)	0	0
Port7 (Sound card Right)	0	0
DTMF tones	-12	
TTY tones	-16	

7.2. Log Into Logical Extension

From the agent desktop, double click the **Sentinel** icon shown below. This icon is created as part of the **PlantCML Sentinel 9-1-1** installation.

The **Sentinel 9-1-1 Login** screen is displayed. Enter a logical agent extension and associated password administered on Avaya Application Enablement Services from **Section 5.7**. Click **OK**.

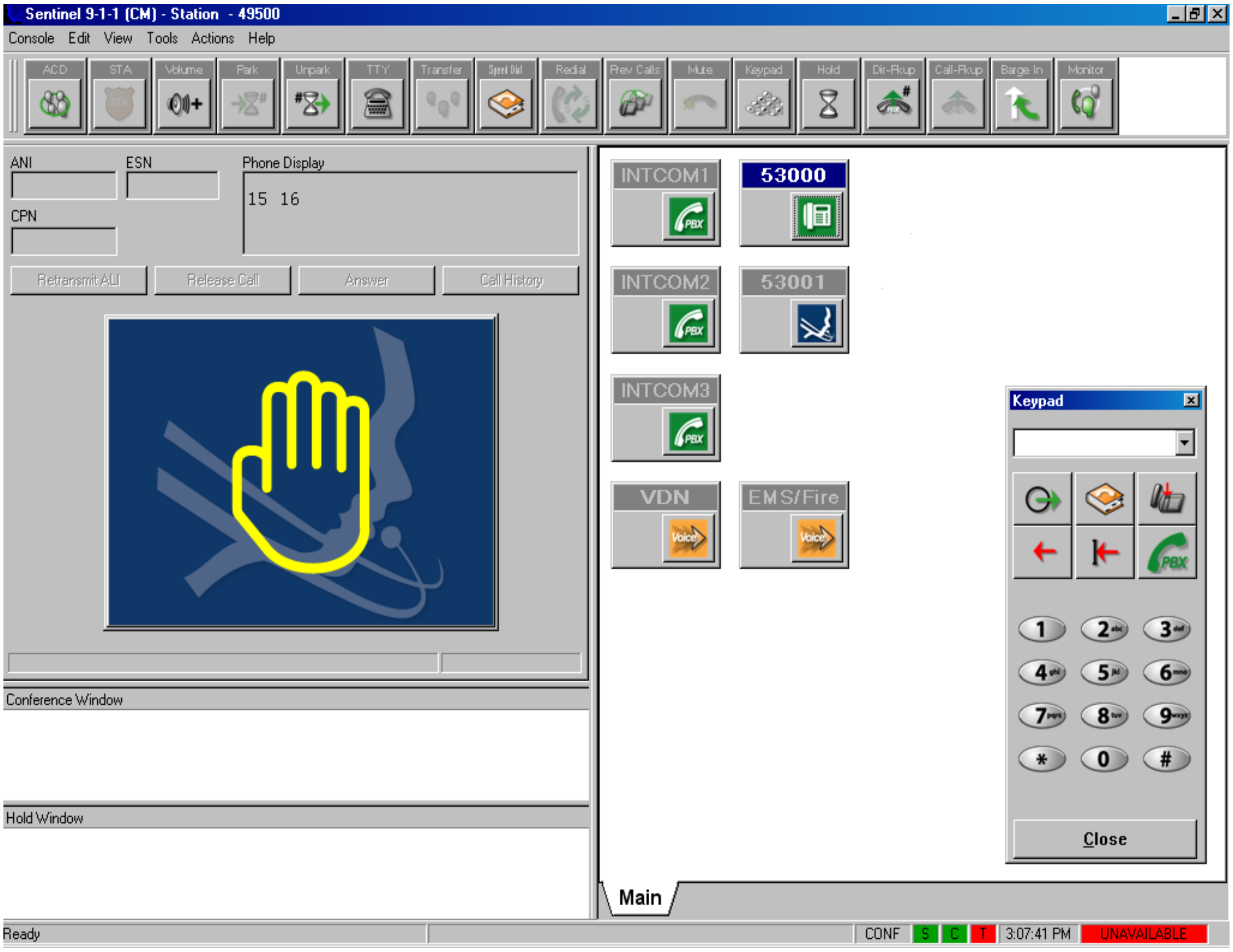


```
Trying to establish communication with system...
Connected with system. You can now log in.
```

7.3. Administer User Configuration File

Upon initial log in, the **User Configuration** screen (not shown) will be displayed. The **User name** field is automatically populated with the agent's physical telephone extension from **Section 7.1**. Click on **Browse** and navigate to **C:** → **Program Files** → **PlantCML** → **Sentinel 9-1-1-Avaya** → **Ini** folder and select "**avayalab.cfg**" file. (This is part of the Sentinel Application and is supplied by Sentinel.) Click **OK**. The avayalab.cfg file contains the configuration information for the Sentinel GUI layout.

The **Sentinel 9-1-1 (Avaya) – Station** screen is displayed as shown below. From this point on, the agent can customize his/her desktop using options under **Console > Preferences > Desktop**. Refer to the Sentinel documentation in **Section 12** for how to customize the graphical user interface, such as creating icons for call related actions, and specifying the fonts for the icons.



Phone Display: 15 16

8. General Test Approach and Test Results

All the test cases were performed manually. Upon start of the Sentinel application, the application automatically queries Avaya Communication Manager for VDN/agent status and requests monitoring. Incoming 911 calls were made to the monitored VDNs. Call controls from both the agent desktop and the agent telephones were exercised to verify event reports associated with features such as conferencing and transferring of calls.

The serviceability testing focused on verifying the ability of Sentinel to recover from adverse conditions, such as WAN failure.

The verification of all tests included checking of proper states at the telephone sets, and Sentinel 9-1-1 clients.

9. Verification

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya Application Enablement Services, and PlantCML Sentinel server and Sentinel 9-1-1 clients.

9.1. Normal Operations

9.1.1. Main PSAP Site

On Avaya Communication Manager at the Main PSAP Site, verify the status of the AE Services server by using the "change ip-services" command. Verify that the **Status** is "in-use" for both the AES administered in **Section 4.3**, as shown below.

```
change ip-services                                            Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      govaes1                                 y        in use
      2:      govaes2                                 y        in use
```

Verify the status of the CTI links by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for both the CTI links administered in **Section 4.4**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     4        no    govaes1          established   1045     1030
2     4        no    govaes2          established   1036     1025
```

Verify the status of the AES links by using the "status aesvcs link" command.

```
status aesvcs link

                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

01/01  govaes1           9.  1.  4. 52  44159   CLAN-01B02      628     1144
01/02  govaes1           9.  1.  4. 52  44161   CLAN-01A02      179     179
02/03  govaes2           9.  1.  1. 51  37526   CLAN-01B02      623     1143
02/04  govaes2           9.  1.  1. 51  37608   CLAN-01A02      180     180
```

Verify the status of the agent registration by using the "list registered-ip-stations" command. Verify that there are two entries for each station, one for IP station and another for PlantCML

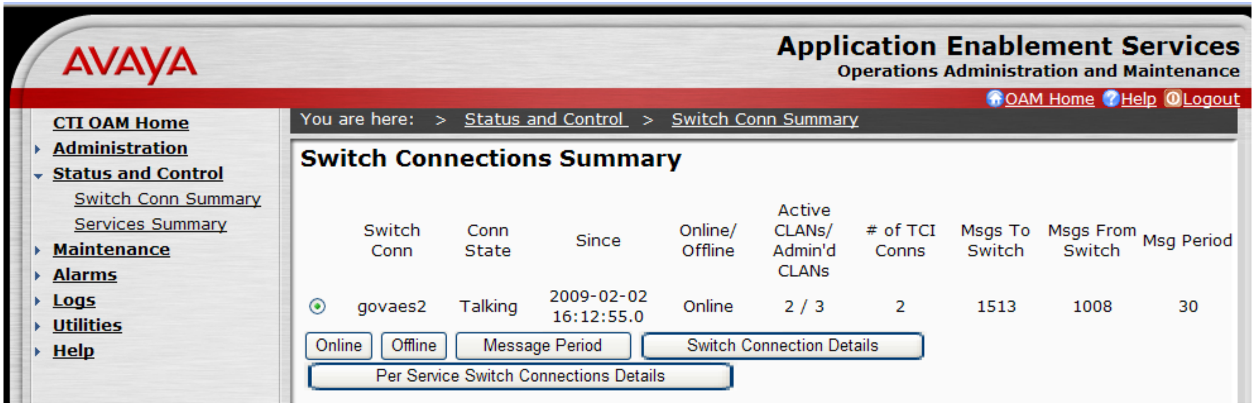
Sentinel 9-1-1 application that will uses the Device, Media and Call Control API via Avaya AES to register the agent/client softphone.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext/  Set     Product    Prod   Station         Net Gatekeeper     TCP
 Orig Port    Type    ID         Rel    IP Address      Rgn IP Address     Skt
49500         4620    IP_Phone   2.8000 9.1.4.155       4   9.1.1.8         y
49500         4620    IP_API_A   3.2040 9.1.1.51        1   9.1.1.9         y
53001         9630    IP_Phone   2.0000 9.1.1.141       1   9.1.1.9         y
53001         9630    IP_API_A   3.2040 9.1.1.51        1   9.1.1.8         y
```

Verify the agent status by using the "list agentID" command.

```
list agent-loginID                                                  Page   1

                               AGENT LOGINID

Login         Name/            Dir Agt COR Ag SO Skil/Lv Skil/Lv Skil/Lv Skil/Lv
ID            Extension        AAS/AUD     Pr
49010         PlantCML Agent1          1   lvl n   15/01   16/01     /       /
              49500                                  /       /       /       /
49011         PlantCMl Agent2          1   lvl n   15/01     /       /       /
              53001                                  /       /       /       /
```

On Avaya AES, verify the status of the switch connection by selecting **Status and Control > Switch Conn Summary** from the left pane. Verify that the **Conn State** is "Talking" for the switch connection administered in **Section 5.3**, as shown below.



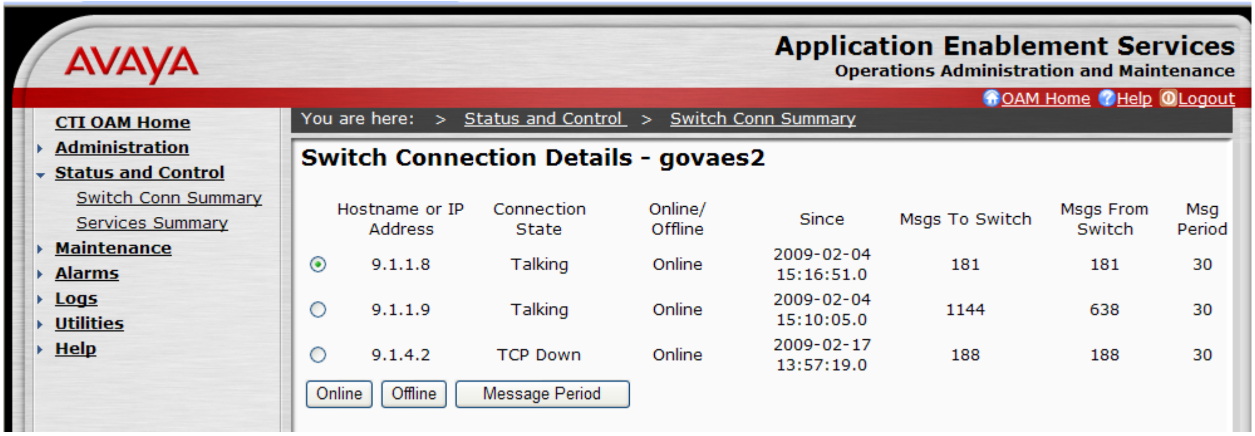
AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
You are here: > Status and Control > Switch Conn Summary
CTI OAM Home
Administration
Status and Control
Switch Conn Summary
Services Summary
Maintenance
Alarms
Logs
Utilities
Help
Online
Offline
Message Period
Switch Connection Details
Per Service Switch Connections Details

Switch Connections Summary

	Switch Conn	Conn State	Since	Online/ Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
◉	govaes2	Talking	2009-02-02 16:12:55.0	Online	2 / 3	2	1513	1008	30

Verify the status of the switch connection by selecting **Switch Connection Details**. Verify that the **Connection State** is:

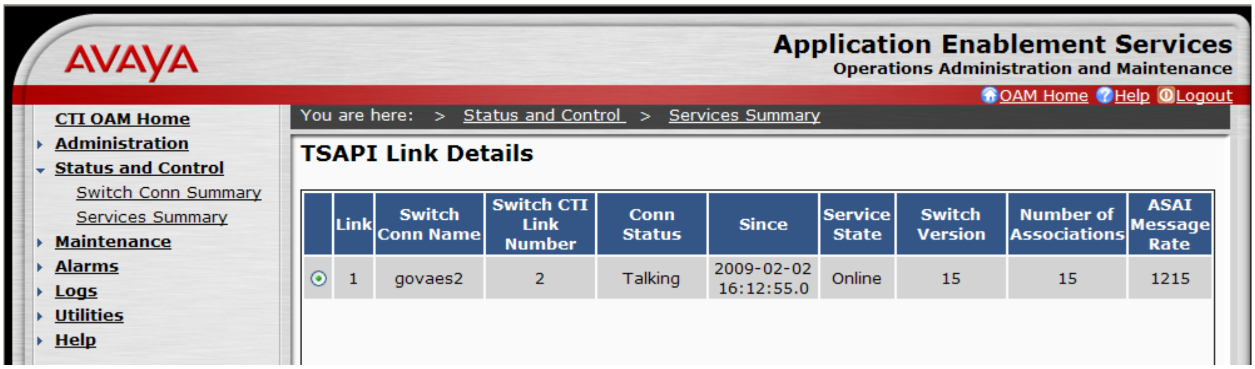
- "Talking" for the two CLANs.
- "TCP Down" for S8300 Media Sever.



Switch Connection Details - govaes2

	Hostname or IP Address	Connection State	Online/ Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
●	9.1.1.8	Talking	Online	2009-02-04 15:16:51.0	181	181	30
○	9.1.1.9	Talking	Online	2009-02-04 15:10:05.0	1144	638	30
○	9.1.4.2	TCP Down	Online	2009-02-17 13:57:19.0	188	188	30

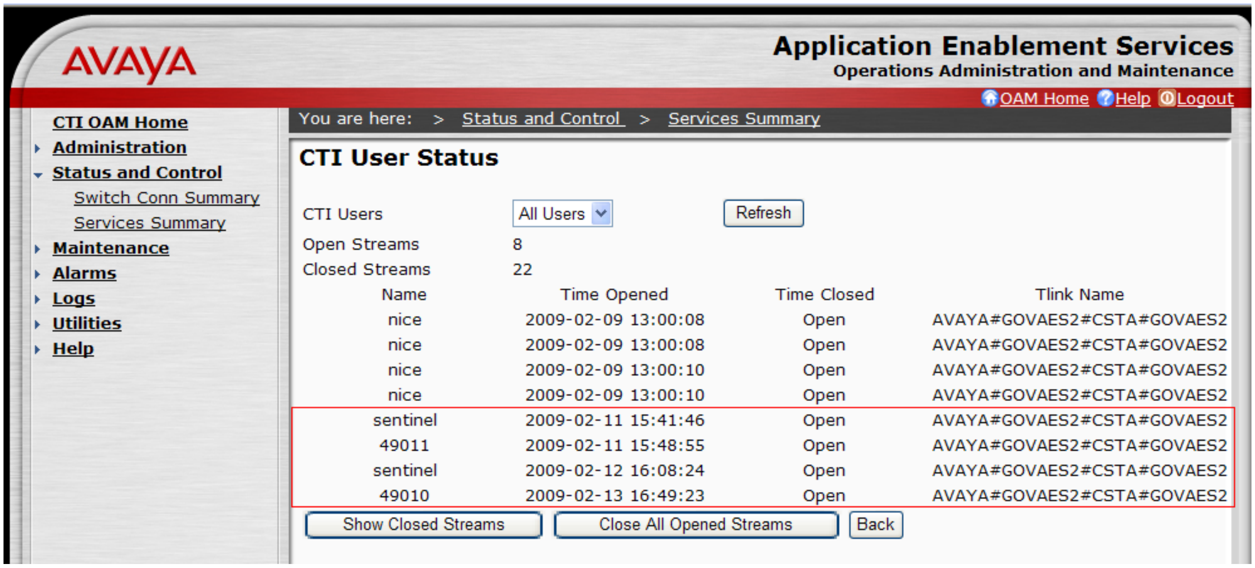
On AES at the Main PSAP Site - verify the status of the TSAPI link by selecting **Status and Control > Services Summary** from the left pane. Click on **TSAPI Service**, followed by **Details** (not shown below). The **TSAPI Link Details** screen is displayed. Verify the **Conn Status** is "Talking" for the TSAPI link administered in **Section 5.4**, as shown below. Also verify the CTI User Status.



TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
●	1	govaes2	2	Talking	2009-02-02 16:12:55.0	Online	15	15	1215

Verify the user status by selecting **User Status** on the bottom of the TSAPI Link Details screen.



CTI User Status

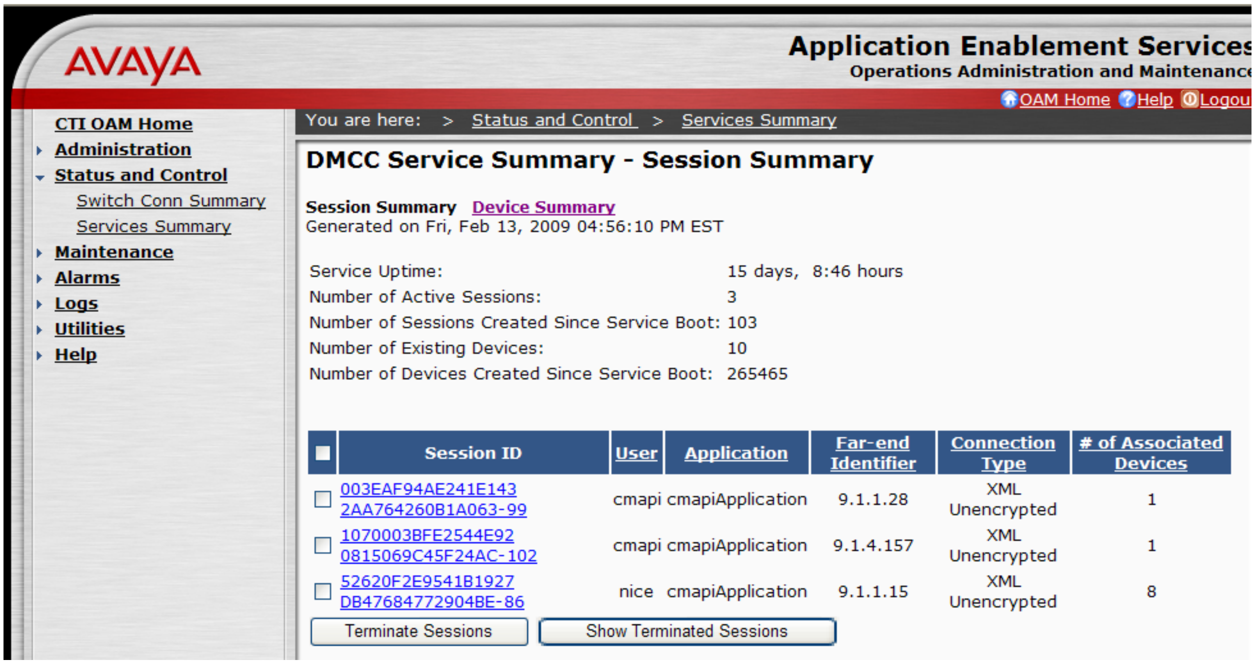
CTI Users: All Users [Refresh]

Open Streams: 8

Closed Streams: 22

Name	Time Opened	Time Closed	Tlink Name
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
sentinel	2009-02-11 15:41:46	Open	AVAYA#GOVAES2#CSTA#GOVAES2
49011	2009-02-11 15:48:55	Open	AVAYA#GOVAES2#CSTA#GOVAES2
sentinel	2009-02-12 16:08:24	Open	AVAYA#GOVAES2#CSTA#GOVAES2
49010	2009-02-13 16:49:23	Open	AVAYA#GOVAES2#CSTA#GOVAES2

On AES at the Main PSAP Site – verify the status of the DMCC by selecting **Status and Control > Services Summary** from the left pane. Click on **DMCC Service**, followed by **Details** (not shown below). The **DMCC Service Summary – Session Summary** screen is displayed.



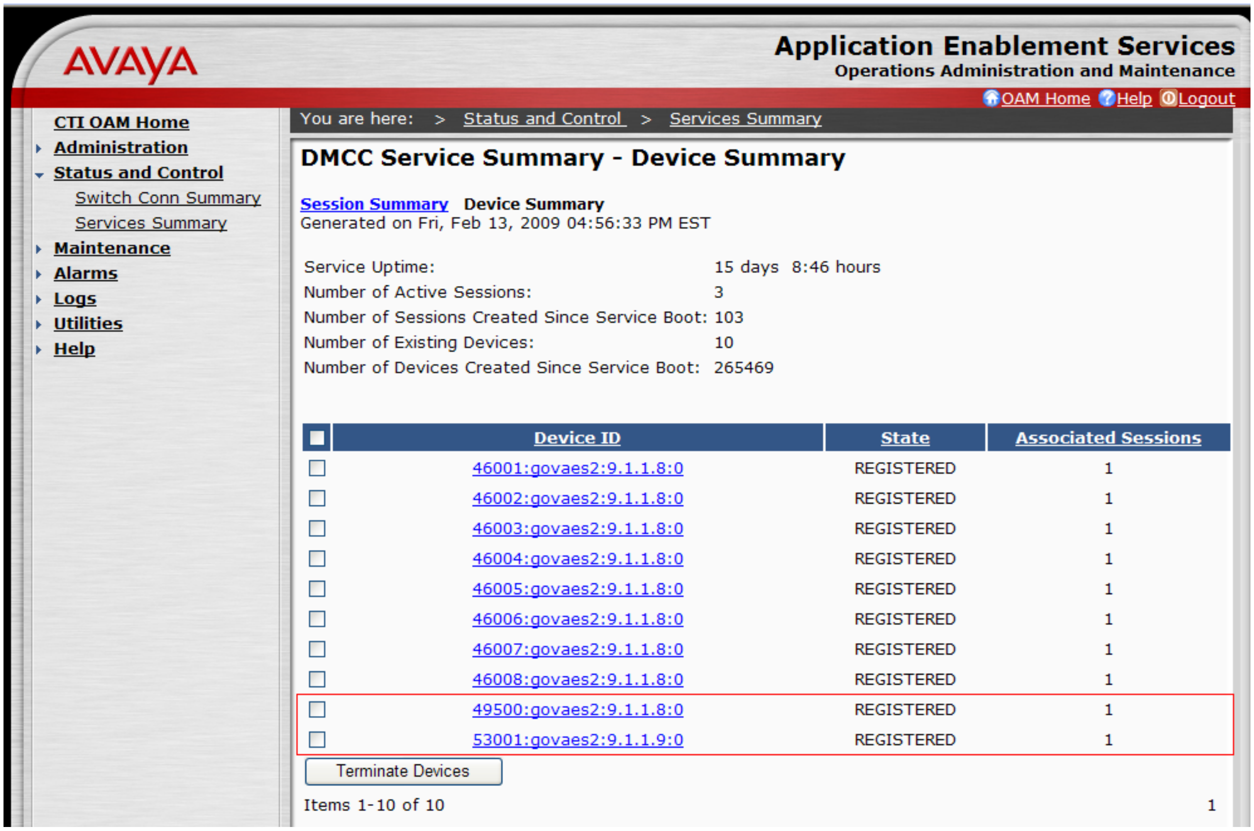
DMCC Service Summary - Session Summary

Session Summary Device Summary
Generated on Fri, Feb 13, 2009 04:56:10 PM EST

Service Uptime:	15 days, 8:46 hours
Number of Active Sessions:	3
Number of Sessions Created Since Service Boot:	103
Number of Existing Devices:	10
Number of Devices Created Since Service Boot:	265465

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	003EAF94AE241E143 2AA764260B1A063-99	cmapi	cmapiApplication	9.1.1.28	XML Unencrypted	1
□	1070003BFE2544E92 0815069C45F24AC-102	cmapi	cmapiApplication	9.1.4.157	XML Unencrypted	1
□	52620F2E9541B1927 DB47684772904BE-86	nice	cmapiApplication	9.1.1.15	XML Unencrypted	8

Verify that all the devices are listed in the **Device Summary** as shown below:



DMCC Service Summary - Device Summary

Session Summary Device Summary
Generated on Fri, Feb 13, 2009 04:56:33 PM EST

Service Uptime: 15 days 8:46 hours
Number of Active Sessions: 3
Number of Sessions Created Since Service Boot: 103
Number of Existing Devices: 10
Number of Devices Created Since Service Boot: 265469

☐	Device ID	State	Associated Sessions
☐	46001:govaes2:9.1.1.8:0	REGISTERED	1
☐	46002:govaes2:9.1.1.8:0	REGISTERED	1
☐	46003:govaes2:9.1.1.8:0	REGISTERED	1
☐	46004:govaes2:9.1.1.8:0	REGISTERED	1
☐	46005:govaes2:9.1.1.8:0	REGISTERED	1
☐	46006:govaes2:9.1.1.8:0	REGISTERED	1
☐	46007:govaes2:9.1.1.8:0	REGISTERED	1
☐	46008:govaes2:9.1.1.8:0	REGISTERED	1
☐	49500:govaes2:9.1.1.8:0	REGISTERED	1
☐	53001:govaes2:9.1.1.9:0	REGISTERED	1

Items 1-10 of 10 1

9.1.2. Remote PSAP Site

On Avaya Communication Manager at the Remote PSAP Site, verify the status of the AE Services server by using the “change ip-services” command. Verify that the **Status** is “idle” for the AES administered in **Section 4.3**, as shown below. Perform these commands on the LSP server.

```
change ip-services                                               Page   4 of   4
                            AE Services Administration

   Server ID     AE Services        Password          Enabled    Status
                   Server
      1:       govaes1                                   y        in use
      2:       govaes2                                   y        idle
```

Verify the status of the CTI links by using the “status aesvcs cti-link” command. Verify that the **Service State** is “down” for the CTI links administered in **Section 4.4**, as shown below.

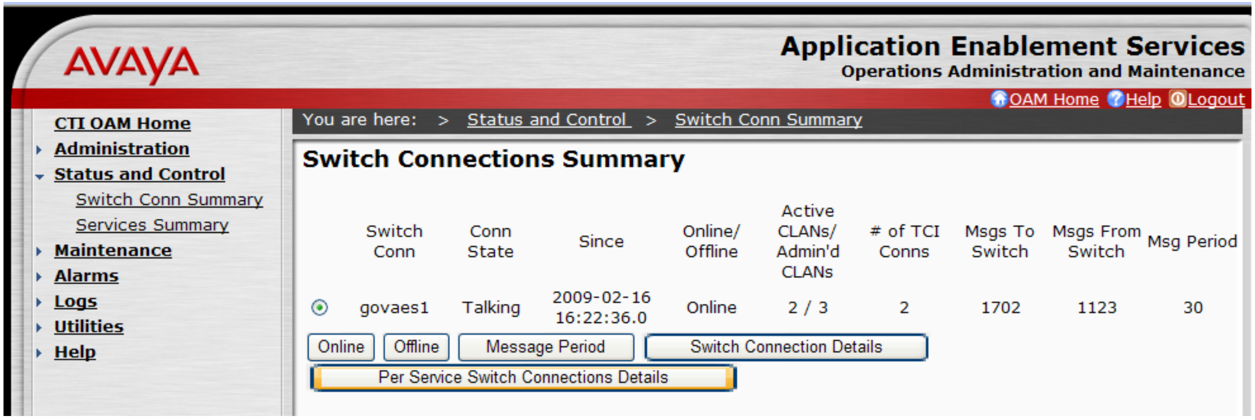
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1              no                     down          0        0
2              no                     down          0        0
```

Verify the status of the AES links by using the “status aesvcs interface” and “status aesvcs link” commands. In normal operations, the Number of Connections will be “0”.

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node        Enabled?  Number of     Status
                            Connections

procr             yes       0             listening
CLAN-01B02        yes       0             intfce-down
```

```
status aesvcs link

                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

01/01  govaes1           9.  1.  4. 52  42488   procr           1       1
```

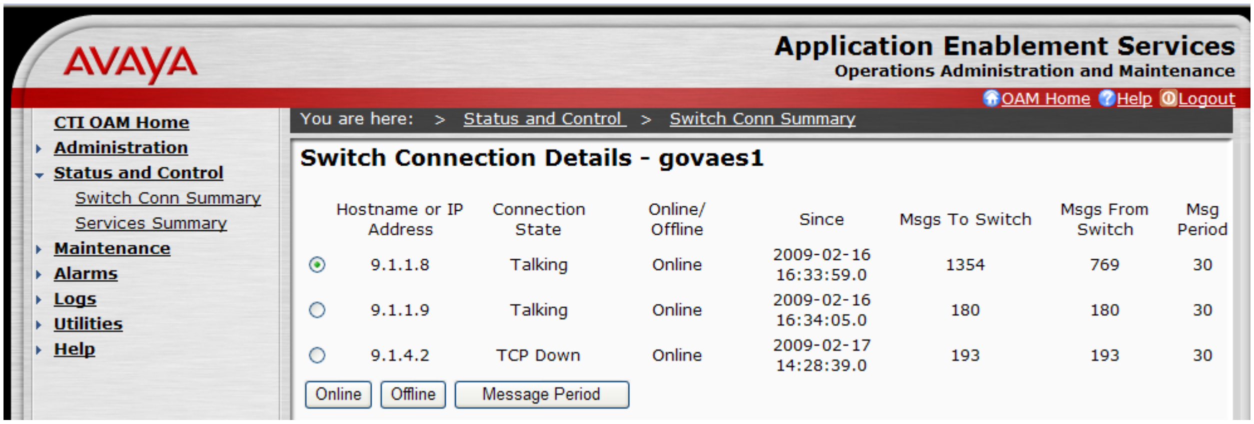
On AES at the Remote PSAP Site, verify the status of the switch connection by selecting **Status and Control > Switch Conn Summary** from the left pane.


AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
CTI OAM Home
Administration
Status and Control
Switch Conn Summary
Services Summary
Maintenance
Alarms
Logs
Utilities
Help
You are here: > Status and Control > Switch Conn Summary

Switch Connections Summary

	Switch Conn	Conn State	Since	Online/ Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
◉	govaes1	Talking	2009-02-16 16:22:36.0	Online	2 / 3	2	1702	1123	30

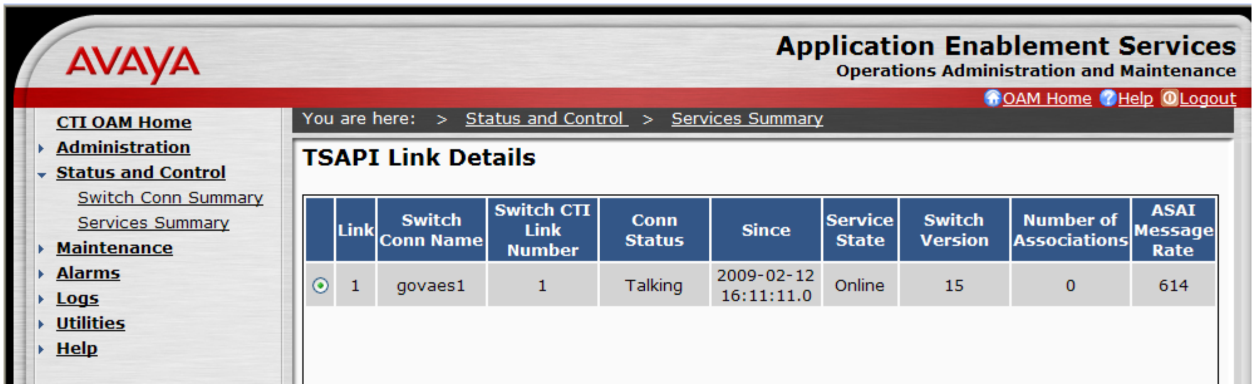
Online
Offline
Message Period
Switch Connection Details
Per Service Switch Connections Details



Switch Connection Details - govaes1

	Hostname or IP Address	Connection State	Online/ Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
◉	9.1.1.8	Talking	Online	2009-02-16 16:33:59.0	1354	769	30
○	9.1.1.9	Talking	Online	2009-02-16 16:34:05.0	180	180	30
○	9.1.4.2	TCP Down	Online	2009-02-17 14:28:39.0	193	193	30

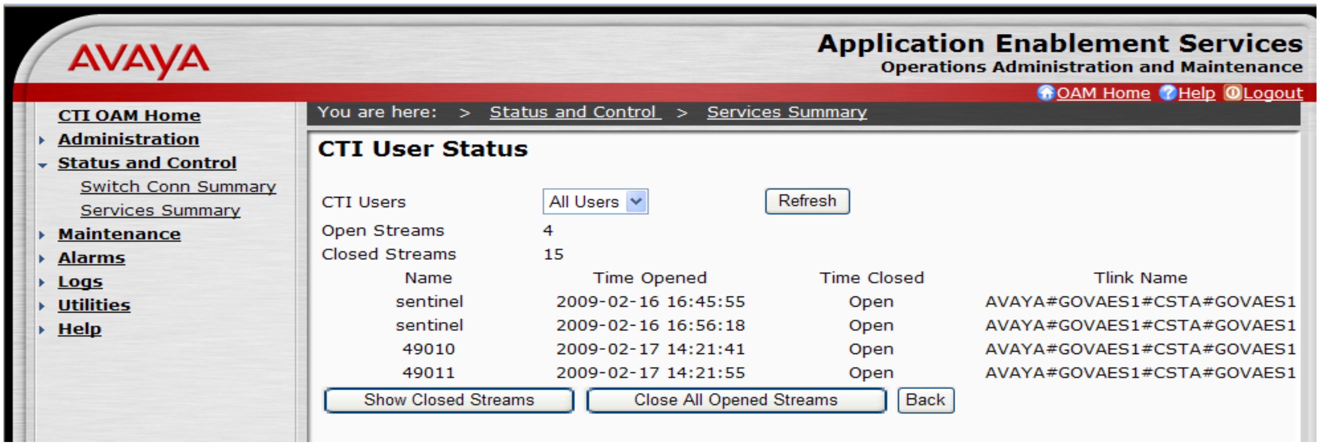
On AES at the Remote PSAP Site - verify the status of the TSAPI link. **The number of associations will be 0.**



TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
◉	1	govaes1	1	Talking	2009-02-12 16:11:11.0	Online	15	0	614

Verify the user status by selecting **User Status** on the bottom of the TSAPI Link Details screen.



CTI User Status

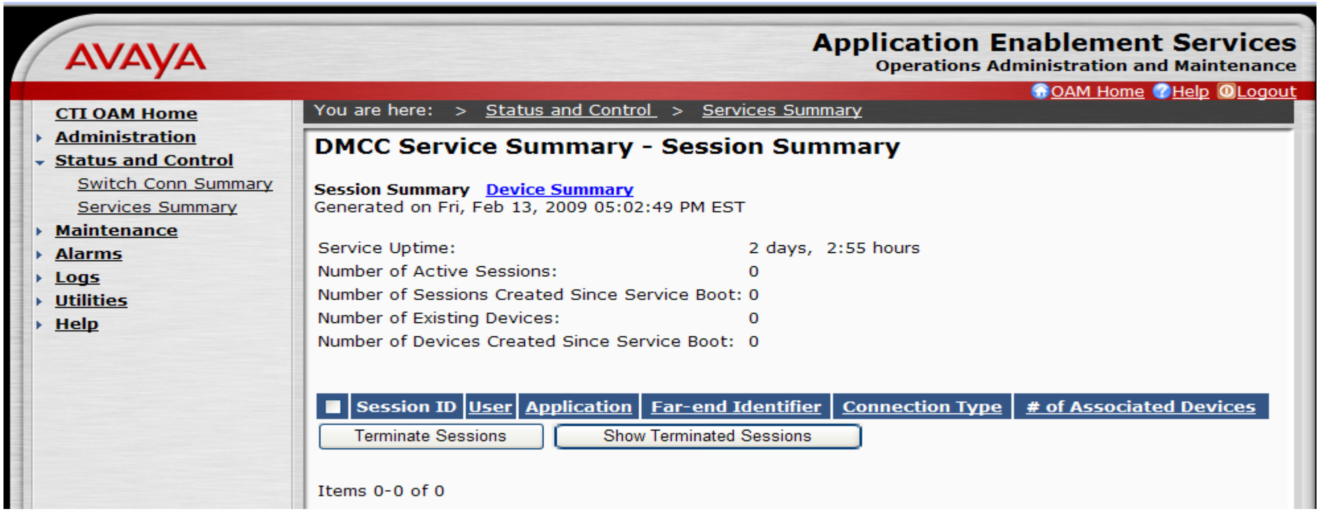
CTI Users: All Users [Refresh]

Open Streams: 4

Closed Streams: 15

Name	Time Opened	Time Closed	Tlink Name
sentinel	2009-02-16 16:45:55	Open	AVAYA#GOVAES1#CSTA#GOVAES1
sentinel	2009-02-16 16:56:18	Open	AVAYA#GOVAES1#CSTA#GOVAES1
49010	2009-02-17 14:21:41	Open	AVAYA#GOVAES1#CSTA#GOVAES1
49011	2009-02-17 14:21:55	Open	AVAYA#GOVAES1#CSTA#GOVAES1

Verify the status of the **DMCC Service**. The **DMCC Service Summary – Session Summary** screens are displayed below.



DMCC Service Summary - Session Summary

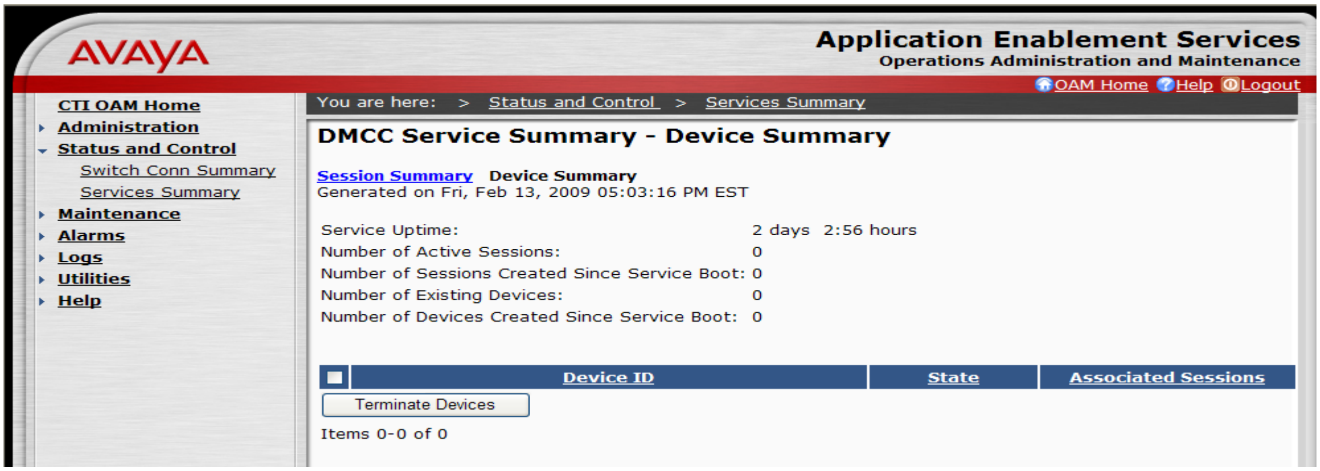
Session Summary Device Summary

Generated on Fri, Feb 13, 2009 05:02:49 PM EST

Service Uptime:	2 days, 2:55 hours
Number of Active Sessions:	0
Number of Sessions Created Since Service Boot:	0
Number of Existing Devices:	0
Number of Devices Created Since Service Boot:	0

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices

Items 0-0 of 0



DMCC Service Summary - Device Summary

Session Summary **Device Summary**

Generated on Fri, Feb 13, 2009 05:03:16 PM EST

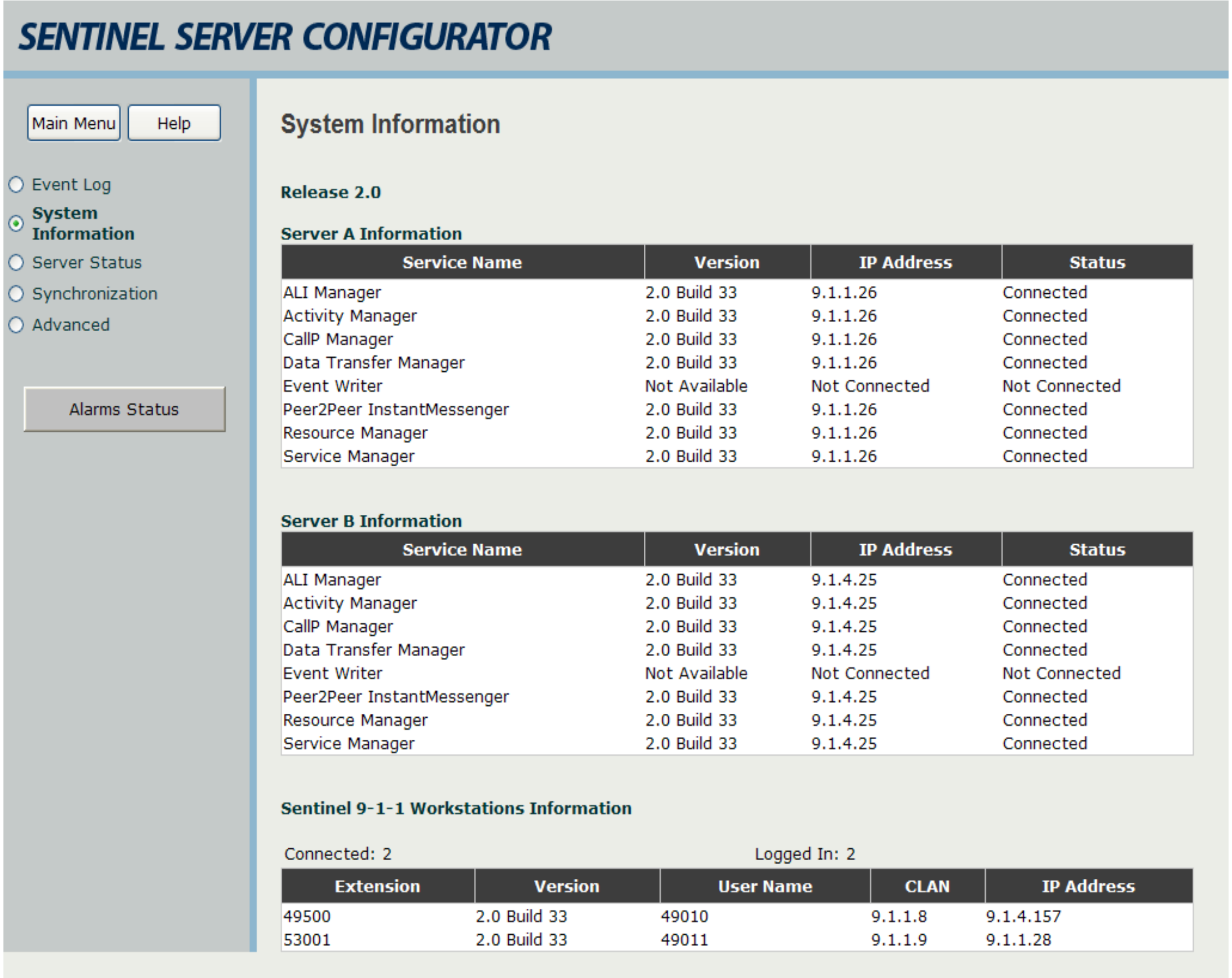
Service Uptime:	2 days 2:56 hours
Number of Active Sessions:	0
Number of Sessions Created Since Service Boot:	0
Number of Existing Devices:	0
Number of Devices Created Since Service Boot:	0

□	Device ID	State	Associated Sessions

Items 0-0 of 0

9.1.3. PlantCML Sentinel CM

Login the sentinel server by using the URL "http://<ip-adress>/Configurator" in an Internet Browser window, where "ip-address" is the IP address of the Sentinel active server. Navigate to **Main Menu → Maintenance**. Select **System Information** from the left side. Following screen will appear. Verify that the Service Names for both Sentinel CM Servers are "Connected".



System Information

Release 2.0

Server A Information

Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 33	9.1.1.26	Connected
Activity Manager	2.0 Build 33	9.1.1.26	Connected
CallP Manager	2.0 Build 33	9.1.1.26	Connected
Data Transfer Manager	2.0 Build 33	9.1.1.26	Connected
Event Writer	Not Available	Not Connected	Not Connected
Peer2Peer InstantMessenger	2.0 Build 33	9.1.1.26	Connected
Resource Manager	2.0 Build 33	9.1.1.26	Connected
Service Manager	2.0 Build 33	9.1.1.26	Connected

Server B Information

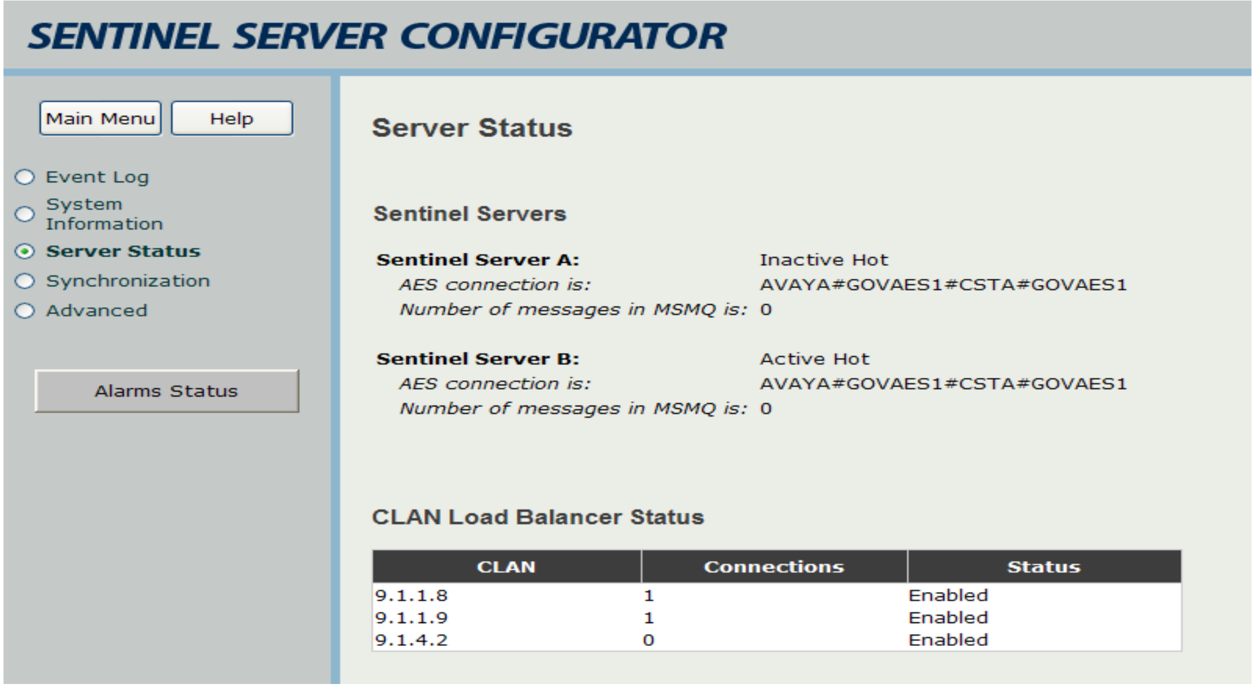
Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 33	9.1.4.25	Connected
Activity Manager	2.0 Build 33	9.1.4.25	Connected
CallP Manager	2.0 Build 33	9.1.4.25	Connected
Data Transfer Manager	2.0 Build 33	9.1.4.25	Connected
Event Writer	Not Available	Not Connected	Not Connected
Peer2Peer InstantMessenger	2.0 Build 33	9.1.4.25	Connected
Resource Manager	2.0 Build 33	9.1.4.25	Connected
Service Manager	2.0 Build 33	9.1.4.25	Connected

Sentinel 9-1-1 Workstations Information

Connected: 2 Logged In: 2

Extension	Version	User Name	CLAN	IP Address
49500	2.0 Build 33	49010	9.1.1.8	9.1.4.157
53001	2.0 Build 33	49011	9.1.1.9	9.1.1.28

Verify the status of the Sentinel CM Servers, by login to **Main Menu → Maintenance**. Select **Server Status** from the left side. Following Server Status screen will appear.



Server Status

Sentinel Servers

Sentinel Server A: Inactive Hot
AES connection is: AVAYA#GOVAES1#CSTA#GOVAES1
Number of messages in MSMQ is: 0

Sentinel Server B: Active Hot
AES connection is: AVAYA#GOVAES1#CSTA#GOVAES1
Number of messages in MSMQ is: 0

CLAN Load Balancer Status

CLAN	Connections	Status
9.1.1.8	1	Enabled
9.1.1.9	1	Enabled
9.1.4.2	0	Enabled

9.2. WAN Failure

9.2.1. Main PSAP Site

On Avaya Communication Manager at the Main PSAP Site, verify the status of the AE Services server by using the “change ip-services” command. Verify that the **Status** is “in-use” for the AES administered in **Section 4.3**, as shown below.

```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID     AE Services        Password          Enabled     Status
                    Server
      1:       govaes1                                  y         idle
      2:       govaes2                                  y         in use
```

Verify the status of the CTI links by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the correct CTI link.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI    Version   Mnt   AE Services       Service        Msgs      Msgs
Link             Busy  Server            State          Sent      Rcvd

1                no                      down           655       655
2      4         no    govaes2           established    688       688
```

Verify the status of the AES links by using the “status aesvcs link” command.

```
status aesvcs link

                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

02/03  govaes2           9.  1.  1. 51  37526   CLAN-01B02      683     1271
02/04  govaes2           9.  1.  1. 51  37608   CLAN-01A02      181     181
```

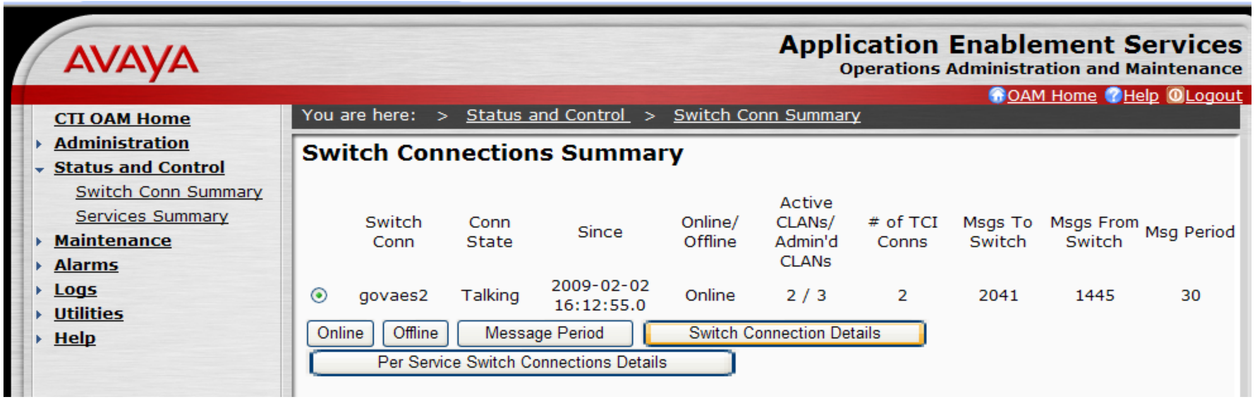
Verify the status of the agent registration by using the “list registered-ip-stations” command. Verify that there are two entries for each station, one for IP station and another for PlantCML Sentinel 9-1-1 application .

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext/  Set     Product    Prod   Station          Net Gatekeeper     TCP
 Orig Port    Type    ID         Rel    IP Address       Rgn IP Address     Skt
53001         9630    IP_Phone   2.0000 9.1.1.141        1   9.1.1.9         y
53001         9630    IP_API_A   3.2040 9.1.1.51         1   9.1.1.9         y
```

Verify the agent status by using the “list agentID” command.

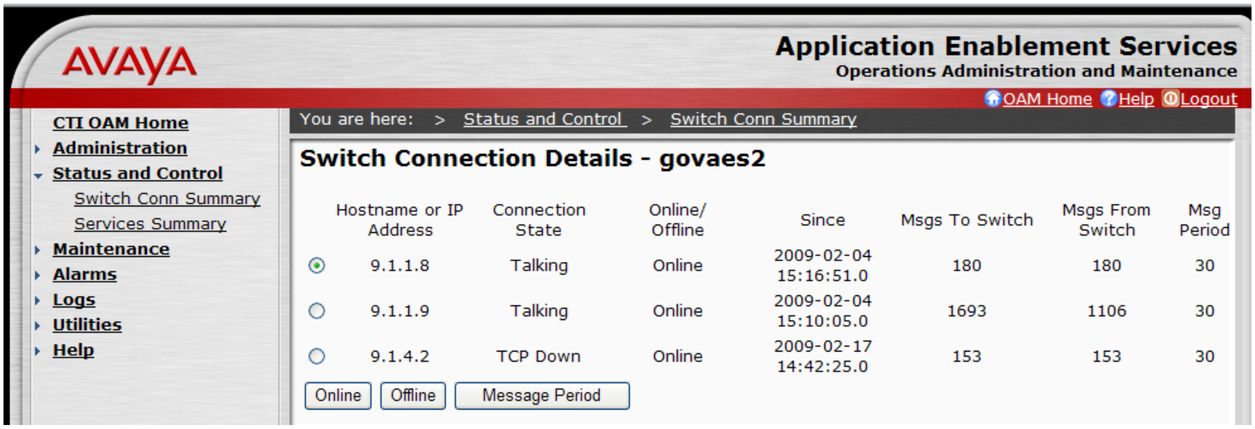
```
list agent-loginID                                                   Page   1

                               AGENT LOGINID

Login         Name/           Dir Agt COR Ag  SO Skil/Lv Skil/Lv Skil/Lv Skil/Lv
ID            Extension       AAS/AUD     Pr
49011         PlantCMl Agent2         1   lvl n   15/01     /       /       /
              53001                                 /       /       /       /
```

On Avaya AES, verify the status of the switch connection by selecting **Status and Control > Switch Conn Summary** from the left pane.


AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
CTI OAM Home
Administration
Status and Control
Switch Conn Summary
Services Summary
Maintenance
Alarms
Logs
Utilities
Help
You are here: > Status and Control > Switch Conn Summary
Online
Offline
Message Period
Switch Connection Details
Per Service Switch Connections Details

Switch Connections Summary

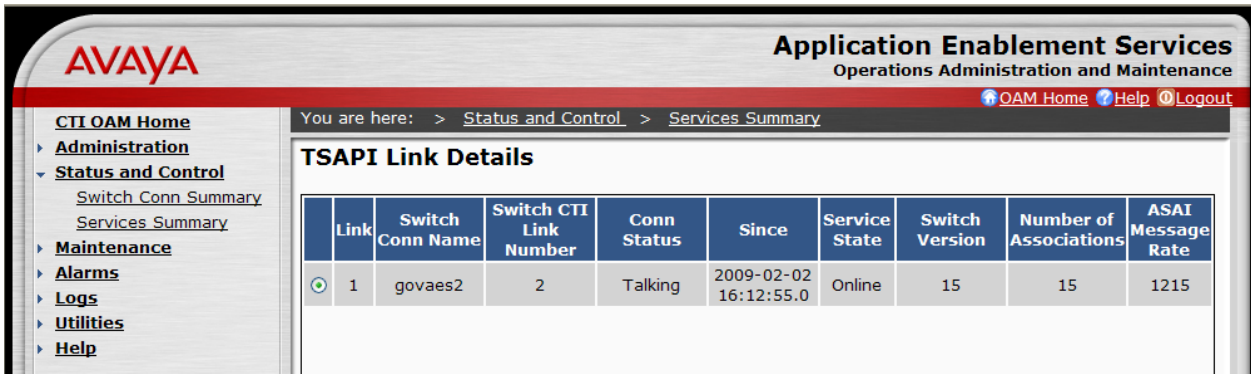
	Switch Conn	Conn State	Since	Online/ Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
●	govaes2	Talking	2009-02-02 16:12:55.0	Online	2 / 3	2	2041	1445	30



Switch Connection Details - govaes2

	Hostname or IP Address	Connection State	Online/ Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
●	9.1.1.8	Talking	Online	2009-02-04 15:16:51.0	180	180	30
○	9.1.1.9	Talking	Online	2009-02-04 15:10:05.0	1693	1106	30
○	9.1.4.2	TCP Down	Online	2009-02-17 14:42:25.0	153	153	30

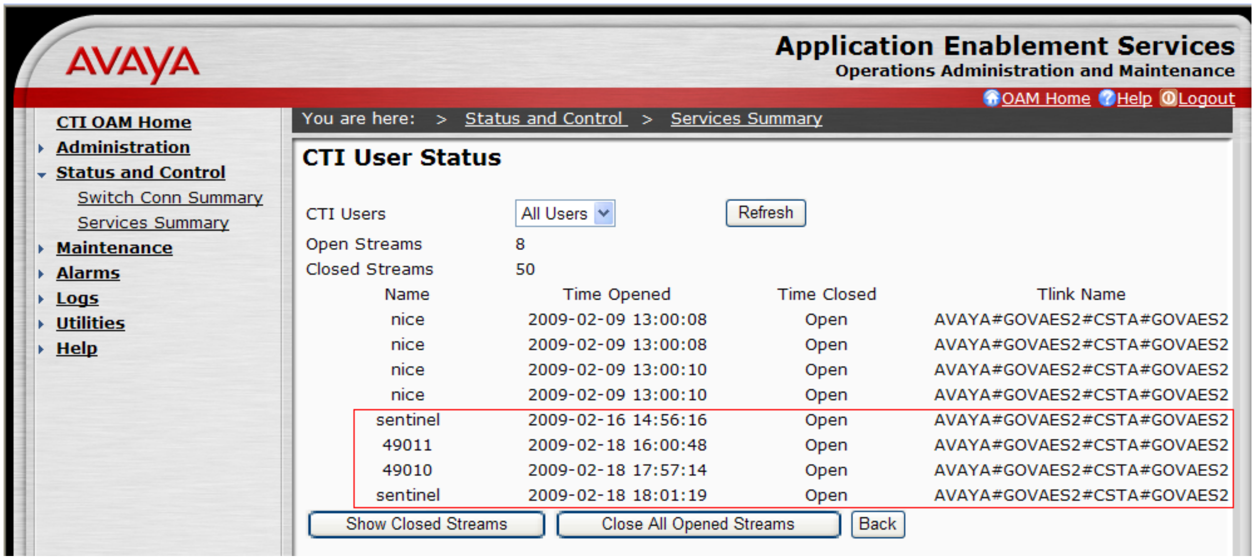
Verify the status of the **TSAPI link**.



TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
●	1	govaes2	2	Talking	2009-02-02 16:12:55.0	Online	15	15	1215

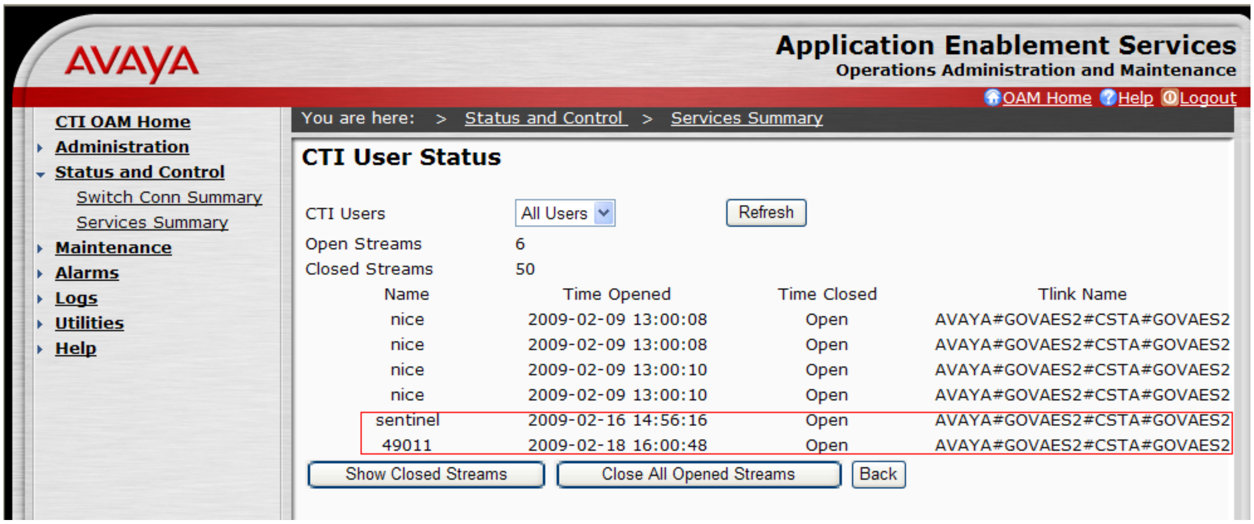
Verify the user status by selecting **User Status** on the bottom of the TSAPI Link Details screen. Initially there will be four CTI User listed. After the timers expire, only two CTI Users will be shown on this screen.



CTI User Status

CTI Users: All Users
Open Streams: 8
Closed Streams: 50

Name	Time Opened	Time Closed	Tlink Name
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
sentinel	2009-02-16 14:56:16	Open	AVAYA#GOVAES2#CSTA#GOVAES2
49011	2009-02-18 16:00:48	Open	AVAYA#GOVAES2#CSTA#GOVAES2
49010	2009-02-18 17:57:14	Open	AVAYA#GOVAES2#CSTA#GOVAES2
sentinel	2009-02-18 18:01:19	Open	AVAYA#GOVAES2#CSTA#GOVAES2

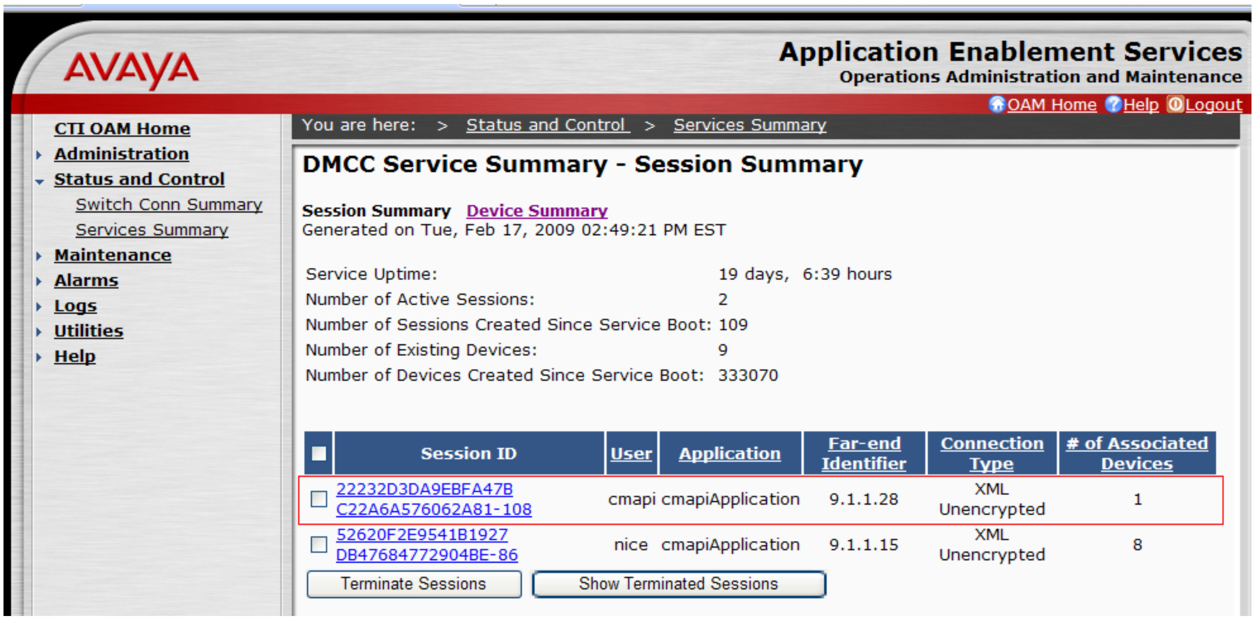


CTI User Status

CTI Users: All Users
Open Streams: 6
Closed Streams: 50

Name	Time Opened	Time Closed	Tlink Name
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:08	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
nice	2009-02-09 13:00:10	Open	AVAYA#GOVAES2#CSTA#GOVAES2
sentinel	2009-02-16 14:56:16	Open	AVAYA#GOVAES2#CSTA#GOVAES2
49011	2009-02-18 16:00:48	Open	AVAYA#GOVAES2#CSTA#GOVAES2

Verify the status of the **DMCC Service**.

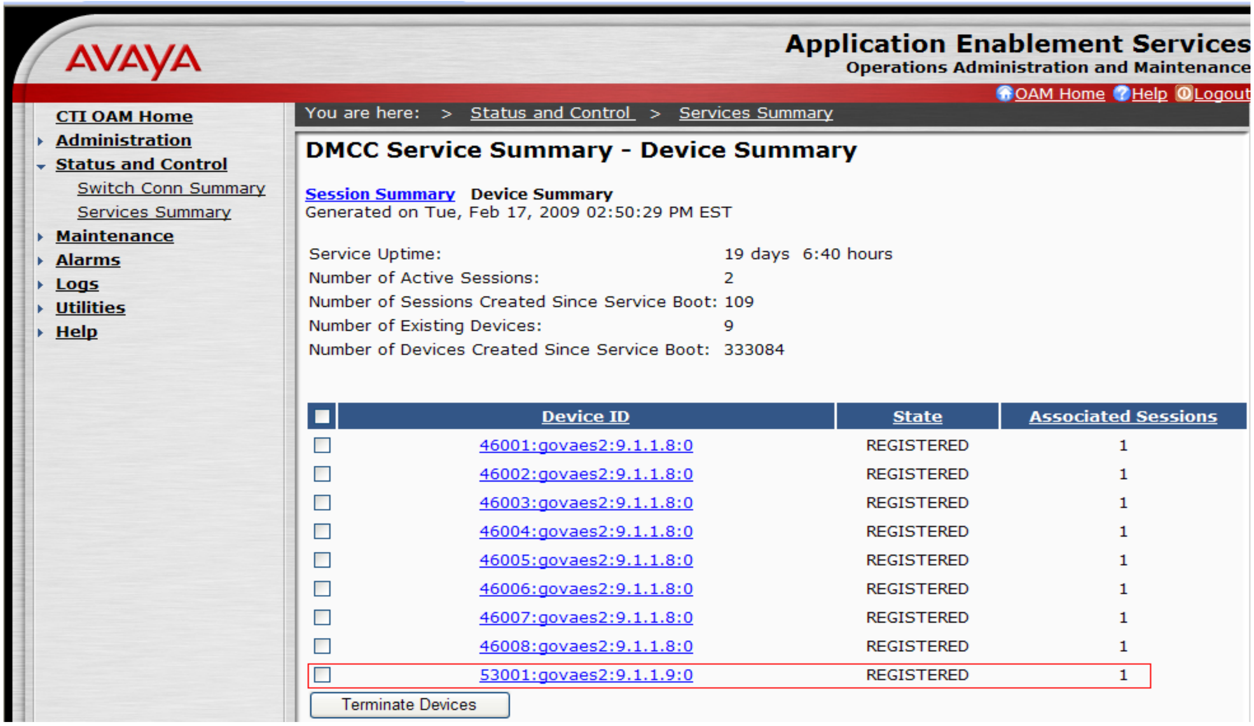


DMCC Service Summary - Session Summary

Session Summary Device Summary
Generated on Tue, Feb 17, 2009 02:49:21 PM EST

```
Service Uptime:                              19 days,  6:39 hours
Number of Active Sessions:                   2
Number of Sessions Created Since Service Boot: 109
Number of Existing Devices:                  9
Number of Devices Created Since Service Boot:  333070
```

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	22232D3DA9EBFA47B C22A6A576062A81-108	cmapi	cmapiApplication	9.1.1.28	XML Unencrypted	1
□	52620F2E9541B1927 DB47684772904BE-86	nice	cmapiApplication	9.1.1.15	XML Unencrypted	8



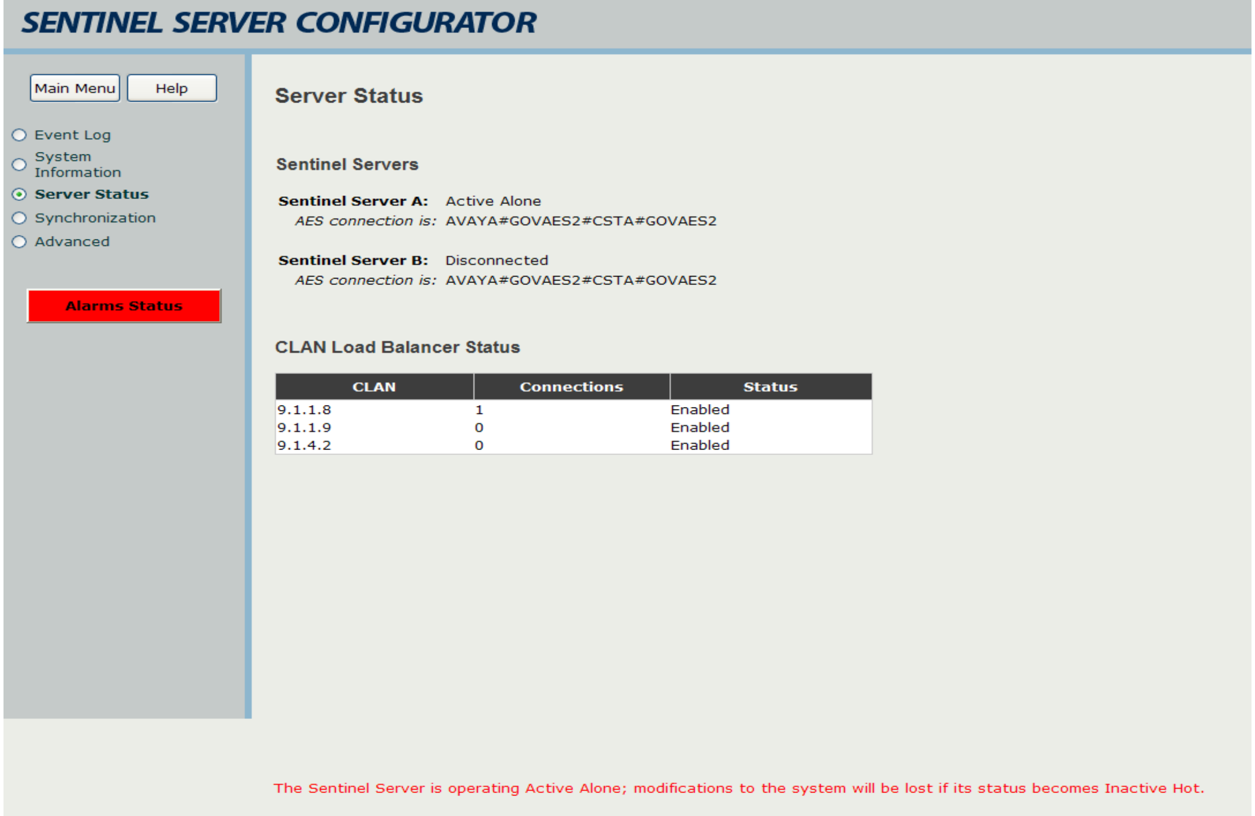
DMCC Service Summary - Device Summary

Session Summary **Device Summary**
Generated on Tue, Feb 17, 2009 02:50:29 PM EST

```
Service Uptime:                              19 days  6:40 hours
Number of Active Sessions:                   2
Number of Sessions Created Since Service Boot: 109
Number of Existing Devices:                  9
Number of Devices Created Since Service Boot:  333084
```

■	Device ID	State	Associated Sessions
□	46001:govaes2:9.1.1.8:0	REGISTERED	1
□	46002:govaes2:9.1.1.8:0	REGISTERED	1
□	46003:govaes2:9.1.1.8:0	REGISTERED	1
□	46004:govaes2:9.1.1.8:0	REGISTERED	1
□	46005:govaes2:9.1.1.8:0	REGISTERED	1
□	46006:govaes2:9.1.1.8:0	REGISTERED	1
□	46007:govaes2:9.1.1.8:0	REGISTERED	1
□	46008:govaes2:9.1.1.8:0	REGISTERED	1
□	53001:govaes2:9.1.1.9:0	REGISTERED	1

Login the Sentinel Server A and navigate to **Main Menu → Maintenance**. Select **Server Status** from the left side. The Alarms Status will be RED. In addition, there will be a message indicating that the Sentinel Server is operating Active Alone.



Server Status

Sentinel Servers

Sentinel Server A: Active Alone
AES connection is: AVAYA#GOVAES2#CSTA#GOVAES2

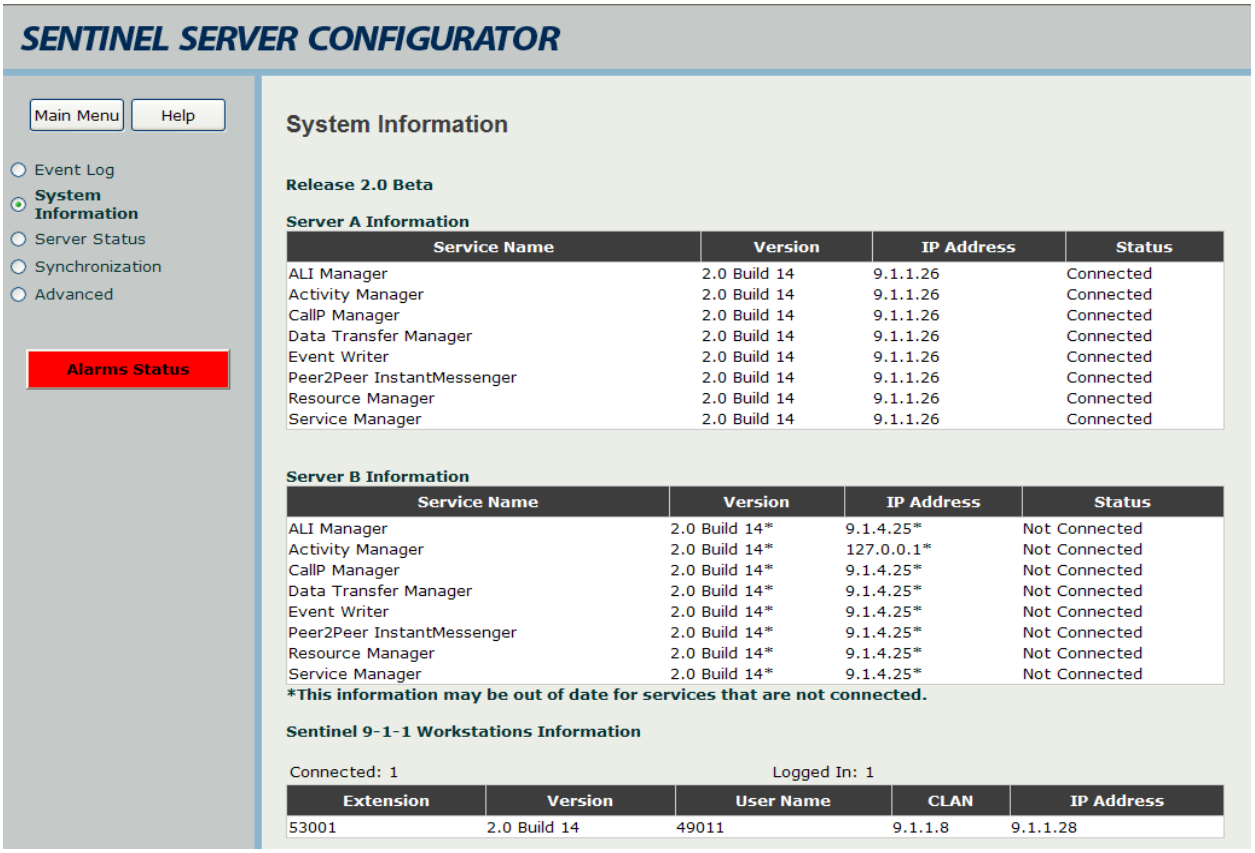
Sentinel Server B: Disconnected
AES connection is: AVAYA#GOVAES2#CSTA#GOVAES2

CLAN Load Balancer Status

CLAN	Connections	Status
9.1.1.8	1	Enabled
9.1.1.9	0	Enabled
9.1.4.2	0	Enabled

The Sentinel Server is operating Active Alone; modifications to the system will be lost if its status becomes Inactive Hot.

Navigate to **Main Menu → Maintenance**. Select **System Information** from the left side.



System Information

Release 2.0 Beta

Server A Information

Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 14	9.1.1.26	Connected
Activity Manager	2.0 Build 14	9.1.1.26	Connected
CallP Manager	2.0 Build 14	9.1.1.26	Connected
Data Transfer Manager	2.0 Build 14	9.1.1.26	Connected
Event Writer	2.0 Build 14	9.1.1.26	Connected
Peer2Peer InstantMessenger	2.0 Build 14	9.1.1.26	Connected
Resource Manager	2.0 Build 14	9.1.1.26	Connected
Service Manager	2.0 Build 14	9.1.1.26	Connected

Server B Information

Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 14*	9.1.4.25*	Not Connected
Activity Manager	2.0 Build 14*	127.0.0.1*	Not Connected
CallP Manager	2.0 Build 14*	9.1.4.25*	Not Connected
Data Transfer Manager	2.0 Build 14*	9.1.4.25*	Not Connected
Event Writer	2.0 Build 14*	9.1.4.25*	Not Connected
Peer2Peer InstantMessenger	2.0 Build 14*	9.1.4.25*	Not Connected
Resource Manager	2.0 Build 14*	9.1.4.25*	Not Connected
Service Manager	2.0 Build 14*	9.1.4.25*	Not Connected

*This information may be out of date for services that are not connected.

Sentinel 9-1-1 Workstations Information

Connected: 1 Logged In: 1

Extension	Version	User Name	CLAN	IP Address
53001	2.0 Build 14	49011	9.1.1.8	9.1.1.28

9.2.2. Remote PSAP Site

On Avaya Communication Manager at the Remote PSAP Site, verify the status of the AE Services server by using the "change ip-services" command. Perform these commands on the LSP server.

```
change ip-services                                            Page   4 of   4
                            AE Services Administration

   Server ID     AE Services         Password          Enabled     Status
                    Server
      1:       govaes1                                    y         in use
      2:       govaes2                                    y         idle
```

Verify the status of the CTI links by using the "status aesvcs cti-link" command.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs      Msgs
Link           Busy  Server           State         Sent      Rcvd

1     4        no    govaes1          established   250       251
2              no                     down          0         0
```

Verify the status of the AES links by using the “status aesvcs link” command.

```
status aesvcs interface

                          AE SERVICES INTERFACE STATUS

Local Node        Enabled?  Number of     Status
                            Connections

procr             yes       1             listening
CLAN-01B02        yes       0             intfce-down
```

```
status aesvcs link

                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

01/01  govaes1           9.  1.  4. 52  43077   procr           267     495
```

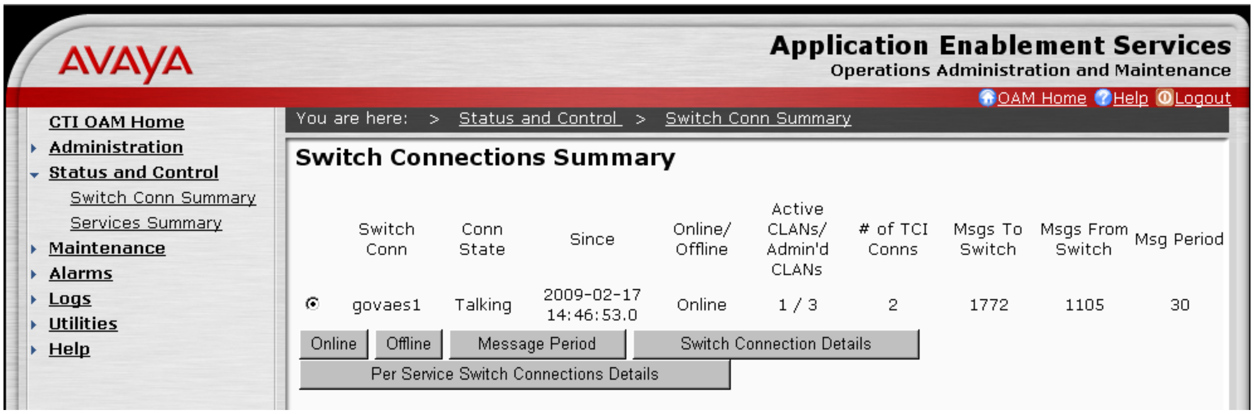
Verify the status of the agent registration by using the “list registered-ip-stations” command. Verify that there are two entries for each station, one for IP station and another for PlantCML Sentinel 9-1-1 application.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext/  Set     Product    Prod   Station          Net Gatekeeper     TCP
 Orig Port    Type    ID         Rel    IP Address       Rgn IP Address     Skt
49500         4620    IP_Phone   2.8000 9.1.4.155        4   9.1.4.2         y
49500         4620    IP_API_A   3.2040 9.1.4.52         4   9.1.4.2         y
```

Verify the agent status by using the “list agentID” command.

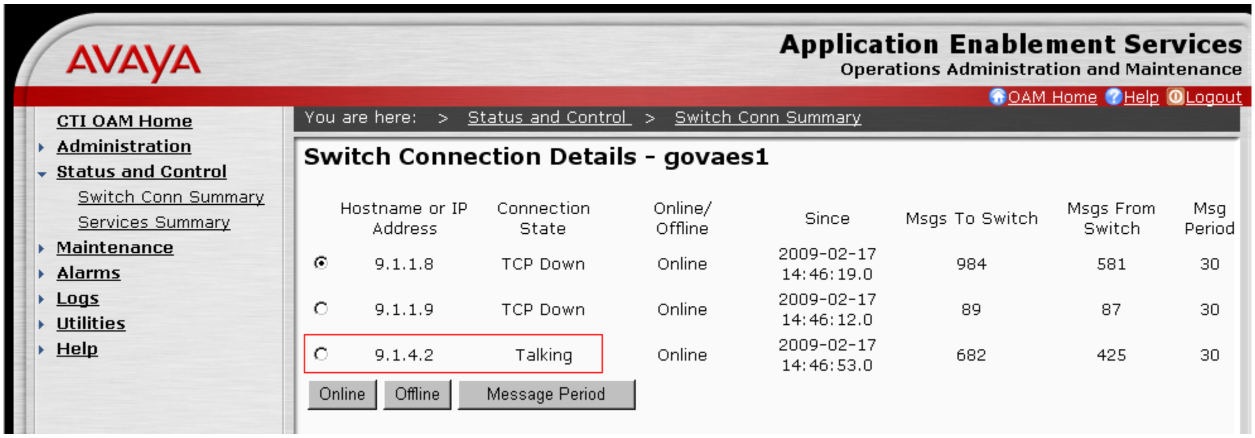
```
list agent-loginID                                                      Page   1

                               AGENT LOGINID

Login         Name/           Dir Agt COR Ag SO Skil/Lv Skil/Lv Skil/Lv Skil/Lv
ID            Extension       AAS/AUD     Pr
49010         PlantCML Agent1         1   lvl n   15/01   16/01     /       /
              49500                                 /       /       /       /
```

On Avaya AES, verify the status of the **switch connection**.


AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home
Help
Logout
CTI OAM Home
Administration
Status and Control
Switch Conn Summary
Services Summary
Maintenance
Alarms
Logs
Utilities
Help
You are here: > Status and Control > Switch Conn Summary
Online
Offline
Message Period
Switch Connection Details
Per Service Switch Connections Details

Switch Connections Summary

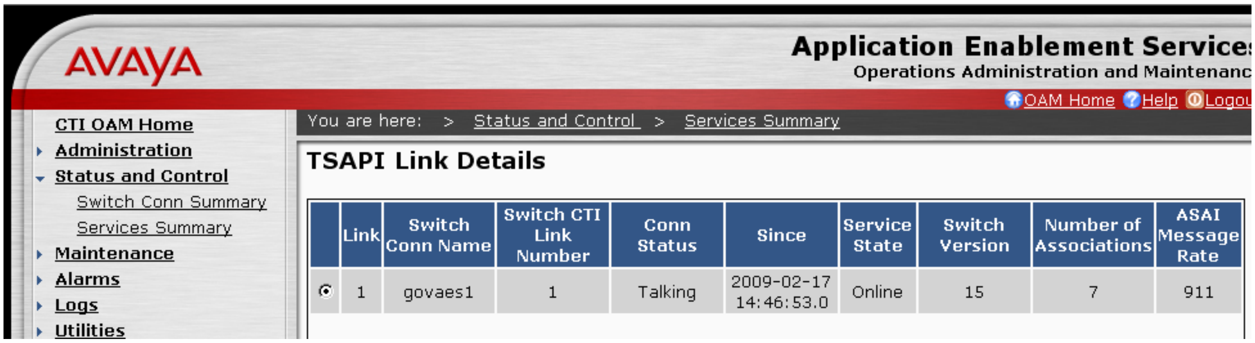
	Switch Conn	Conn State	Since	Online/ Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
●	govaes1	Talking	2009-02-17 14:46:53.0	Online	1 / 3	2	1772	1105	30



Switch Connection Details - govaes1

	Hostname or IP Address	Connection State	Online/ Offline	Since	Msgs To Switch	Msgs From Switch	Msg Period
●	9.1.1.8	TCP Down	Online	2009-02-17 14:46:19.0	984	581	30
○	9.1.1.9	TCP Down	Online	2009-02-17 14:46:12.0	89	87	30
○	9.1.4.2	Talking	Online	2009-02-17 14:46:53.0	682	425	30

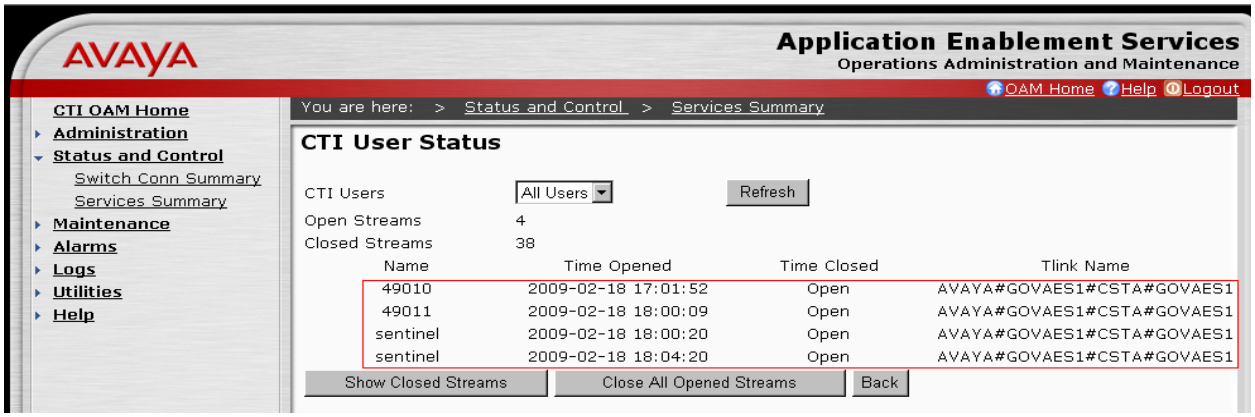
Verify the status of the **TSAPI link**.



TSAPI Link Details

	Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
●	1	govaes1	1	Talking	2009-02-17 14:46:53.0	Online	15	7	911

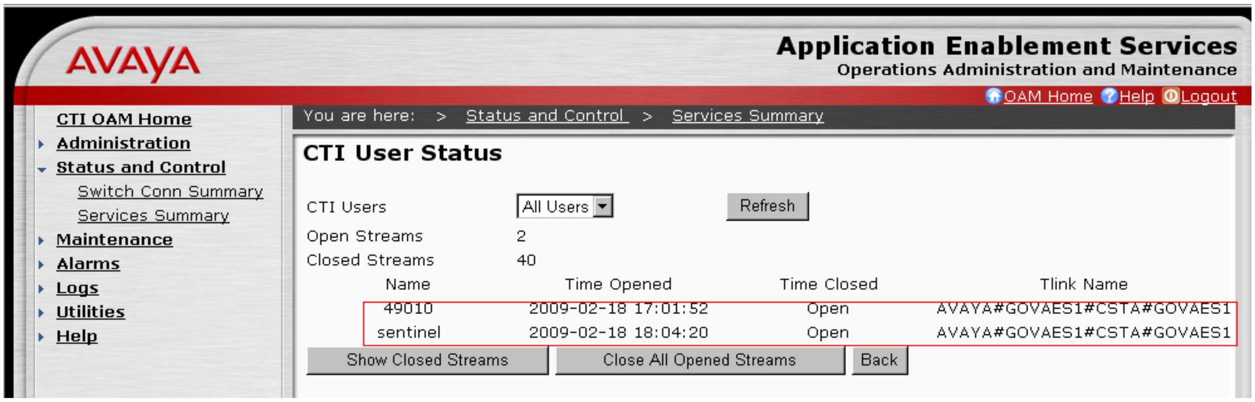
Verify the user status by selecting **User Status** on the bottom of the TSAPI Link Details screen. Initially there will be four CTI User listed. After the timers expire, only two CTI Users will be shown on this screen.



CTI User Status

CTI Users: All Users
Open Streams: 4
Closed Streams: 38

Name	Time Opened	Time Closed	Tlink Name
49010	2009-02-18 17:01:52	Open	AVAYA#GOVAES1#CSTA#GOVAES1
49011	2009-02-18 18:00:09	Open	AVAYA#GOVAES1#CSTA#GOVAES1
sentinel	2009-02-18 18:00:20	Open	AVAYA#GOVAES1#CSTA#GOVAES1
sentinel	2009-02-18 18:04:20	Open	AVAYA#GOVAES1#CSTA#GOVAES1

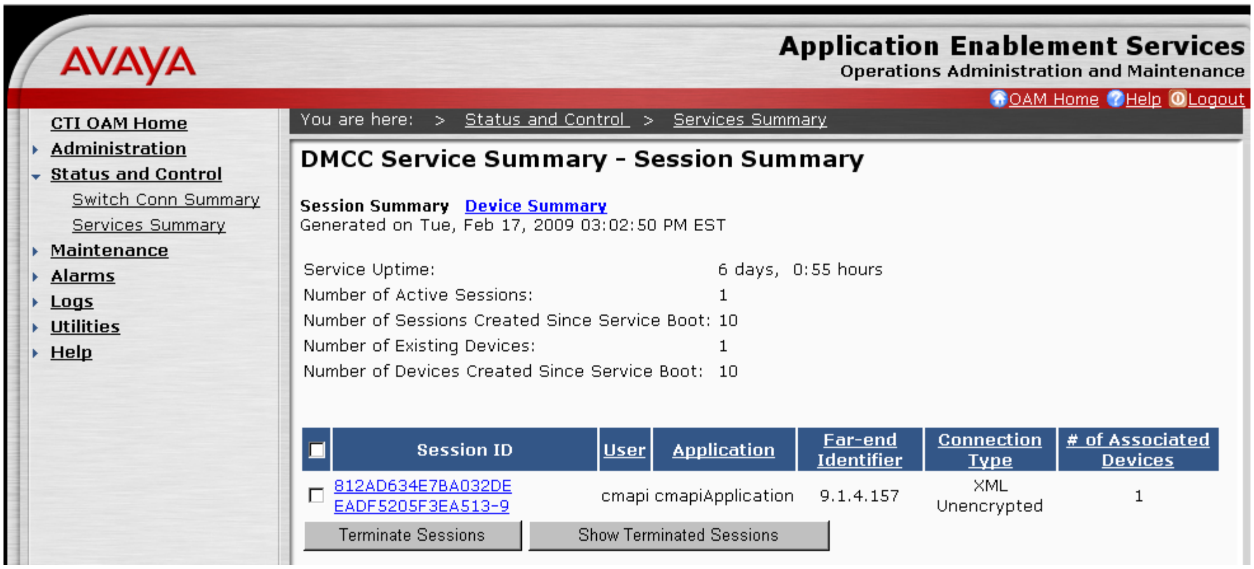


CTI User Status

CTI Users: All Users
Open Streams: 2
Closed Streams: 40

Name	Time Opened	Time Closed	Tlink Name
49010	2009-02-18 17:01:52	Open	AVAYA#GOVAES1#CSTA#GOVAES1
sentinel	2009-02-18 18:04:20	Open	AVAYA#GOVAES1#CSTA#GOVAES1

Verify the status of the **DMCC Service**.



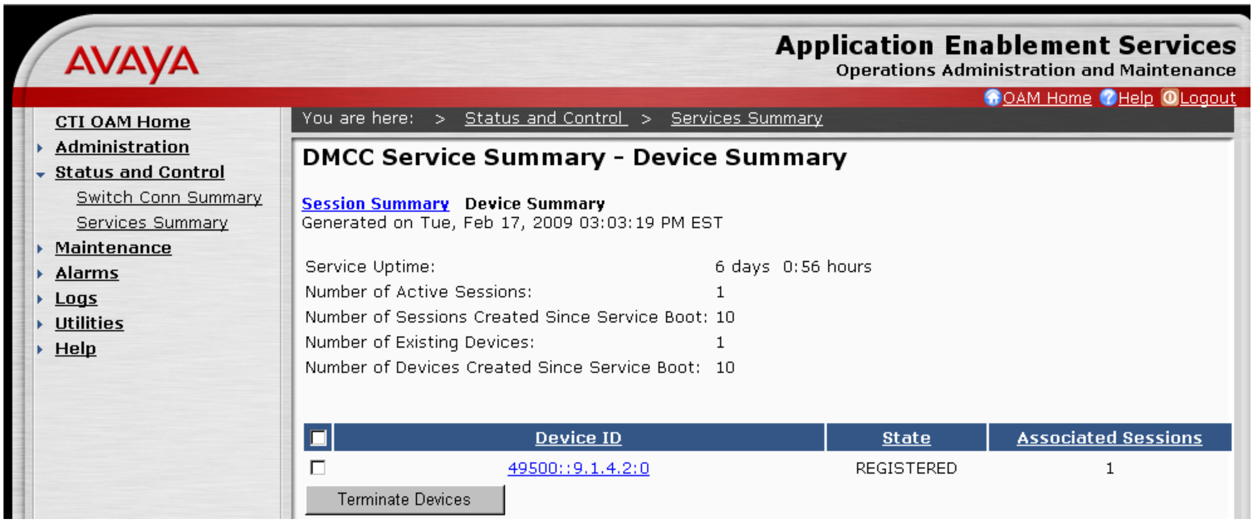
You are here: > Status and Control > Services Summary

DMCC Service Summary - Session Summary

Session Summary Device Summary
Generated on Tue, Feb 17, 2009 03:02:50 PM EST

```
Service Uptime:                              6 days,  0:55 hours
Number of Active Sessions:                   1
Number of Sessions Created Since Service Boot: 10
Number of Existing Devices:                  1
Number of Devices Created Since Service Boot:  10
```

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	812AD634E7BA032DE EADF5205F3EA513-9	cmapi	cmapiApplication	9.1.4.157	XML Unencrypted	1



You are here: > Status and Control > Services Summary

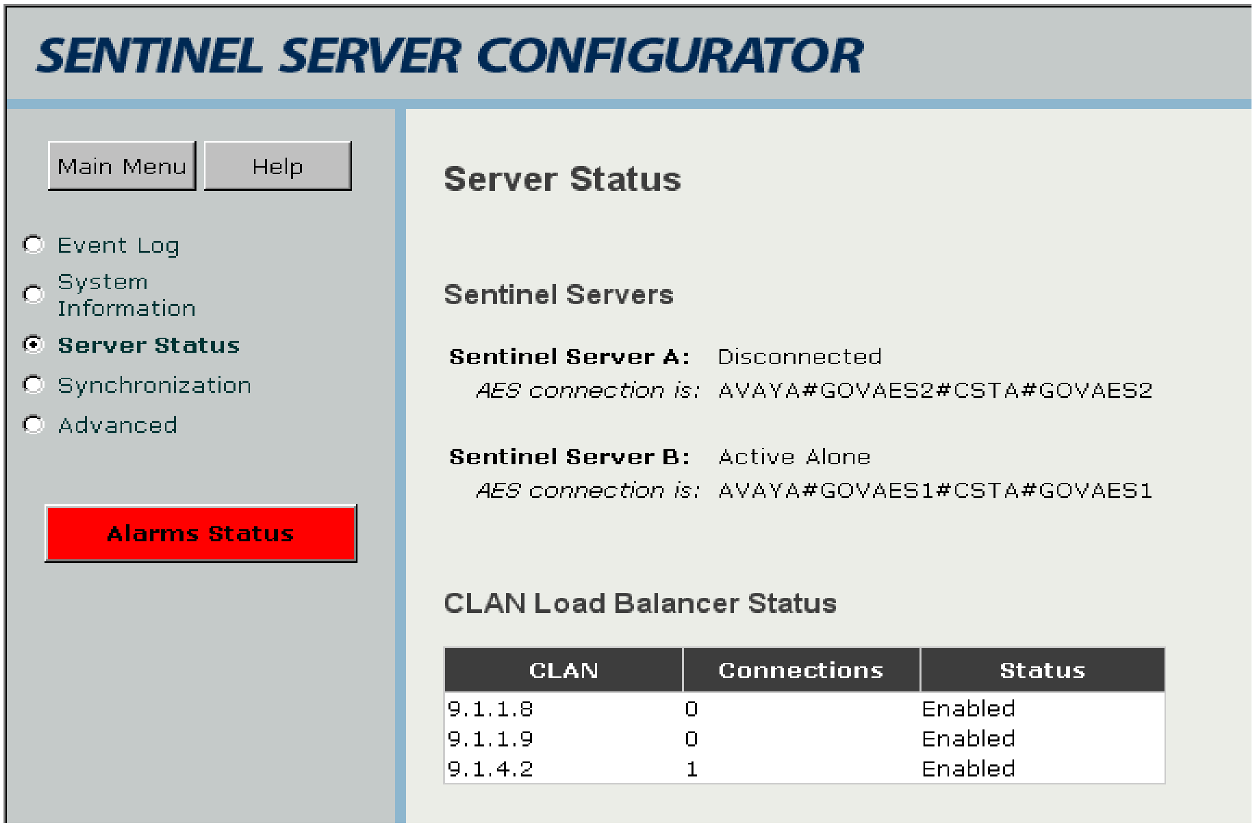
DMCC Service Summary - Device Summary

Session Summary Device Summary
Generated on Tue, Feb 17, 2009 03:03:19 PM EST

```
Service Uptime:                              6 days  0:56 hours
Number of Active Sessions:                   1
Number of Sessions Created Since Service Boot: 10
Number of Existing Devices:                  1
Number of Devices Created Since Service Boot:  10
```

□	Device ID	State	Associated Sessions
□	49500::9.1.4.2:0	REGISTERED	1

Login the Sentinel Server B and navigate to **Main Menu → Maintenance**. Select **Server Status** from the left side. The Alarms Status will be RED. In addition, there will be a message indicating that the Sentinel Server is operating Active Alone.



Server Status

Sentinel Servers

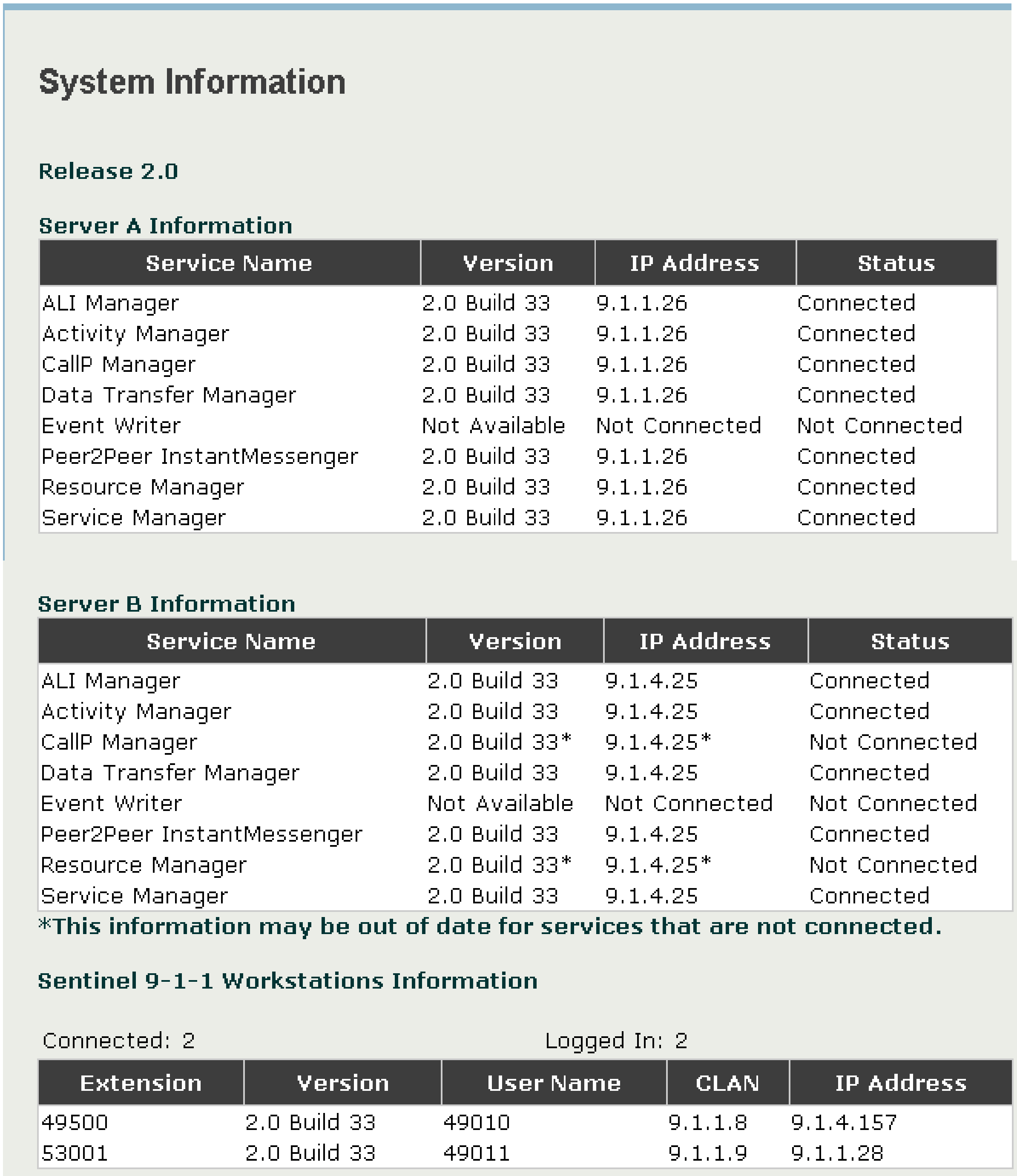
Sentinel Server A: Disconnected
AES connection is: AVAYA#GOVAES2#CSTA#GOVAES2

Sentinel Server B: Active Alone
AES connection is: AVAYA#GOVAES1#CSTA#GOVAES1

CLAN Load Balancer Status

CLAN	Connections	Status
9.1.1.8	0	Enabled
9.1.1.9	0	Enabled
9.1.4.2	1	Enabled

Navigate to **Main Menu → Maintenance**. Select **System Information** from the left side.



System Information

Release 2.0

Server A Information

Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 33	9.1.1.26	Connected
Activity Manager	2.0 Build 33	9.1.1.26	Connected
CallP Manager	2.0 Build 33	9.1.1.26	Connected
Data Transfer Manager	2.0 Build 33	9.1.1.26	Connected
Event Writer	Not Available	Not Connected	Not Connected
Peer2Peer InstantMessenger	2.0 Build 33	9.1.1.26	Connected
Resource Manager	2.0 Build 33	9.1.1.26	Connected
Service Manager	2.0 Build 33	9.1.1.26	Connected

Server B Information

Service Name	Version	IP Address	Status
ALI Manager	2.0 Build 33	9.1.4.25	Connected
Activity Manager	2.0 Build 33	9.1.4.25	Connected
CallP Manager	2.0 Build 33*	9.1.4.25*	Not Connected
Data Transfer Manager	2.0 Build 33	9.1.4.25	Connected
Event Writer	Not Available	Not Connected	Not Connected
Peer2Peer InstantMessenger	2.0 Build 33	9.1.4.25	Connected
Resource Manager	2.0 Build 33*	9.1.4.25*	Not Connected
Service Manager	2.0 Build 33	9.1.4.25	Connected

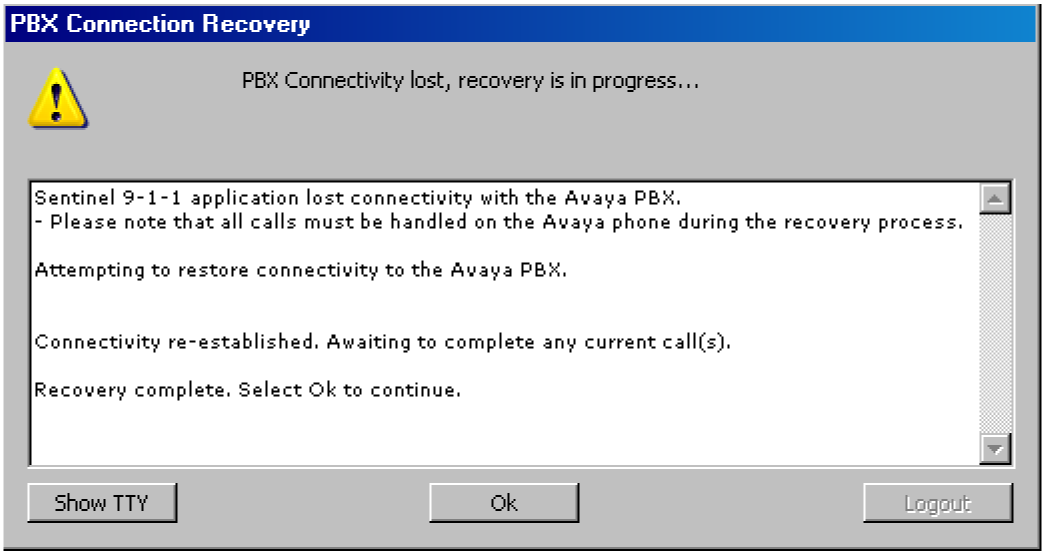
***This information may be out of date for services that are not connected.**

Sentinel 9-1-1 Workstations Information

Connected: 2 Logged In: 2

Extension	Version	User Name	CLAN	IP Address
49500	2.0 Build 33	49010	9.1.1.8	9.1.4.157
53001	2.0 Build 33	49011	9.1.1.9	9.1.1.28

The Sentinel Client on the Remote PSAP Site will see the following error message.



Sentinel 9-1-1 application lost connectivity with the Avaya PBX.
- Please note that all calls must be handled on the Avaya phone during the recovery process.

Attempting to restore connectivity to the Avaya PBX.

Connectivity re-established. Awaiting to complete any current call(s).

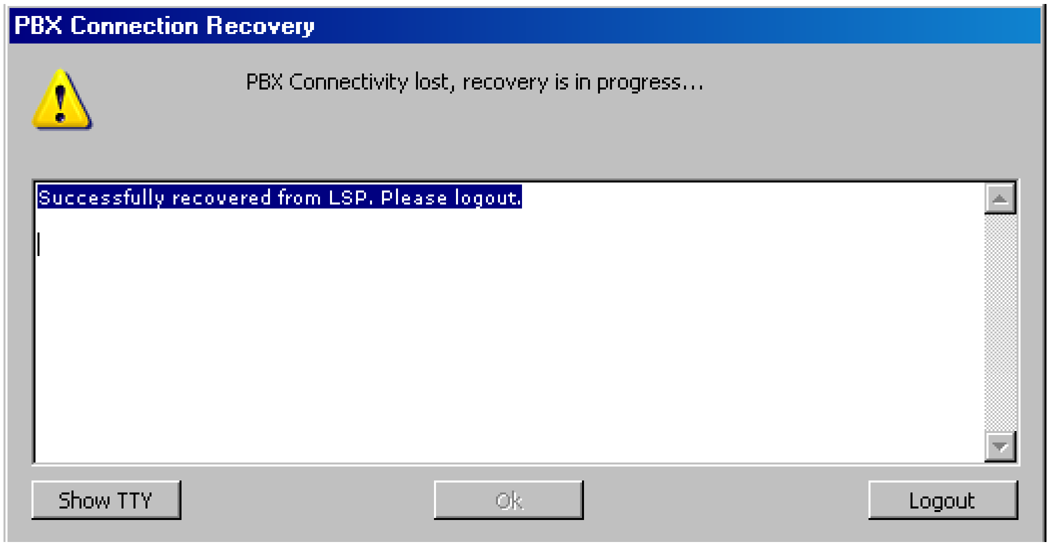
Recovery complete. Select Ok to continue.

Click OK and the agent should be able to proceed

9.3. Recovery from WAN Failure

When the connectivity to the main servers is back up, the Remote Site AES server will switch back to the administered C-LANs on the Main Site G650 Media Gateways. The verification steps described in **Section 9.1** will apply.

All Sentinel clients at both the Main and Remote Sites will see the following error message and will have to log back into the Sentinel Application.



Successfully recovered from LSP. Please logout.

10. Terminology

AES	Avaya Application Enablement Services
ALI	Automatic Location Information
ANI	Automatic Number Identification
CAMA	Centralized Automated Message Accounting
DMCC	Device, Media and Call Control
IWS	Intelligent Workstation
NENA	National Emergency Number Association
PSAP	Public Safety Answering Point
SES	SIP Enablement Services
TSAPI	Telephony Services Application Programming Interface

11. Conclusion

These Application Notes describe the configuration steps required for PlantCML Sentinel to successfully interoperate with Avaya Communication Manager Release 5.0 and Avaya Application Enablement Services Release 4.2.1.

12. Additional References

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

1. *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 2, January 2008, available at http://support.avaya.com.

2. *Avaya Application Enablement Services 4.1 Administration and Maintenance Guide*, Document ID 02-300357, Issue 1, January 2008, available at http://support.avaya.com.

3. *Avaya Communication Manager Guide to ACD Call Centers*, Document ID 07-6025685, Issue 1, January 2008, available at http://support.avaya.com

4. *Sentinel CM – Operations and Maintenance Guide,* Issue 1.0, September 2008, available at http://www.peinc.com

5. *Application Notes for PlantCML Sentinel CM Release 2.0 with Avaya Communication Manager and Avaya Application Enablement Services Release 4.2.*

6. *Configuring NICE Call Recording System – CLS 8.90.4 and VoIP Logger 9.10.5 with Avaya Application Enablement Services Release 4.2 and Avaya Communication Manager.*

7. *Application Notes for Raytheon JPS ACU-2000IP with Avaya Communication Manager and Avaya SIP Enablement Services Release 5.1.*

8. *Configuring Avaya Media Server as Local Survivable Processor for Avaya Media Gateways and Standard Local Survivability on Avaya G250 Media Gateways.*

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.