



Avaya Solution & Interoperability Test Lab

Application Notes for PlantCML Sentinel CM with Avaya Communication Manager 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 Communication Manager using Avaya Application Enablement Services. The PlantCML Sentinel CM is an integral part of the Avaya Public Safety Communication Solution. These Application Notes also present a sample configuration for a public safety environment.

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.....	4
1.1.	Public Safety Solution Overview	4
1.2.	Interoperability Compliance Testing	6
1.3.	Support.....	6
1.4.	PlantCML Sentinel CM Overview.....	6
2.	Network Topology	9
3.	Equipment and Software Validated.....	11
4.	Configure Avaya Communication Manager.....	11
4.1.	Verify Avaya Communication Manager License	12
4.2.	Administer IP Node Name for C-LAN.....	13
4.3.	Administer IP Interface for C-LAN.....	14
4.4.	Administer Data Module for C-LAN.....	15
4.5.	Administer IP Services for AES Transport Link	15
4.6.	Administer CTI Link for TSAPI Service	16
4.7.	Administer Physical Stations.....	17
4.8.	Administer System Parameters	19
4.9.	Administer Feature Access Codes	19
4.10.	Administer Hunt Group and Skill group	20
4.11.	Administer Agent LoginIDs.....	21
4.12.	Administer Vector and VDNs.....	22
4.13.	System-Parameter Features	23
4.14.	Create Login for PlantCML	23
5.	Configure Avaya Application Enablement Services.....	24
5.1.	Verify Avaya Application Enablement Services License	24
5.2.	Administer Local IP	26
5.3.	Administer Switch Connection	26
5.4.	Administer TSAPI Link.....	28
5.5.	Administer Security Database	29
5.6.	Obtain Tlink Name.....	30
5.7.	Administer Sentinel Users	31
5.8.	Administer Device Groups	34
5.9.	Restart TSAPI Service	36
5.10.	Administer Second AES Server	37
6.	Configure PlantCML Sentinel Server	37
6.1.	Administer Sentinel Server Configuration	38
6.2.	Launch Sentinel Server Configurator	39
6.3.	Administer Global Settings	39
6.4.	Restart CallP Manager	43
6.5.	Administer Sentinel Clients.....	44
6.6.	Verify Sentinel Accounts.....	45
6.7.	Selective Transfer Agencies Configuration.....	45
6.8.	Administer Trunks	46
7.	Configure PlantCML Sentinel 9-1-1 Clients	47
7.1.	Administer Physical Extension	47
7.2.	Log Into Logical Extension	51

7.3.	Administer User Configuration File	51
8.	General Test Approach and Test Results.....	52
9.	Verification	54
9.1.	Verify Avaya Communication Manager	54
9.2.	Verify Avaya Application Enablement Services	55
9.3.	Verify PlantCML Sentinel Server and Sentinel 9-1-1 Client.....	57
10.	Troubleshooting.....	59
10.1.	Sentinel 9-1-1 Cannot Login	59
10.2.	Incorrect User Name or Password	59
10.3.	PBX Connectivity lost.....	60
11.	Terminology	61
12.	Conclusion	61
13.	Additional References.....	61

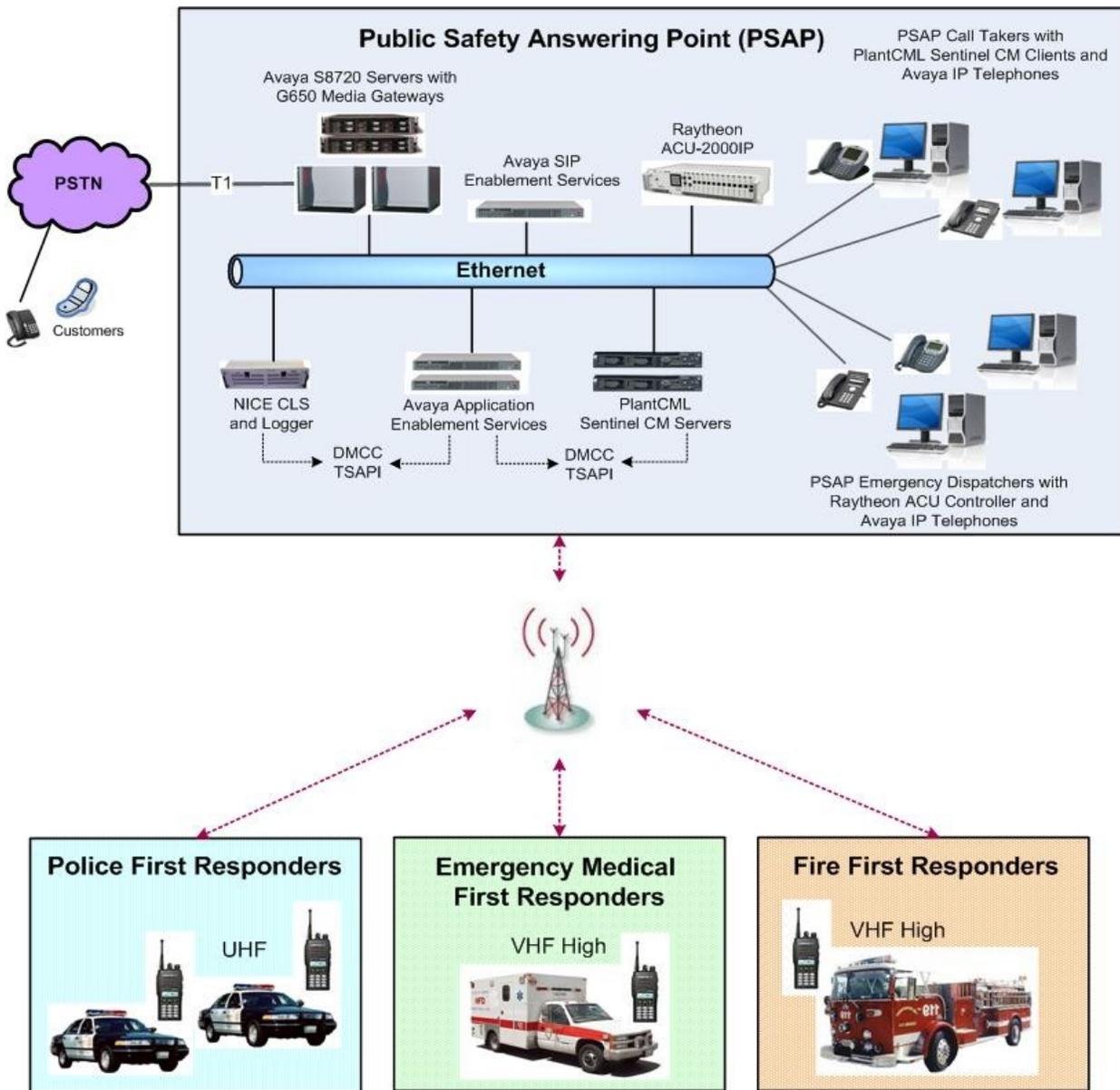
1. Introduction

These Application Notes describe the configuration steps required for the PlantCML Sentinel CM 911 incident management solution to successfully interoperate with Avaya Communication Manager using Avaya Application Enablement Services. The PlantCML Sentinel CM is an integral part of the Avaya Public Safety Solution. These Application Notes also present a sample configuration for a public safety environment.

1.1. Public Safety 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.



Solution and Interoperability Test Lab

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
- Busyout C-LANs and CTI links
- Server Redundancy and Fail-over of the PlantCML Sentinel servers
- Workstation Scenarios – PC fails

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 9-1-1 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.

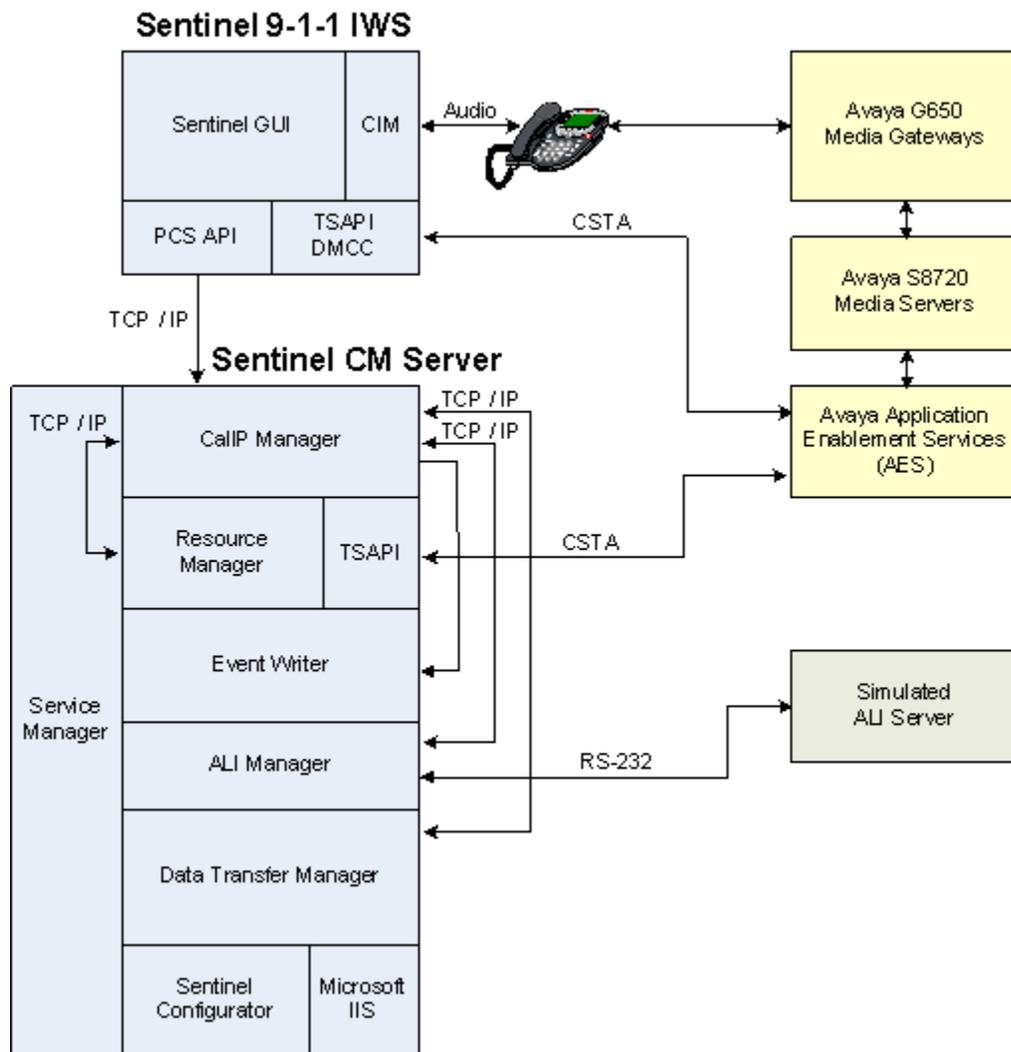
1.4.5. DMCC

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 backup 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

2. Network Topology

The network implemented for the reference configuration is shown in **Figure 2**. 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. The PSAP location also has NICE Call Recording System. Please refer [5] for configuration information related to NICE Call Recording System.

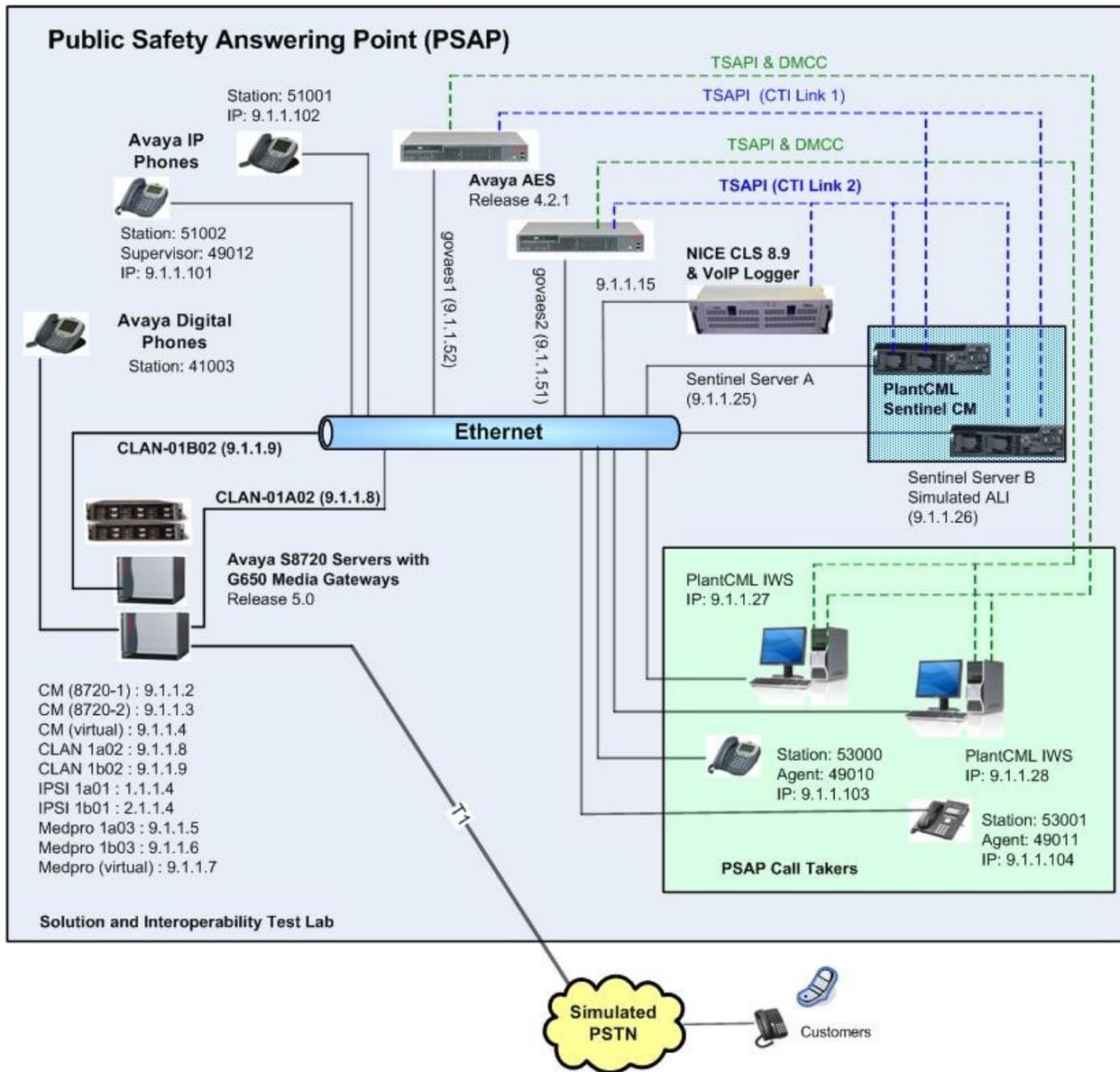


Figure 2: PlantCML Sentinel CM with Avaya Communication Manager and Avaya AES

Note: The sample configuration does not have duplicated LAN network. In customer deployments, duplicated LAN can be used. The PlantCML Sentinel CM servers can be on different LANs. The two servers need to have routable addresses.

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	Release 5.1.2 (R015x.01.2.416.4)
Avaya G650 Media Gateway - IPSI (TN2312BP) - CLAN (TN799DP) - MedPro (TN2602AP)	- HW15 FW044 - HW01 FW026 - HW02 FW044
Avaya AES	Release 4.2.1 (Build 20-5)
Avaya 4600 Series H.323 Telephones	R2.8
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 Build 33 Release 2 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 node name for C-LAN
- Administer IP interface for C-LAN
- Administer data module for C-LAN
- 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
- Create Login for PlantCML

As shown in **Figure 2**, two C-LAN modules, two AES servers, and two CTI links need to be administered.

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 Backup 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
ASAI Link Core Capabilities? y                DCS (Basic)? y
ASAI Link Plus Capabilities? y                DCS Call Coverage? 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
                                BCMS (Basic)? y
                                BCMS/VuStats Service Level? y
BSR Local Treatment for IP & ISDN? y Service Observing (Basic)? y
                                Business Advocate? y Service Observing (Remote/By FAC)? y
                                Call Work Codes? y Service Observing (VDNs)? y
DTMF Feedback Signals For VRU? y Timed ACW? y
                                Dynamic Advocate? y Vectoring (Basic)? y
                                Expert Agent Selection (EAS)? y Vectoring (Prompting)? 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. Administer IP Node Name for C-LAN

Enter the “change node-names ip” command, and add an entry for the C-LAN that will be used for connectivity to the AES server. For the PlantCML Sentinel CM application, two AES servers will be used. These two AES servers will use two C-LAN modules.

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

C-LAN	
Name	IP Address
CLAN-01A02	9.1.1.8
CLAN-01B02	9.1.1.9

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
Name           IP Address
AES1           9.1.1.50
CLAN-01A02    9.1.1.8
CLAN-01B02    9.1.1.9
CLAN-RETAIL   30.1.1.4
FCSWinsuite   9.1.1.203
GVT-S8300-LSP 9.1.4.2
MedPro-01A03  9.1.1.5
MedPro-01B07  9.1.1.6
RedSky1       9.1.1.55
RedSky2       9.1.1.56
S8500-ESS     9.1.1.13
SES1          9.1.1.34
VAL-01A12     9.1.1.12
clan-trade    5.1.1.4
default       0.0.0.0
govmas1       9.1.1.31
( 16 of 17 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

4.3. Administer IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface <board location>” command. In the sample configuration, “1a02” for CLAN-01A02 and “1b02” for CLAN-01B02” will be used. Note that the actual slot number may vary. Enter the C-LAN node name assigned from **Section 4.2** into the **Node Name** field. The **IP Address** field will be populated automatically.

Enter proper values for the **Subnet Mask** and **Gateway Address** fields. Set the **Enable Ethernet Port** field to “y”, and select the appropriate **Network Region** for the C-LAN dedicated for AES connectivity. Default values may be used in the remaining fields. For the sample configuration, Network Region 1 is used. Submit these changes.

Note two C-LAN modules need to be administered, one for each AES server.

```
add ip-interface 1a02                                     Page 1 of 1
                                                         IP INTERFACES

Type: C-LAN
Slot: 01A02
Code/Suffix: TN799 D
Node Name: CLAN-01A02
IP Address: 9 .1 .1 .8
Subnet Mask: 255.255.255.0                               Link: 1
Gateway Address: 9 .1 .1 .1
Enable Ethernet Port? y                                  Allow H.323 Endpoints? y
Network Region: 1                                       Allow H.248 Gateways? n
VLAN: n                                                  Gatekeeper Priority: 1

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                         ETHERNET OPTIONS
Auto? y
```

```
add ip-interface 1b02                                     Page 1 of 1
                                                         IP INTERFACES

Type: C-LAN
Slot: 01B02
Code/Suffix: TN799 D
Node Name: CLAN-01B02
IP Address: 9 .1 .1 .9
Subnet Mask: 255.255.255.0                               Link: 2
Gateway Address: 9 .1 .1 .1
Enable Ethernet Port? y                                  Allow H.323 Endpoints? y
Network Region: 1                                       Allow H.248 Gateways? n
VLAN: n                                                  Gatekeeper Priority: 1

Target socket load and Warning level: 400
Receive Buffer TCP Window Size: 8320
                                                         ETHERNET OPTIONS
Auto? y
```

4.4. Administer Data Module for C-LAN

Add a new data module using the “add data-module n” command, where “n” is an available extension for each C-LAN module. Enter the following values:

- **Name:** A descriptive name
- **Type:** “ethernet”
- **Port:** Same slot number from **Section 4.3**, suffixed with port “17”
- **Link:** An available link number

```
add data-module 40000
                                DATA MODULE

Data Extension: 40000           Name: CLAN-01A02
Type: ethernet
Port: 01A0217
Link: 1

Network uses 1's for Broadcast Addresses? Y
```

```
add data-module 49999
                                DATA MODULE

Data Extension: 49999           Name: CLAN-01B02
Type: ethernet
Port: 01b0217
Link: 2

Network uses 1's for Broadcast Addresses? Y
```

4.5. 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

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

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

- **AE Services Server:** Name obtained from the AES server.
- **Password:** Same 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 Server	Password	Enabled	Status
1:	govaes1	*	y	
2:	govaes2	*	y	
3:				

4.6. 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
```

4.7. 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, either on **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, two stations were administered as shown below.

```

list station 53000 count 2
                                                    STATIONS
Ext/      Port/      Name/      Room/      Cv1/  COR/      Cable/
Type      Hunt-to   Surv GK NN  Move      Data Ext  Cv2  COS      Jack

53000     S00192   PlantCML 46XX      no      1
          4620
53001     S00195   PlantCML 96xx      no      1
          9630

```

4.8. 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
```

4.9. 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
```

4.10. 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
```

4.11. 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, two 911 call answering agents were administered as shown below:

```
list agent-loginID 49010 count 2
```

AGENT LOGINID										
Login ID	Name/Extension	Dir AAS/AUD	Agt	COR	Ag Pr	SO	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
49010	PlantCML Agent1 unstaffed		1	lv1	n		15/01	16/01	/	/
49011	PlantCML Agent2 unstaffed		2	lv1	n		15/01	/	/	/

4.12. 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	
08	

4.13. 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	

4.14. 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**.

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The title bar indicates 'This Server: [2] sa-gvt-2 Duplicate Server: [1] sa-gvt-1'. The main heading is 'Administrator Accounts -- Add Login: Privileged Administrator'. Below the heading, a message states: '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.'

The form contains the following fields and options:

- Login name:
- Primary group:
- Additional groups (profile):
- Linux shell:
- Home directory:
- 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

At the bottom of the form are three buttons: **Submit**, **Cancel**, and **Help**.

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

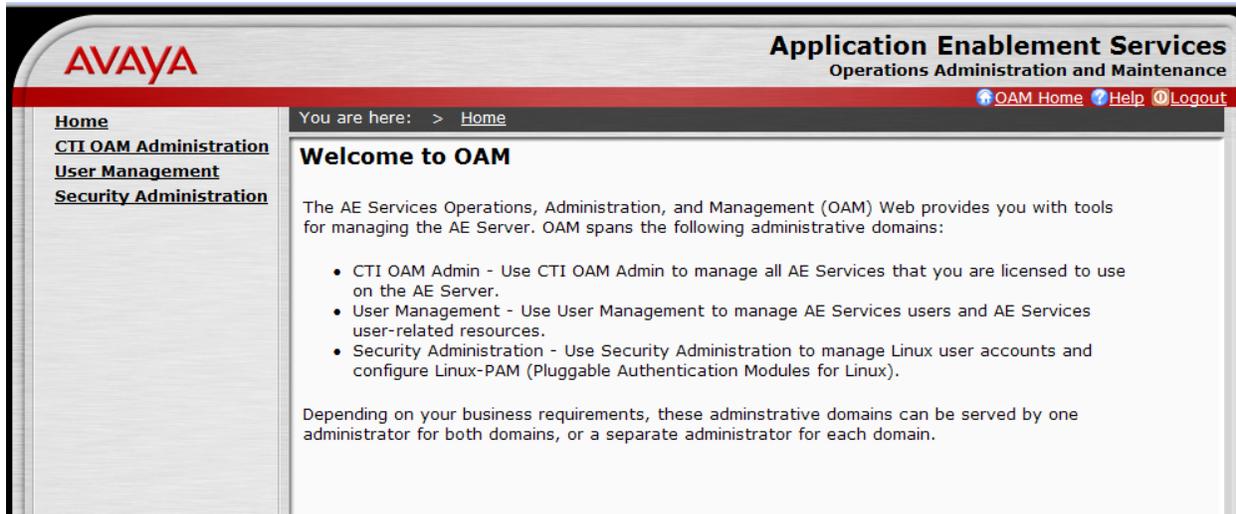
As shown in **Figure 2**, two AES servers need to be administered. Administration Steps described in **Section 5.1 to Section 5.9** should be followed for both AES servers.

5.1. Verify Avaya Application Enablement Services License

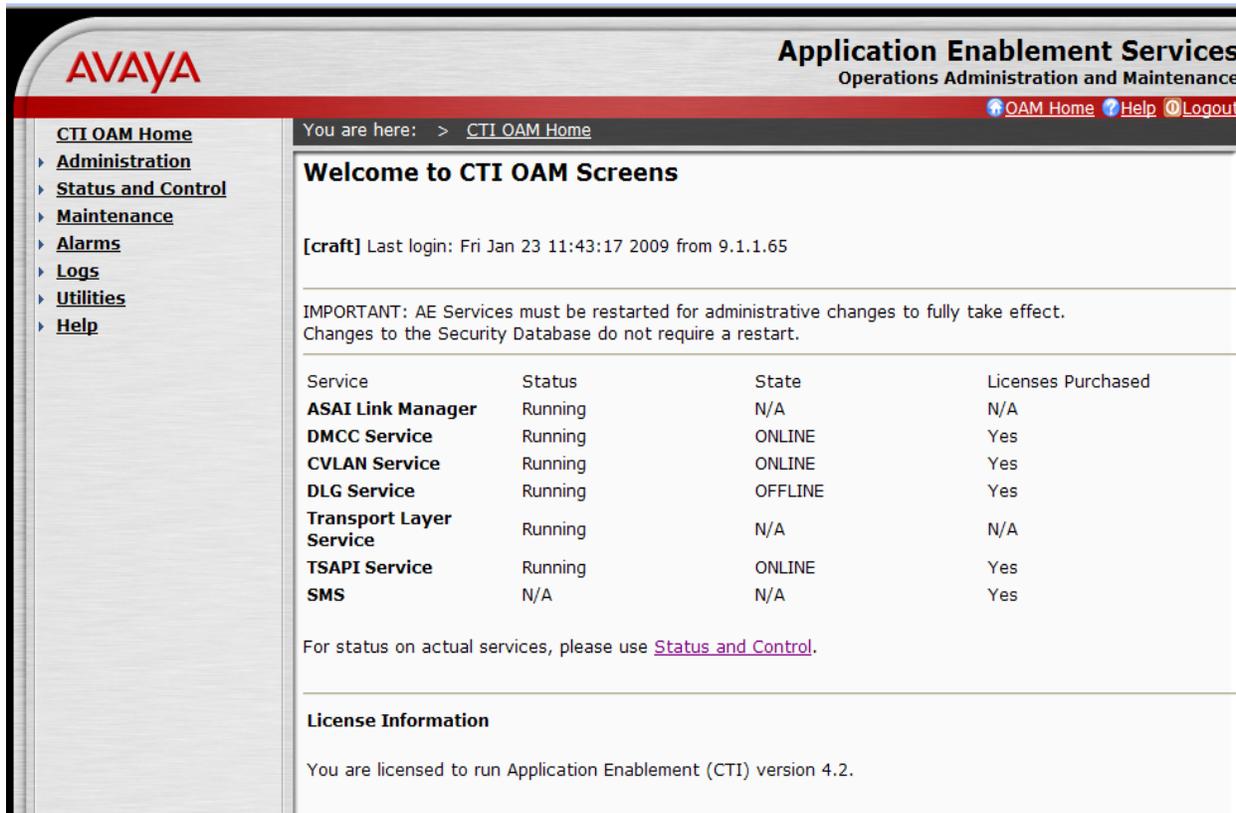
Access the AES OAM web based interface by using the URL “https://ip-address:8443/MVAP” in an Internet browser window, where “ip-address” is the IP address of the AES server. The **Login** screen is displayed as shown below. Note that the AES OAM includes two separate administrative accounts, one to access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



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

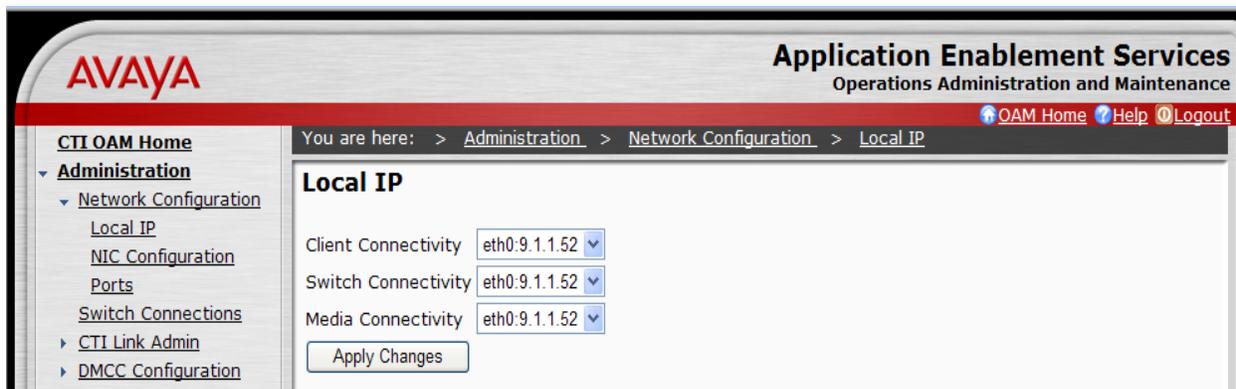


The **Welcome to CTI OAM Screens** is displayed. Verify that AES is licensed for the TSAPI service, as shown below. If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.



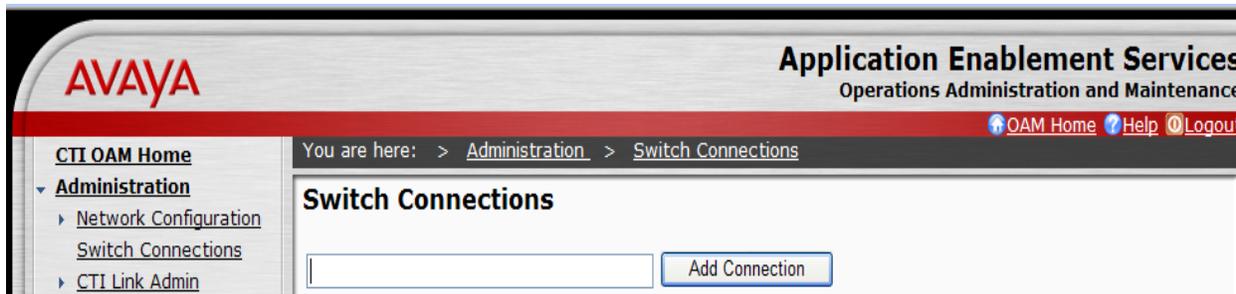
5.2. Administer Local IP

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**.



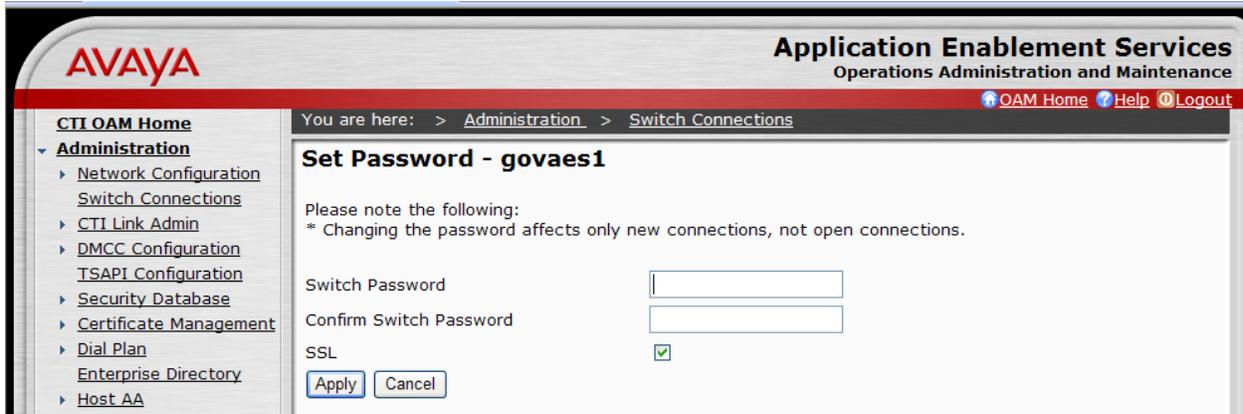
5.3. Administer Switch Connection

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, "govaes1" is used. Note that the actual switch connection name may vary.

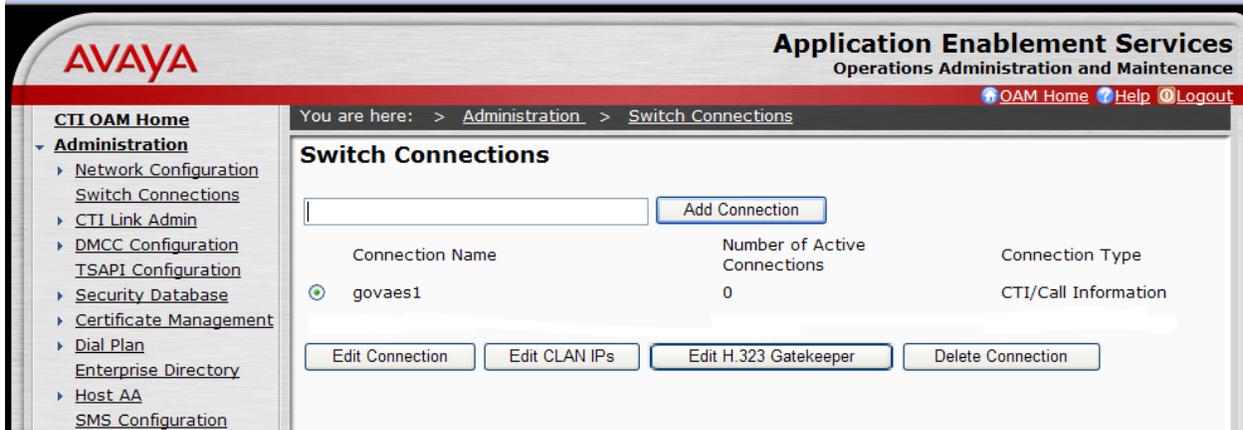


Next, the **Set Password – govaes1** screen is displayed. Enter the following values for the specified fields and click on **Apply**.

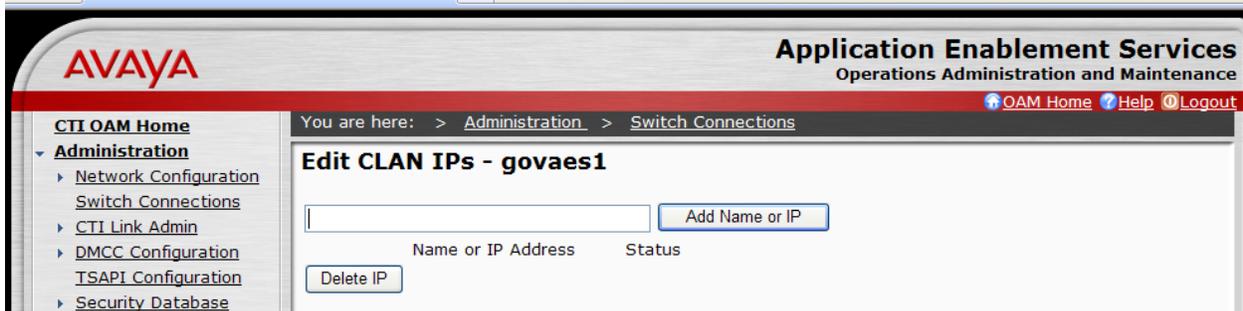
- **Switch Password:** Same password from **Section 4.5**.
- **Confirm Switch Password:** Re-enter the same password from **Section 4.5**.
- **SSL:** Retain the check.



The **Switch Connections** screen is displayed next, as shown below. Select the newly added switch connection name from the listing, and click on **Edit CLAN IPs**.

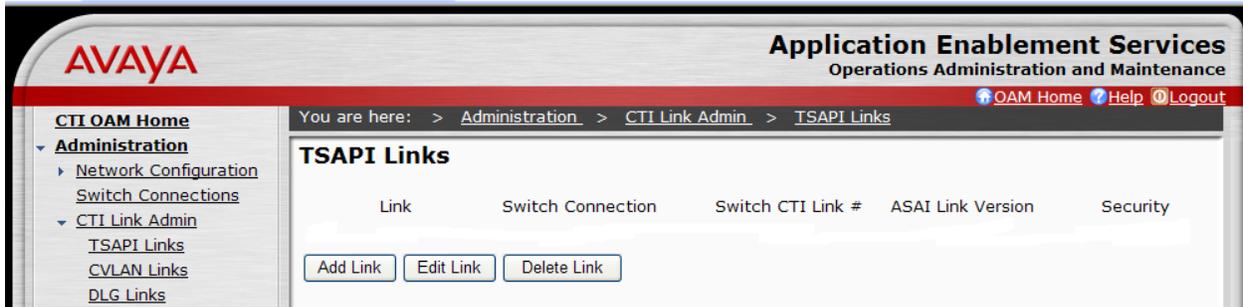


The **Edit CLAN IPs – govaes1** screen is displayed next. Enter the host name or IP address of the C-LAN used for AES connectivity from **Section 4.2**. Click on **Add Name or IP**.

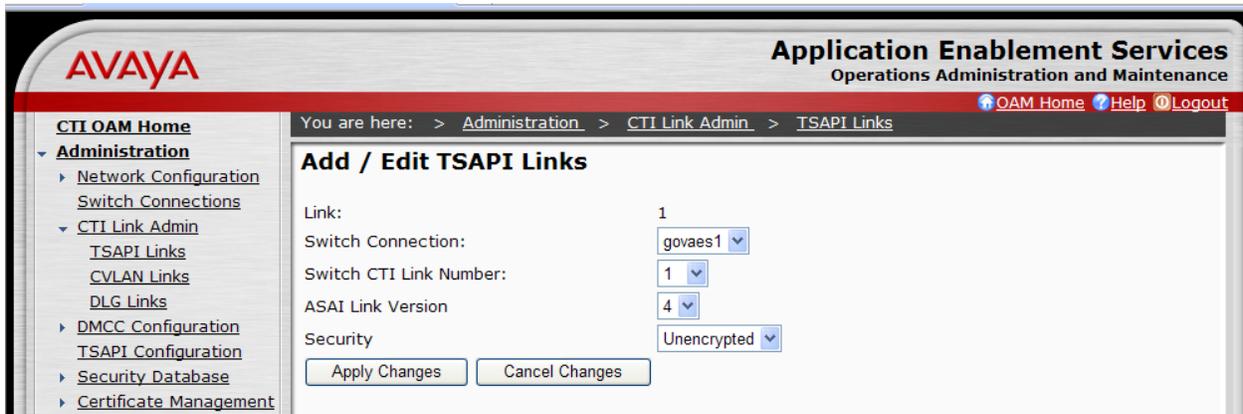


5.4. Administer TSAPI Link

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**.



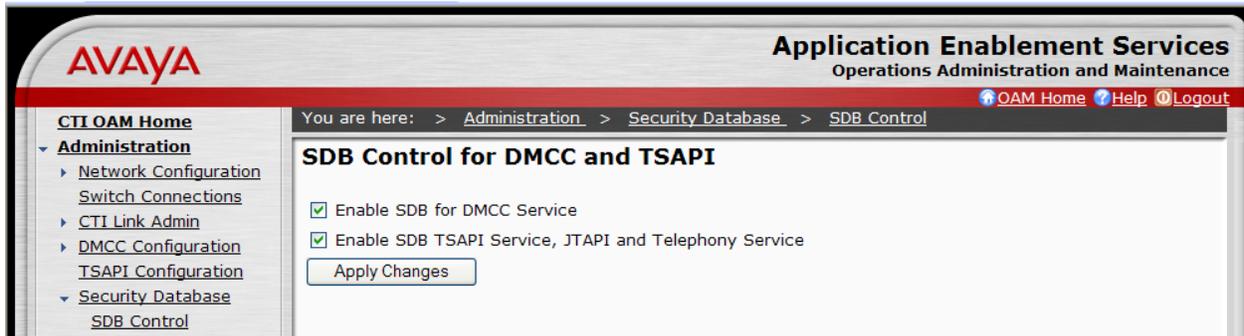
The **Add / Edit TSAPI Links** screen is displayed next. The **Link** field is only local to the AES server, and may be set to any available number. For **Switch Connection**, select the name of the switch connection from **Section 5.3**. For **Switch CTI Link Number**, select the CTI link number from **Section 4.6**. Accept the default values for **ASAI Link Version** and **Security**. Click on **Apply Changes**.



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

5.5. Administer Security Database

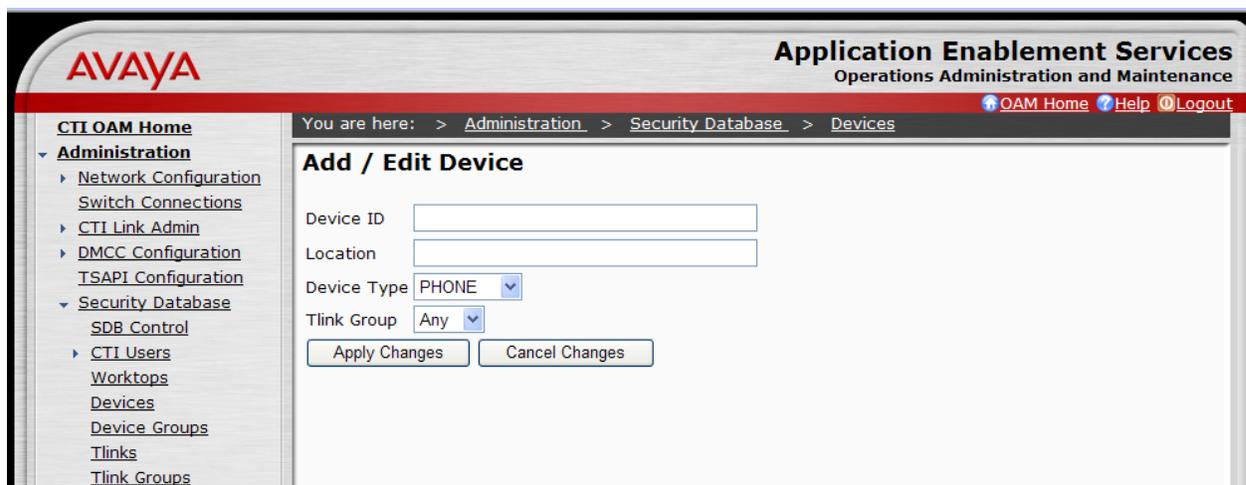
Enable the security database on AES, as this functionality is utilized by Sentinel. Select **Administration > Security Database > SDB Control** to display the **SDB Control for DMCC and TSAPI** screen shown below. Click on **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony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



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.



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.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > Devices

Devices

	Device ID	Tlink Group	Device Type	Location
<input checked="" type="radio"/>	49010	Any	AGENT ID	PlantCML Agent1
<input type="radio"/>	49011	Any	AGENT ID	PlantCML Agent2
<input type="radio"/>	53000	Any	PHONE	PlantCML
<input type="radio"/>	53001	Any	PHONE	PlantCML
<input type="radio"/>	53002	Any	PHONE	Plantcml (no nice)
<input type="radio"/>	53003	Any	PHONE	PlantCML (no nice)
<input type="radio"/>	53015	Any	VDN	PlantCML VDN 1
<input type="radio"/>	53020	Any	VDN	PlantCML VDN 2

Buttons: Add Device, Edit Device, Delete Device

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.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Security Database > Tlinks

Tlinks

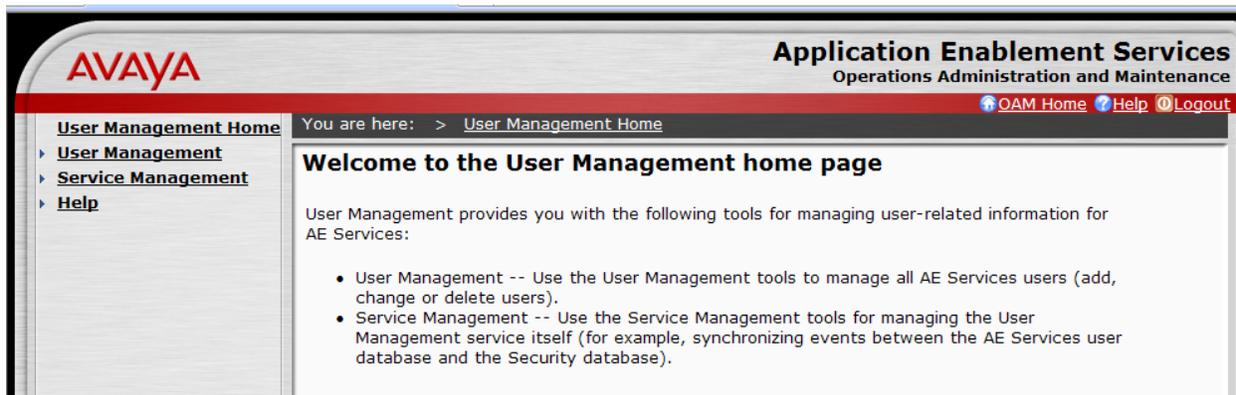
Tlink Name

AVAYA#GOVAES1#CSTA#GOVAES1

Buttons: Edit Tlink, Delete Tlink

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.



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"

AVAYA Application Enablement Services
Operations Administration and Maintenance

[OAM Home](#) [Help](#) [Logout](#)

[User Management Home](#) You are here: > [User Management](#) > [Add User](#)

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

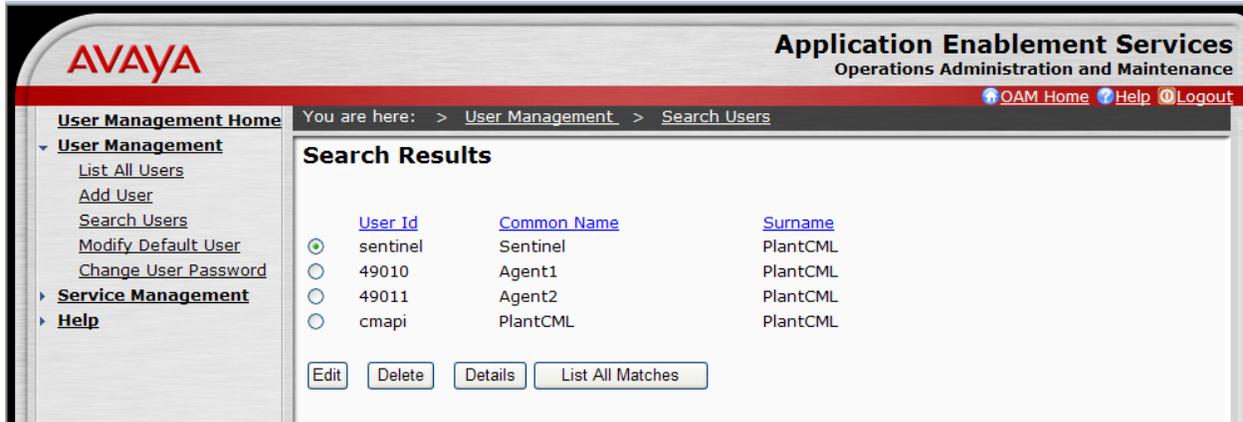
Given Name

Home Phone

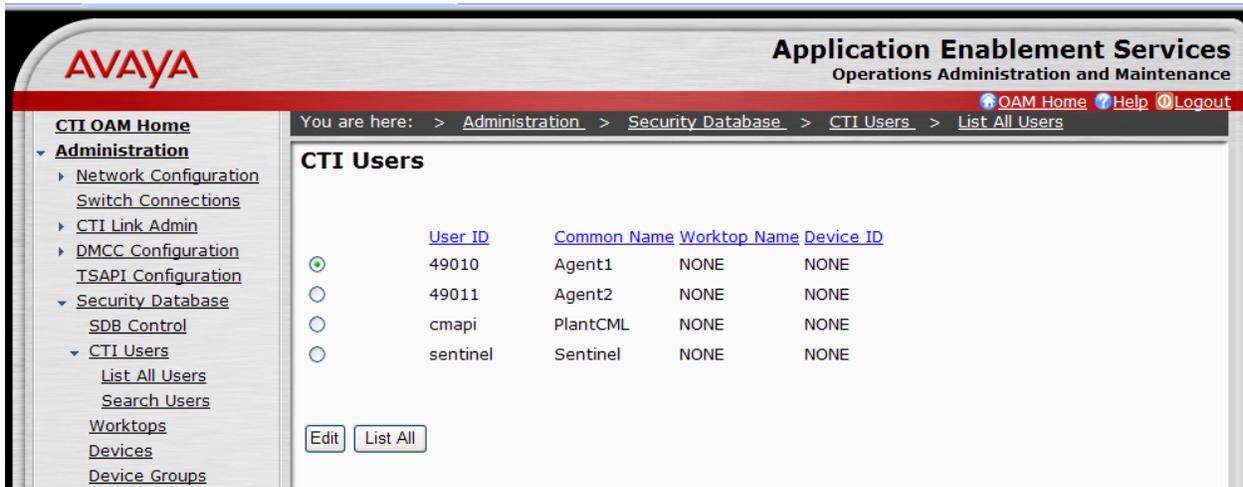
Home Postal Address

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 6.1**. All the administered user accounts created for PlantCML Sentinel application are shown below:

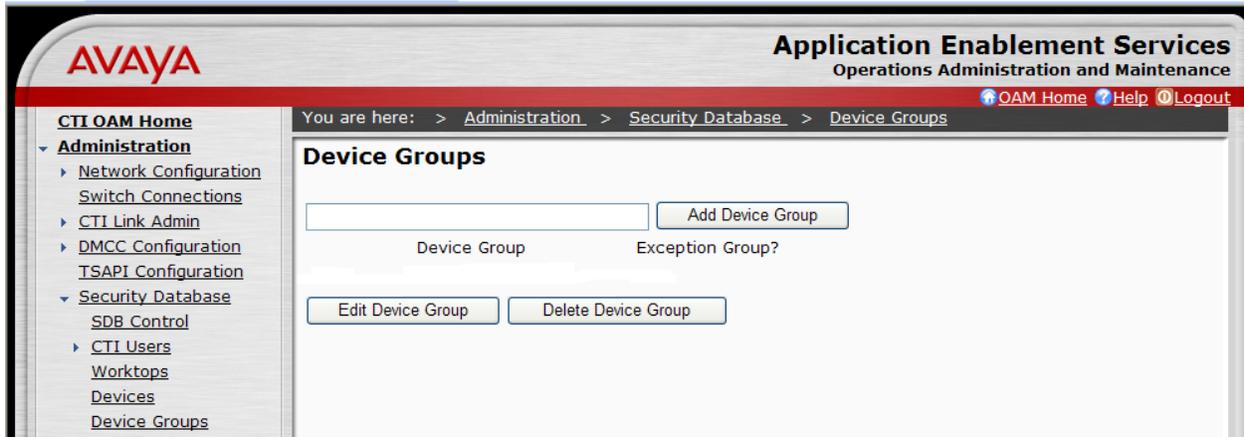


Follow the login procedures in **Section 5.1**, and log in with the CTI OAM Admin user name and password. Select **Administration > Security Database > CTI Users > List All Users** to get a listing of all CTI users, as shown below.

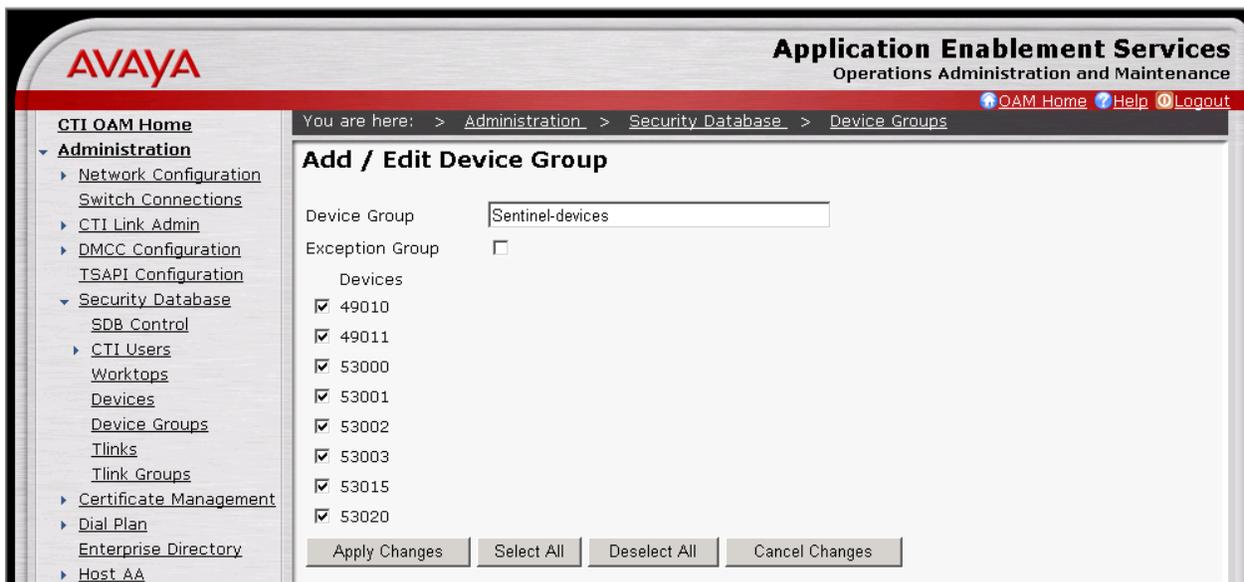


5.8. Administer Device Groups

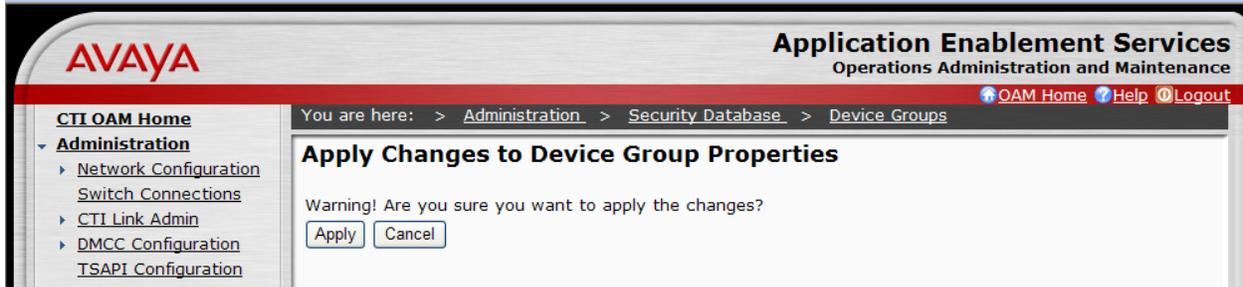
Administer a device group to be used by Sentinel, to control user access of devices. Select **Administration > Security Database > Device Groups** from the left pane. In the **Device Groups** screen shown below, enter a descriptive value, and click on **Add Device Group**.



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**.



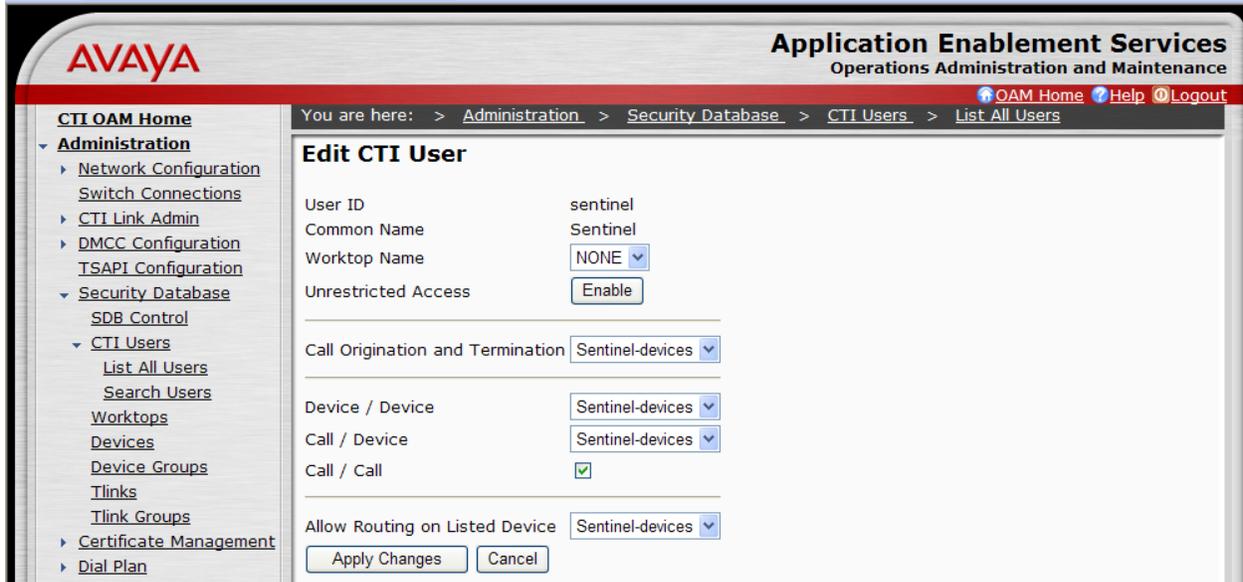
The **Apply Changes to Device Group Properties** screen is displayed next. Click on **Apply** to confirm the changes.



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”.



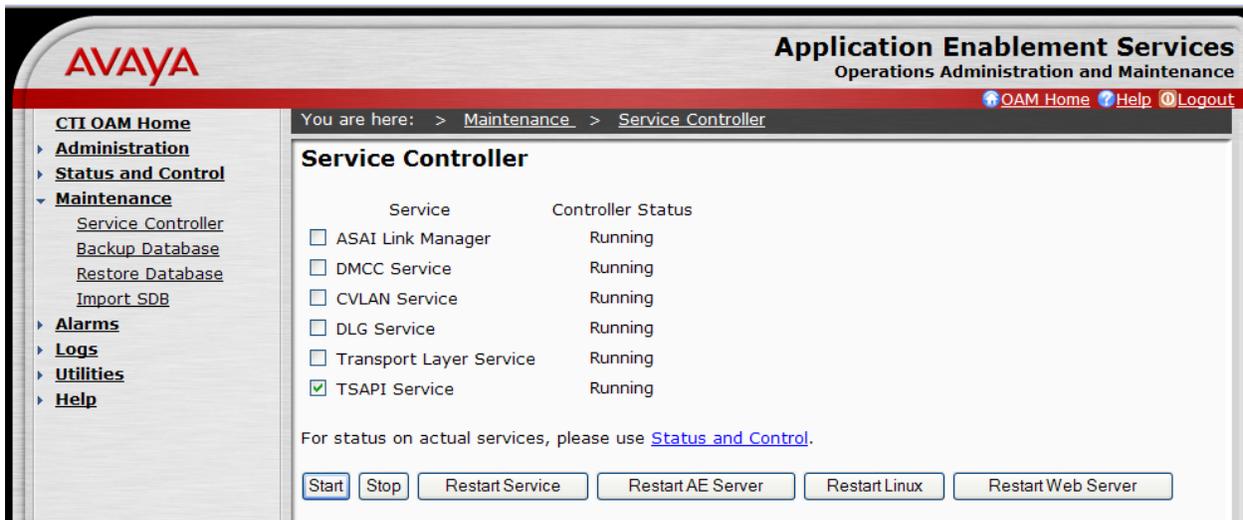
The **Edit CTI User** screen is displayed, as shown below. Select the newly created device group for the **Call Origination and Termination, Device / Device, Call / Device, and Allow Routing on Listed Device** fields. Click on **Call / Call**, followed by **Apply Changes**.



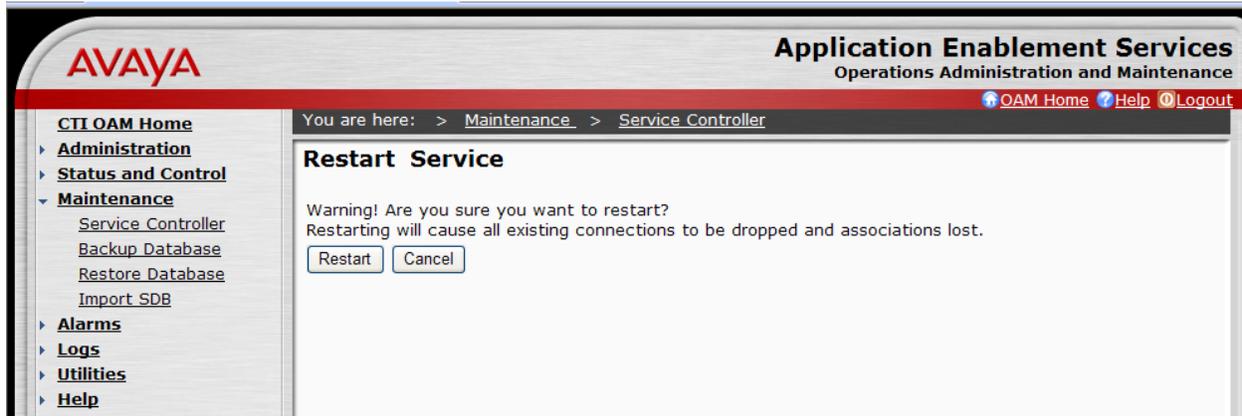
Repeat this procedure for all CTI users listed in the **CTI Users** screen above – “49010”, “49011” and “cmapi”.

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**.



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



5.10. Administer Second AES Server

As described in **Section 1.2** and shown in **Figure 2**, two AES servers need to be administered. Repeat steps described in **Section 5.1 to Section 5.9** to configure the second AES server. For the sample configuration, repeat the steps for “goveaes2”.

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.

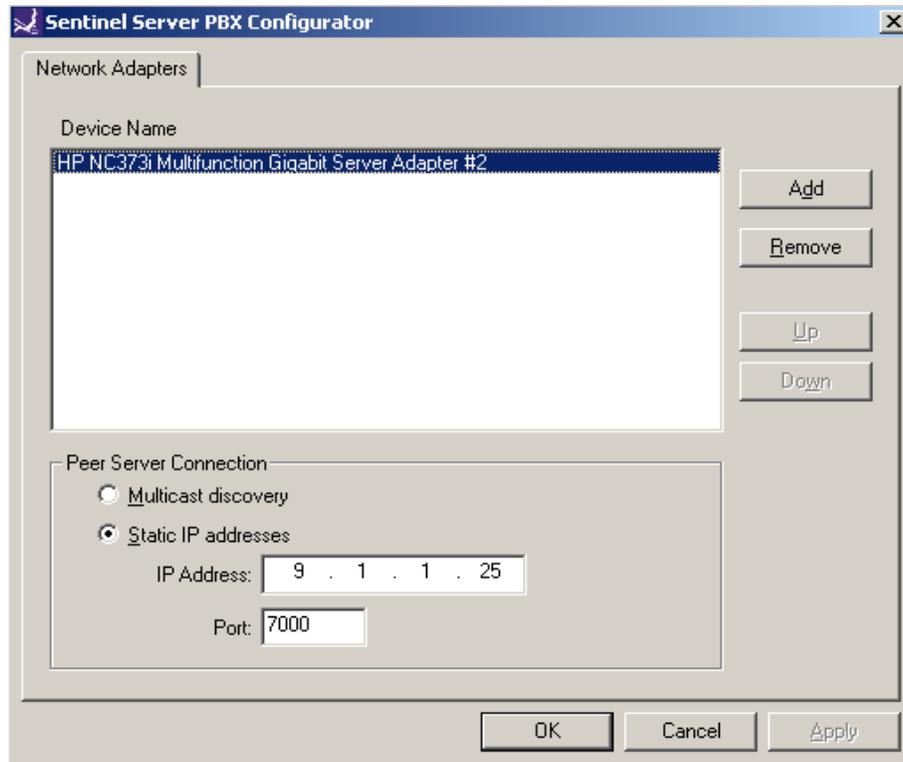
For the sample configuration, use the following in the **Name** and **IP Address**. The actual name and IP address may vary.

Sentinel CM Servers	
Name	IP Address
Server-A	9.1.1.25
Server-B	9.1.1.26

6.1. Administer Sentinel Server Configuration

On the first sentinel server (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 second sentinel server (Server-B).
- Click on **OK** at the bottom of the screen.

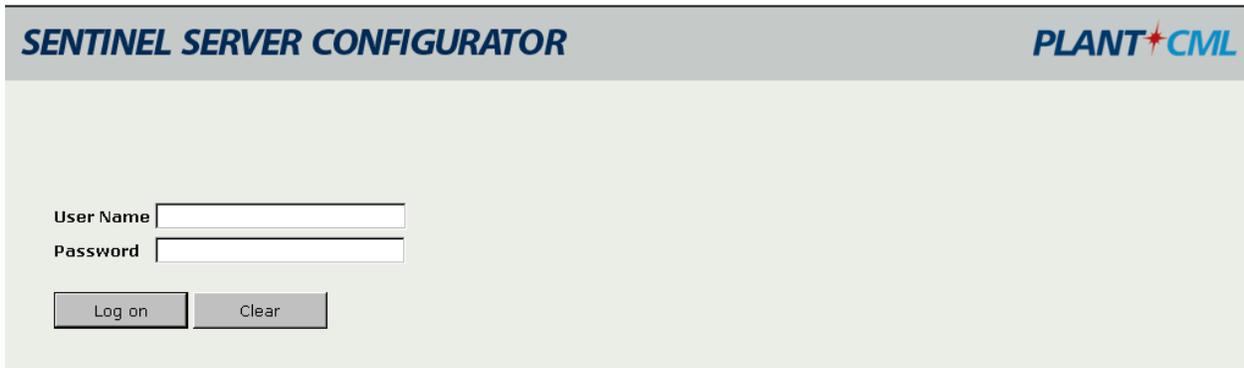


On the second sentinel server (on Server-B), select **Start → Control Panel**. Double click on the **Sentinel Server** icon. The **Sentinel Server PBX Configurator** screen will appear (not shown). For the **Peer Server Connection**, select **Static IP addresses** and enter the IP address of the first sentinel server (Server-A). Click on **OK** at the bottom of the screen.

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.

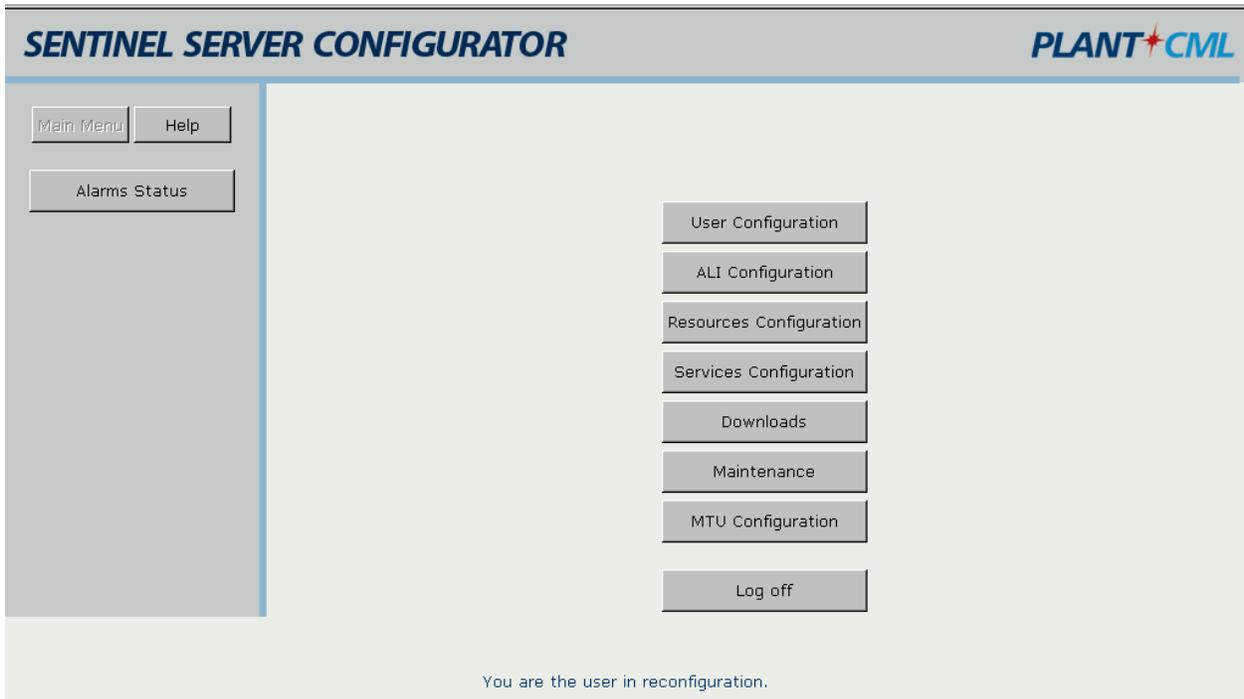
Note that the configuration steps described in **Section 6.2 to Section 6.8** are performed on the active server only. The backup server will automatically synch up with the primary server.



The screenshot shows the login interface for the Sentinel Server Configurator. At the top, there is a header bar with the text "SENTINEL SERVER CONFIGURATOR" on the left and the "PLANT CML" logo on the right. Below the header, there are two input fields: "User Name" and "Password". Below these fields are two buttons: "Log on" and "Clear".

6.3. Administer Global Settings

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



The screenshot shows the main menu of the Sentinel Server Configurator. At the top, there is a header bar with the text "SENTINEL SERVER CONFIGURATOR" on the left and the "PLANT CML" logo on the right. Below the header, there is a left sidebar with three buttons: "Main Menu", "Help", and "Alarms Status". To the right of the sidebar, there is a vertical list of buttons: "User Configuration", "ALI Configuration", "Resources Configuration", "Services Configuration", "Downloads", "Maintenance", "MTU Configuration", and "Log off". At the bottom of the page, there is a message: "You are the user in reconfiguration."

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
- Leave the LSP – IP Address field blank.
- Uncheck the Enable LSP box.
- Enter the **Username and password created in Section 4.14** 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 and 5.10**).
- 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

Sentinel Server

Server A Name		Server B Name	
Name	<input type="text" value="Server-A"/>	Name	<input type="text" value="Server-B"/>
Media Gateway ID	<input type="text" value="0"/>	Media Gateway ID	<input type="text" value="0"/>
Server Group			
PSAP Name	<input type="text" value="PSAPName"/>		

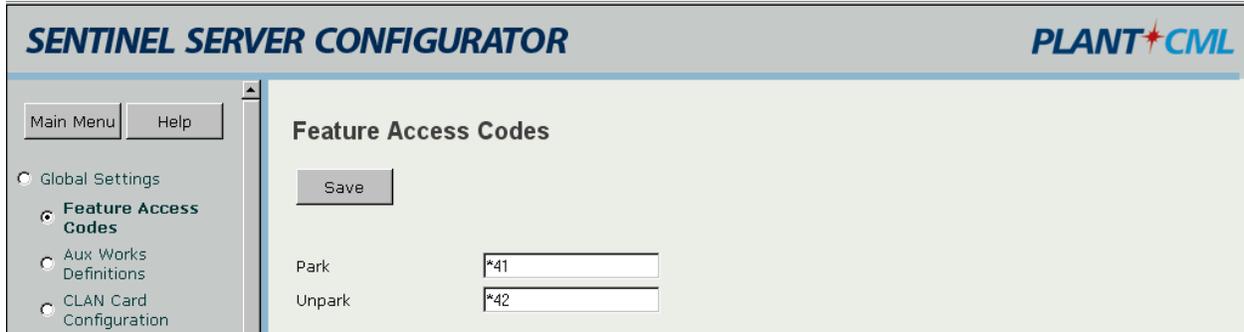
Avaya Media Server

Enable LSP	<input type="checkbox"/>	Site Administration Account	
Main - IP Address	<input type="text" value="9.1.1.4"/>	Username	<input type="text" value="plantcml"/>
LSP - IP Address	<input type="text"/>	Password	<input type="password" value="....."/>
		PIN	<input type="text"/>

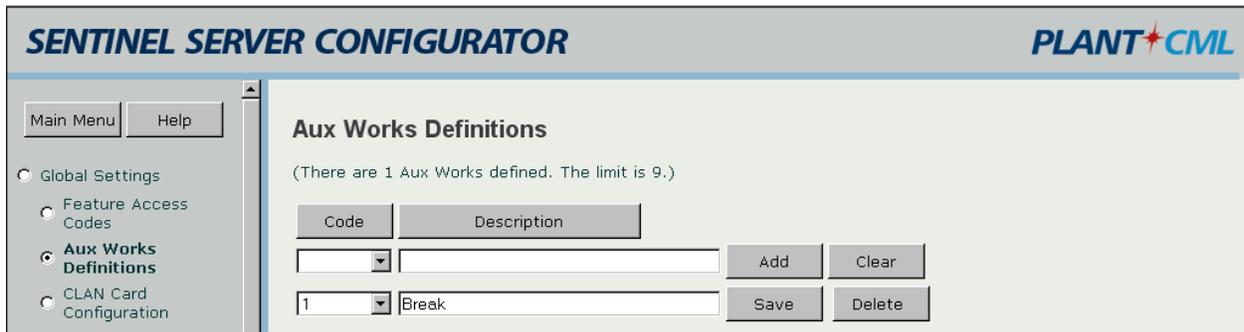
Avaya Application Enablement Server

AES A		AES B	
IP Address	<input type="text" value="9.1.1.51"/>	IP Address	<input type="text" value="9.1.1.52"/>
Server ID	<input type="text" value="1"/>	Server ID	<input type="text" value="2"/>
CTI (TSAPI)		CMAPI (DMCC)	
User	<input type="text" value="sentinel"/>	User	<input type="text" value="cmapi"/>
Password	<input type="password" value="....."/>	Password	<input type="password" value="....."/>
Primary TLink	<input type="text" value="AVAYA#GOVAES2#CS"/>	Port Number	<input type="text" value="4721"/>
Secondary TLink	<input type="text" value="AVAYA#GOVAES1#CS"/>		

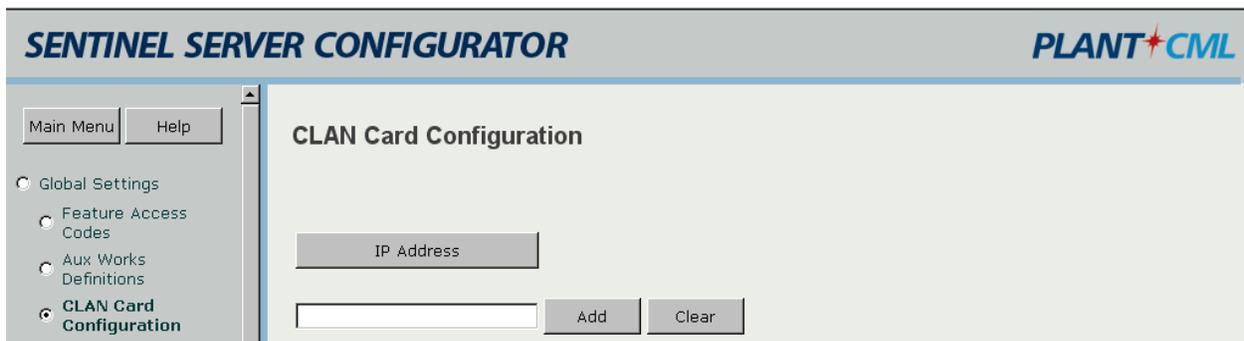
Select **Feature Access Codes** in the left pane. Enter the corresponding feature access code for Call Park and Answer Back Access Code from **Section 4.9**, in **Park and Unpark** fields. Click on **Save** at the top of the screen.



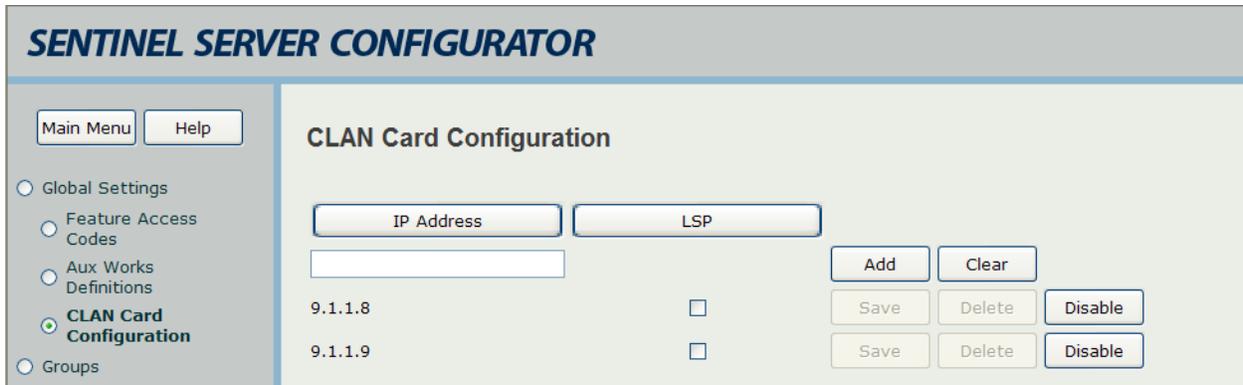
Select **Aux Works Definitions** in the left pane. Enter appropriate **Code** and **Description**. Click on **Add**.



Select **CLAN Card Configuration** in the left pane. Enter the IP address for the C-LAN module. Click on **Add**.

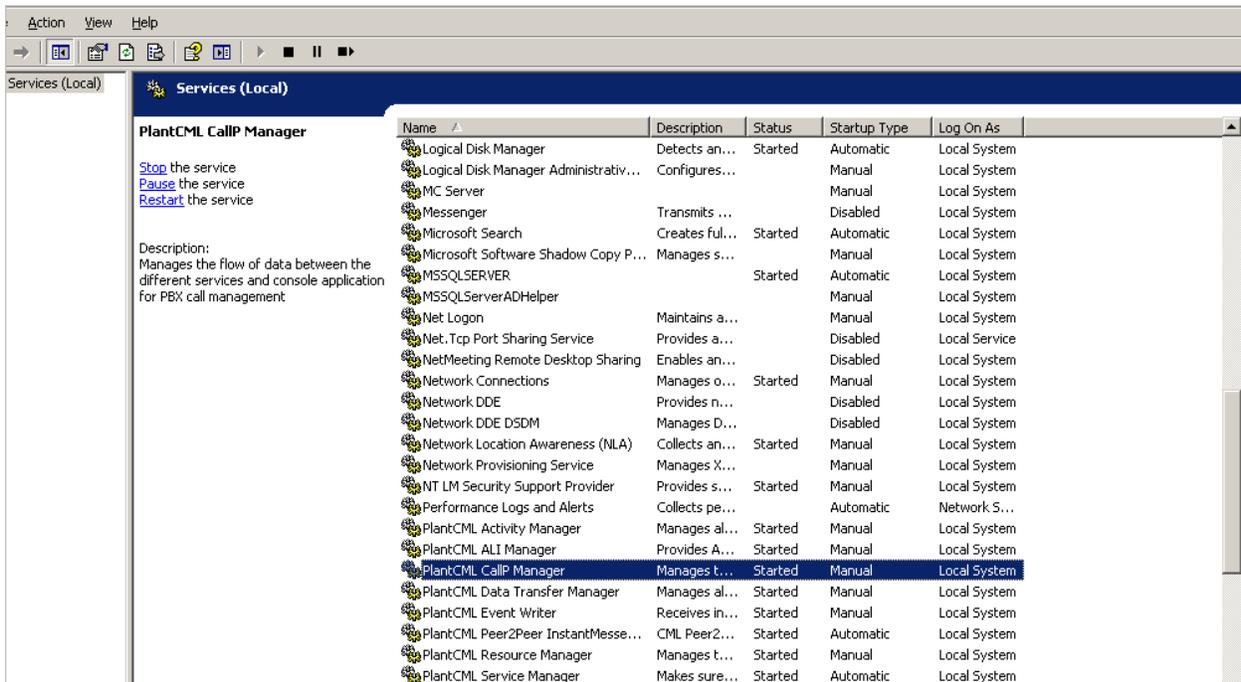


For the sample configuration, two C-LAN modules are used. The screen below displays the C-LAN modules administered.



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.



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 Extension	Label	Type	Group	Save	Details
53000	53000	Sentinel	PHONES	Save	Details
53001	53001	Sentinel	PHONES	Save	Details

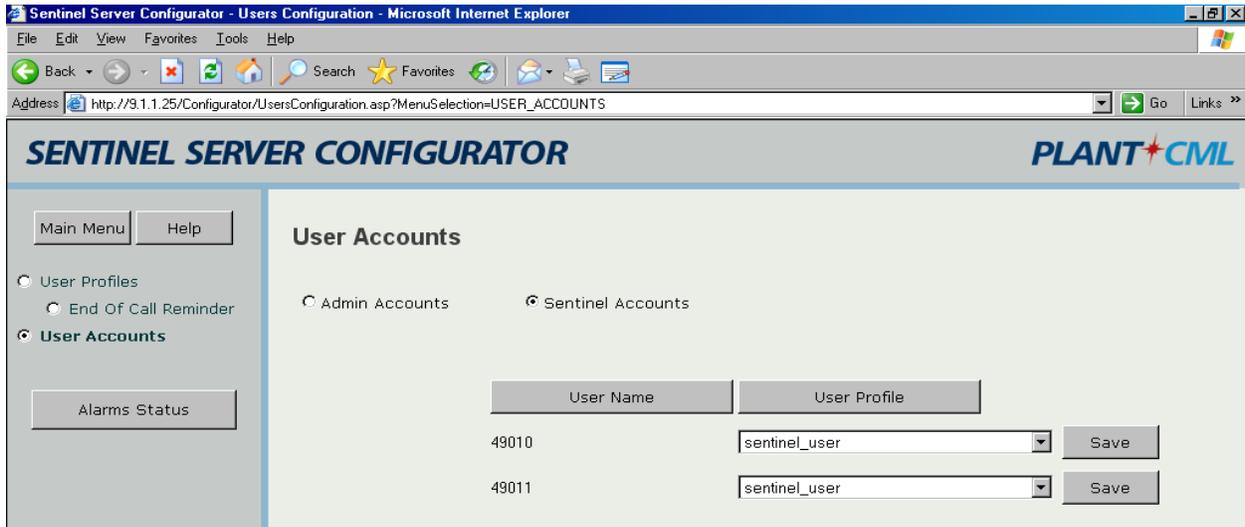
To view the Phone details, click on Details button. It is recommended to populate the **Phone IP (Optional)** field if static IP addresses are used for 911 call answering agents IP Phones. Click on **Save** button if any changes were made to the Phone Details.

Save

Extension 53000
ID 53000
Label 53000
Phone Interface Sentinel
Site Type Host Main
Group PHONES
CAD Group None
ALI Print Out None
Phone Type IP Phone IP Address 9.1.1.103

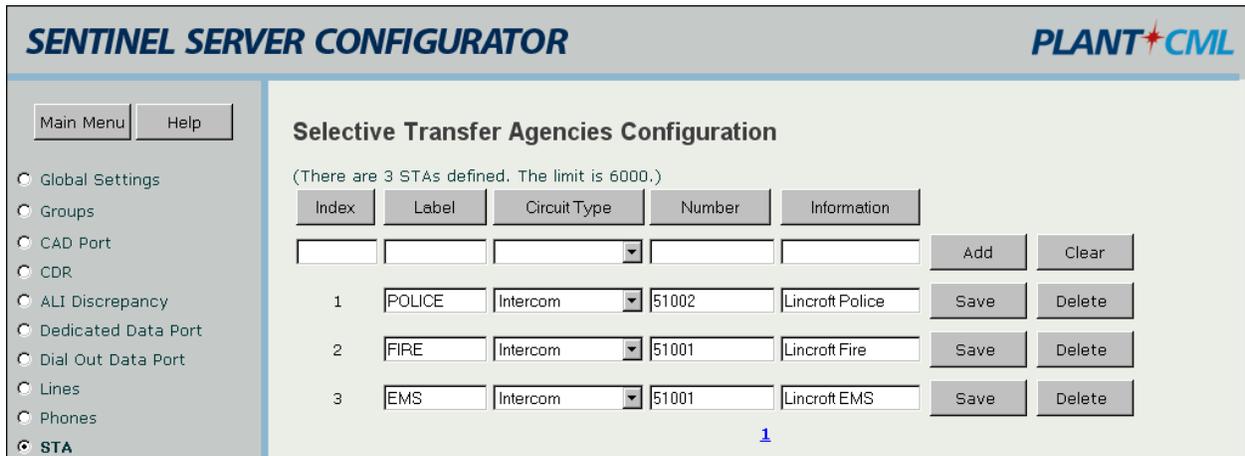
6.6. Verify Sentinel Accounts

From the main menu select **User Configuration**. Select **User Accounts** and click on **Sentinel Accounts**. Verify the Agents created in **Section 4.11** 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.



6.7. Selective Transfer Agencies Configuration

Select **STA** from the left pane to administer information for pre-programmed buttons. These can be used for outside agencies like Police, Fire or EMS. This is an optional step.



6.8. 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.

The screenshot displays the 'SENTINEL SERVER CONFIGURATOR' interface with the 'PLANT CML' logo. The 'Line Configuration' section is active, showing a table with the following data:

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

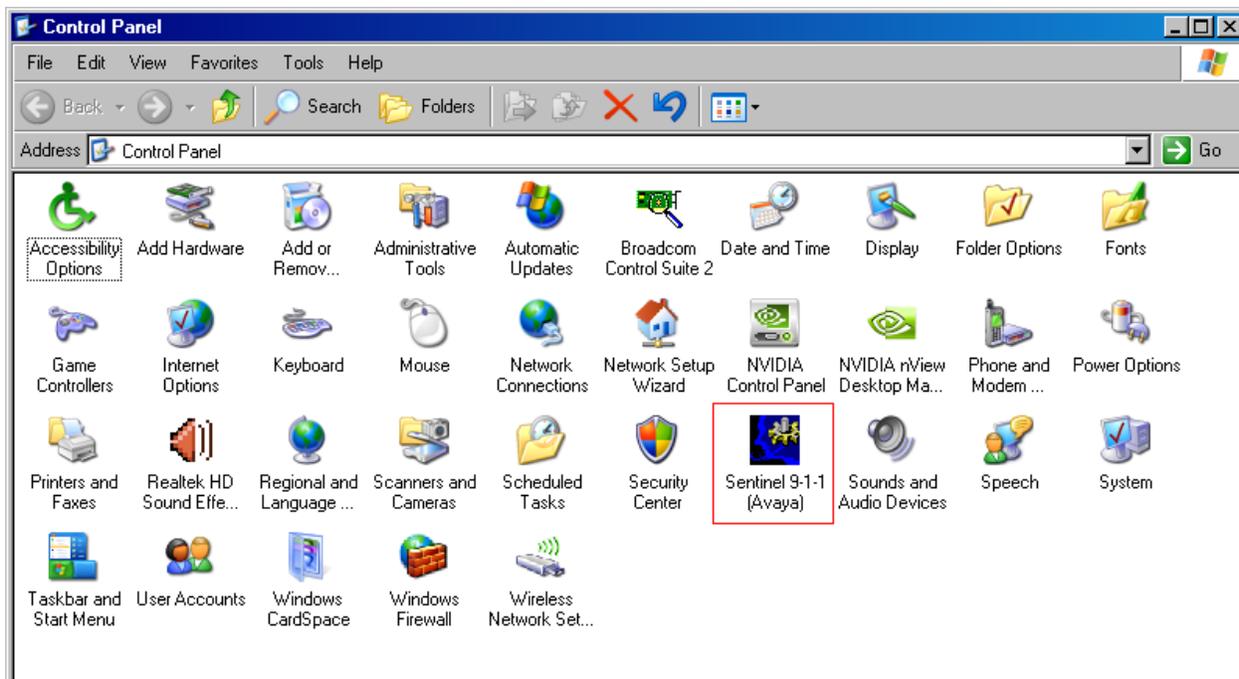
7. Configure PlantCML Sentinel 9-1-1 Clients

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

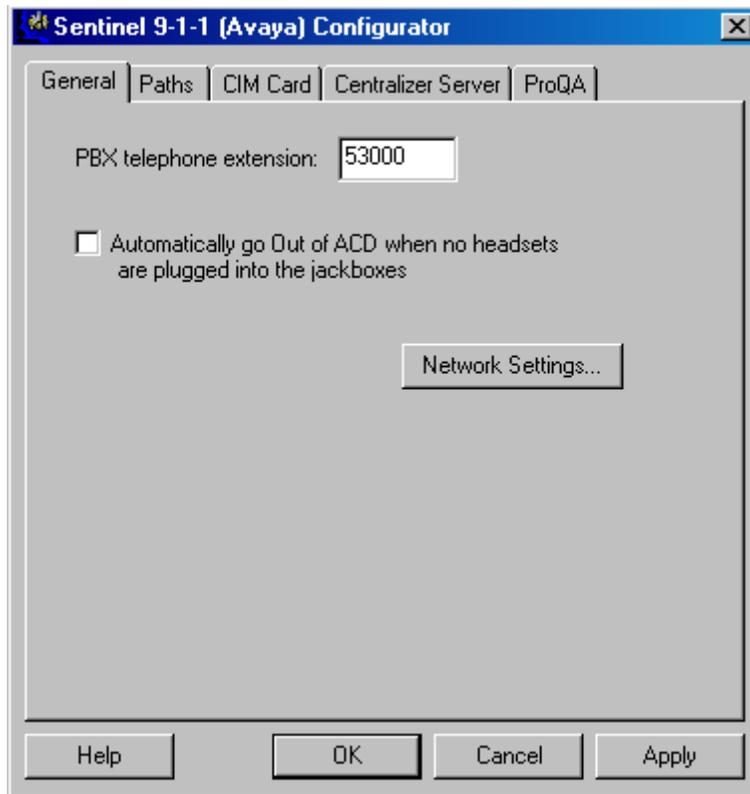
- Administer physical extension
- Log into logical extension
- Administer user configuration file

7.1. Administer Physical Extension

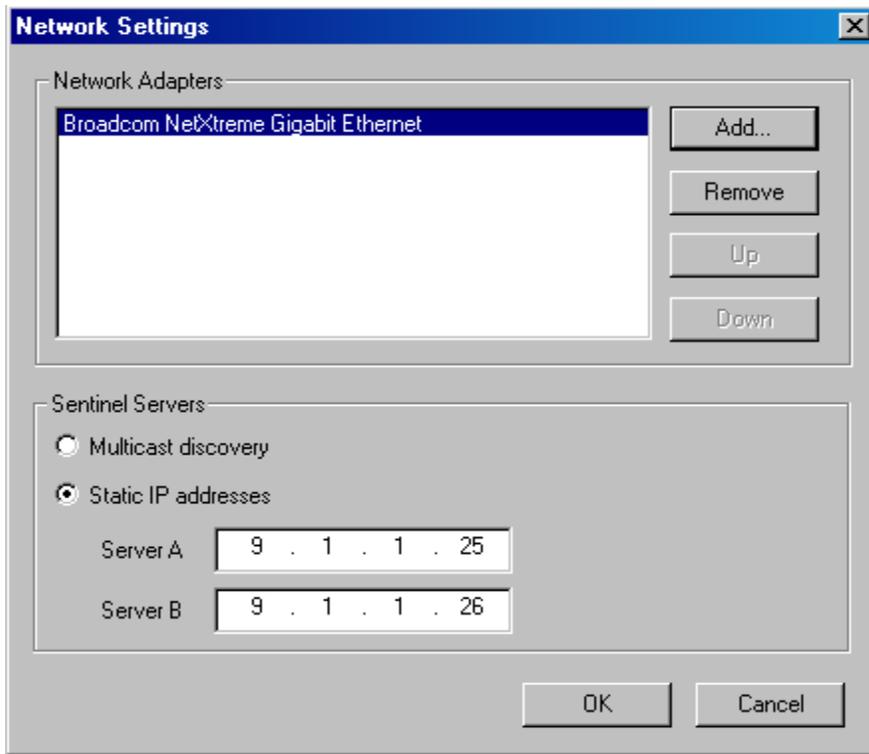
From each Sentinel 9-1-1 client PC, select **Start > Control Panel** to bring up the **Control Panel** screen. Double click on the **Sentinel 9-1-1 (Avaya)** icon, which was created as part of the **PlantCML Sentinel 9-1-1** installation.



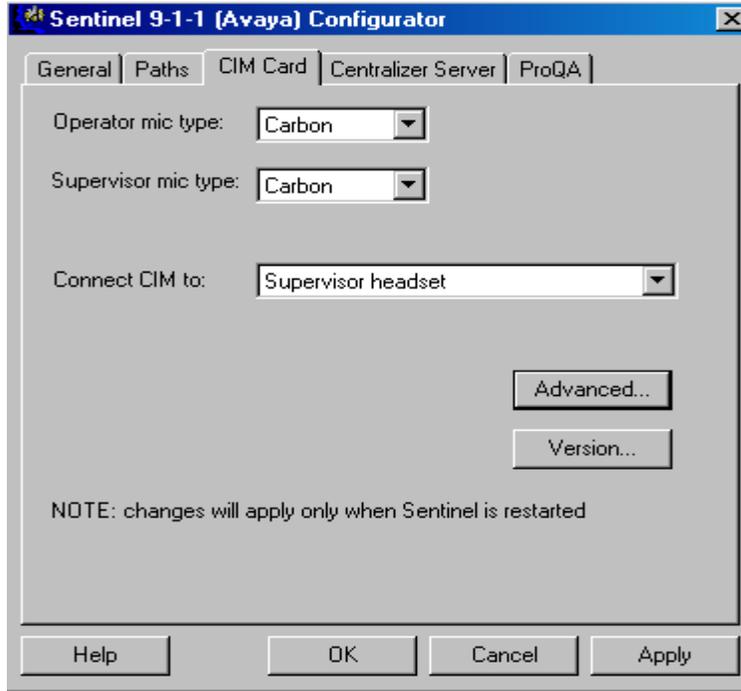
The **Sentinel 9-1-1 (Avaya) Configurator** screen is displayed. Enter the extension associated with the agent's physical telephone from **Section 4.7**, and click on **Network Settings**.



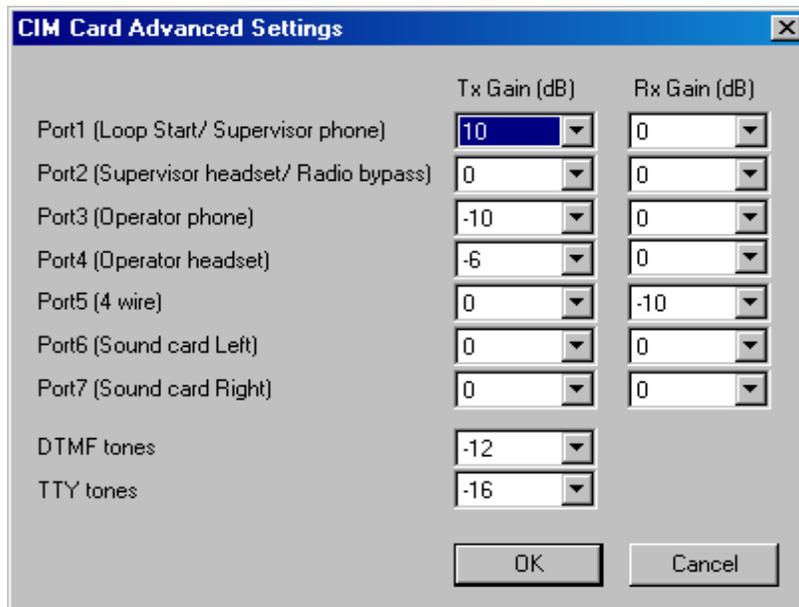
The **Network Settings** screen is displayed next. Select **Static IP addresses** and enter the IP addresses for Sentinel Server A and Sentinel Server B, and click **OK**.



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

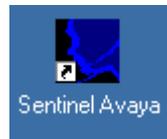


Click the **Advanced ...** button. Set the parameters as shown below and click **OK**.

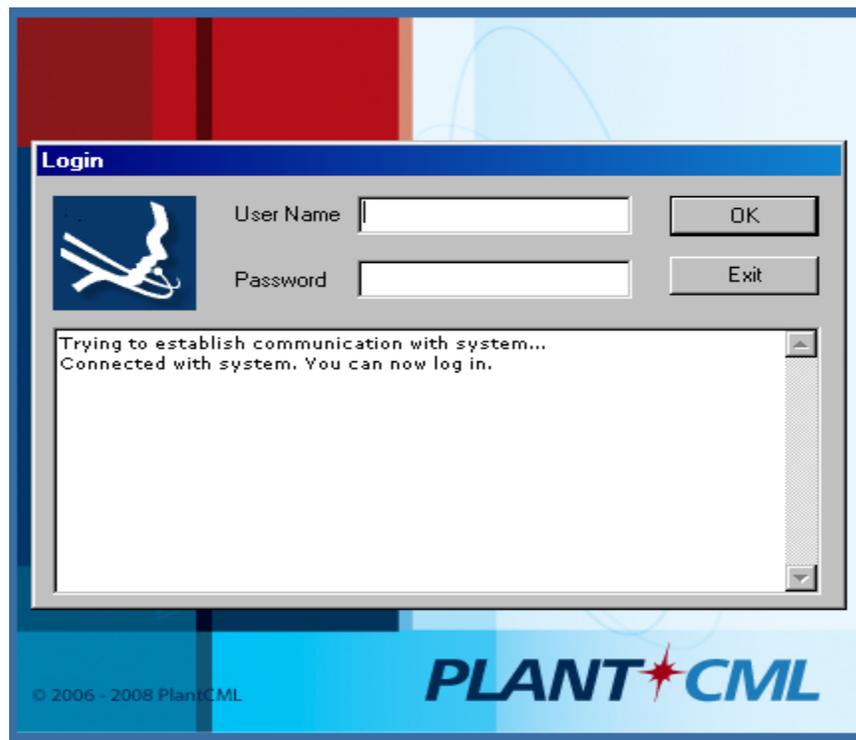


7.2. Log Into Logical Extension

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**.

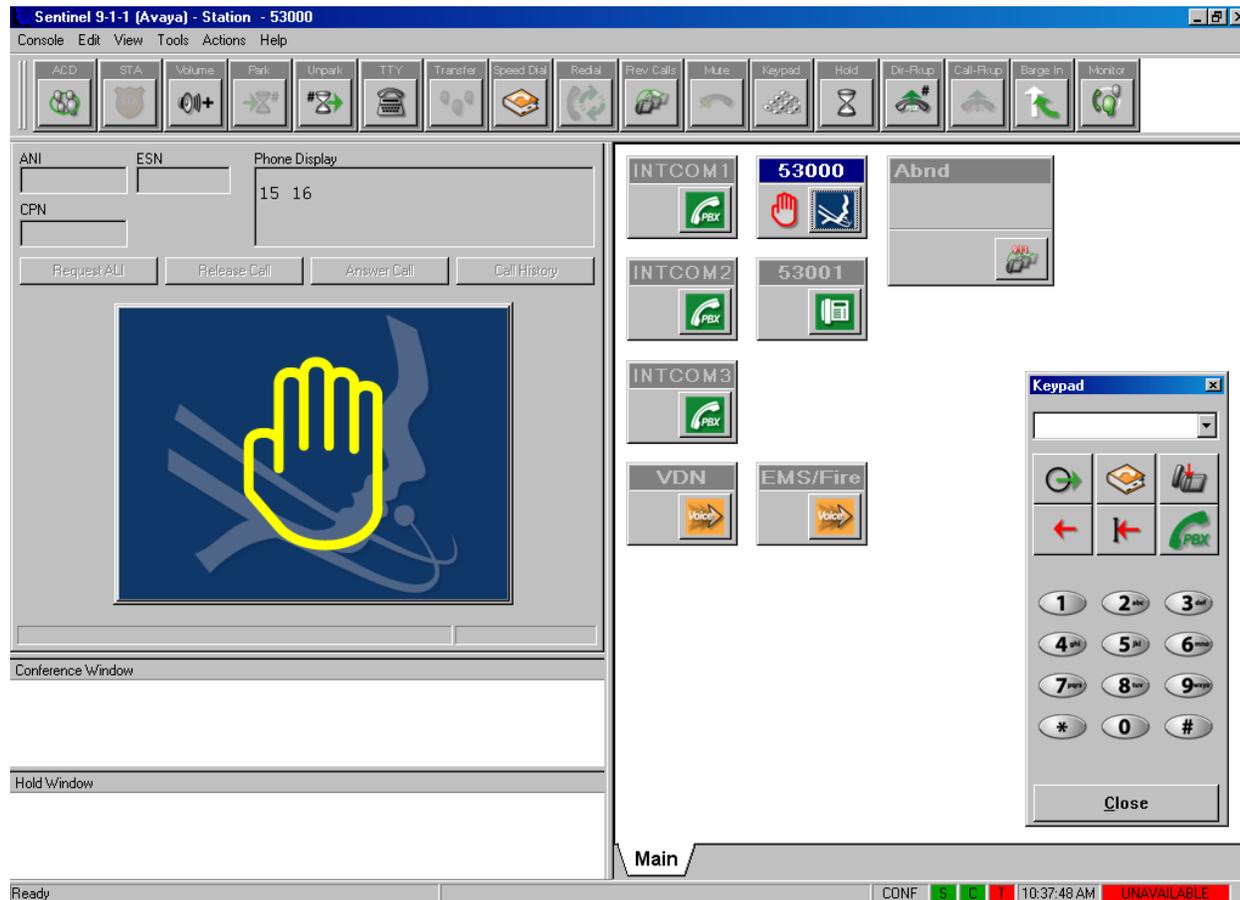


7.3. Administer User Configuration File

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 their desktop using options under **Console > Preferences > Desktop**.

Refer to the Sentinel documentation in **Section 13** for how to customize the graphical user interface, such as creating icons for call related actions, and specifying the fonts for the icons.



8. General Test Approach and Test Results

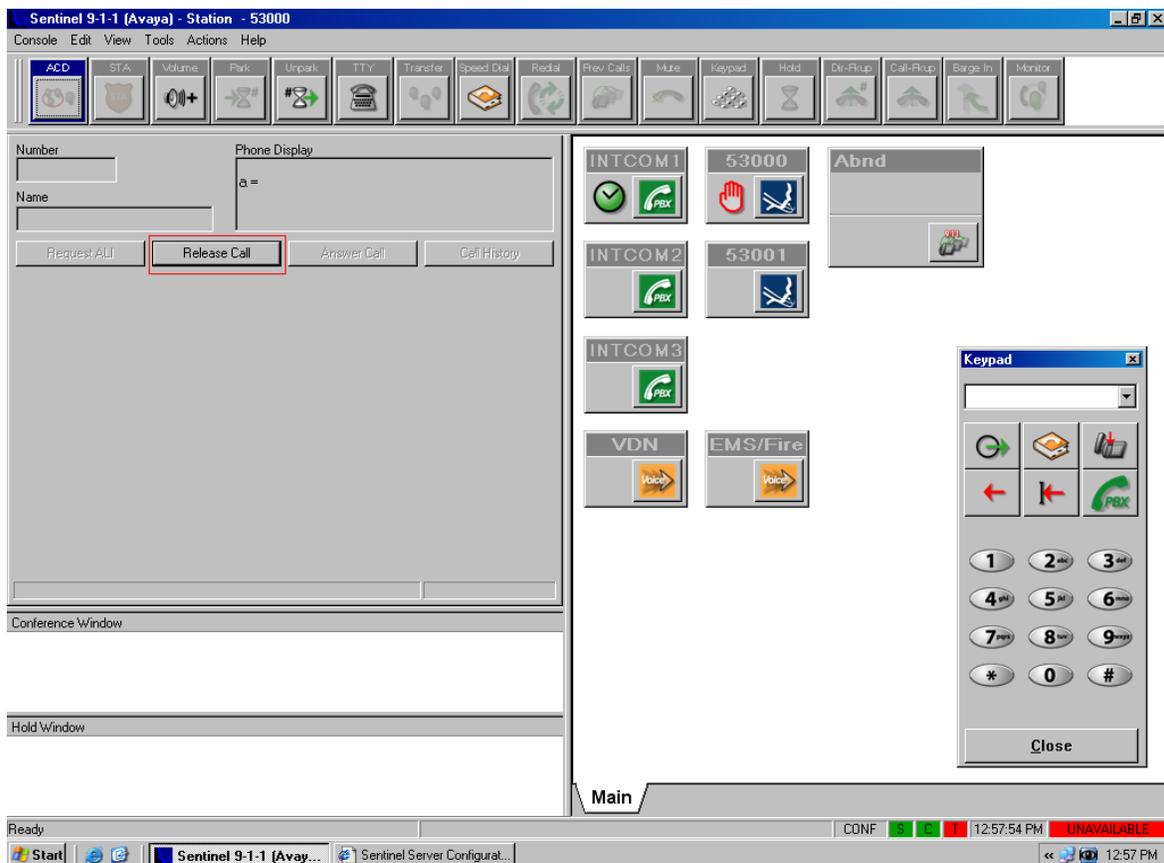
All the test cases were performed manually. Upon start of the Sentinel application, the application automatically queries Avaya Communication Manager for VDN/agent status and requests monitoring. Incoming 911 calls were made to the monitored VDNs. Call controls from both the agent desktop and the agent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

The serviceability test cases were performed by busying out and releasing the CTI link, and by disconnecting and reconnecting the LAN cables to the Sentinel server and to the Sentinel 9-1-1 clients.

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

Few observations were made during testing which are noted below:

1. Display for conferencing is different on 4600 Series phones and 9600 Series phones. For a 3-party conference, the 4600 Series Phones will show “3-party Conference in progress” and 9600 Series Phone will show “CONFERENCE 2”.
2. It is recommended to use the Sentinel 9-1-1 application to log-in, change ACD states, log-out, call-park and call pickup. Avaya Communication Manager Feature Access Codes (FAC) should only be used when the Sentinel 9-1-1 application is not available.
3. The 911 call answering agents should not be equipped to handle multiple incoming calls. The Sentinel 9-1-1 application does not support this feature. By default, Multiple ACD Calls is set to “N”.
4. It is recommended to have a NTP timing source for Sentinel applications to synchronize. If NTP timing is not configured, a batch file needs to be installed on Sentinel servers which will synchronize the servers on a regular basis (like every hour).
5. The 911 Agent needs to enable the “headset” button on the Avaya IP Telephones. A call will be launched when the agent activates the “headset” button on the IP phone. The 911 Agent will need to release the call from the Sentinel 9-1-1 as shown below:



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. Verify Avaya Communication Manager

On Avaya Communication Manager, verify the status of the administered CTI links by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link numbers administered in **Section 4.6**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	govaes1	established	672	672
2	4	no	govaes2	established	15	15

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 ext 53000 count 2
```

REGISTERED IP STATIONS								
Station	Ext/Orig Port	Set Type	Product ID	Prod Rel	Station IP Address	Net Rgn	Gatekeeper IP Address	TCP Skt
53000		4620	IP_Phone	2.8300	9.1.1.103	1	9.1.1.9	y
53000		4620	IP_API_A	3.2040	9.1.1.52	1	9.1.1.8	y
53001		9630	IP_Phone	1.5000	9.1.1.104	1	9.1.1.9	y
53001		9630	IP_API_A	3.2040	9.1.1.52	1	9.1.1.8	y

9.2. Verify Avaya Application Enablement Services

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.

Application Enablement Services
Operations Administration and Maintenance

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
govaes1	Talking	2009-01-21 11:08:52.0	Online	1 / 1	2	1815	1216

Buttons:

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.

Application Enablement Services
Operations Administration and Maintenance

You are here: > [Status and Control](#) > [Services Summary](#)

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	2009-02-02 16:16:44.0	Online	15	7	767

Buttons:

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

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

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Status and Control > Services Summary

CTI User Status

CTI Users: All Users (dropdown) Refresh

Open Streams: 4
Closed Streams: 1

Name	Time Opened	Time Closed	Tlink Name
sentinel	2009-02-09 12:58:04	Open	AVAYA#GOVAES1#CSTA#GOVAES1
sentinel	2009-02-09 12:58:04	Open	AVAYA#GOVAES1#CSTA#GOVAES1
49011	2009-02-09 12:58:04	Open	AVAYA#GOVAES1#CSTA#GOVAES1
49010	2009-02-09 13:38:37	Open	AVAYA#GOVAES1#CSTA#GOVAES1

Show Closed Streams Close All Opened Streams Back

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.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Status and Control > Services Summary

DMCC Service Summary - Session Summary

Session Summary Device Summary
Generated on Mon, Feb 9, 2009 01:42:53 PM EST

Service Uptime: 11 days, 5:17 hours
Number of Active Sessions: 2
Number of Sessions Created Since Service Boot: 51
Number of Existing Devices: 2
Number of Devices Created Since Service Boot: 51

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/> 5194ADE463A995790 240F47605C219C3-49	cmapi	cmapiApplication	9.1.1.28	XML Unencrypted	1
<input type="checkbox"/> CCBB16169F3F27589 BBB75D0F021DCF3-50	cmapi	cmapiApplication	9.1.1.27	XML Unencrypted	1

Terminate Sessions Show Terminated Sessions

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

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Status and Control > Services Summary

DMCC Service Summary - Device Summary

Session Summary **Device Summary**
Generated on Mon, Feb 9, 2009 01:39:25 PM EST

Service Uptime: 11 days 5:13 hours
 Number of Active Sessions: 2
 Number of Sessions Created Since Service Boot: 51
 Number of Existing Devices: 2
 Number of Devices Created Since Service Boot: 51

Device ID	State	Associated Sessions
53000::9.1.1.8:0	REGISTERED	1
53001:govaes1:9.1.1.9:0	REGISTERED	1

Terminate Devices

9.3. Verify PlantCML Sentinel Server and Sentinel 9-1-1 Client

Make an incoming 911 call, and verify the available agent is alerted by a visual flashing 9-1-1 display on the desktop and a siren sound on the headset. Click on the **Answer Call** icon or the 9-1-1 display.

Sentinel 9-1-1 (Avaya) - Station - 53000

Console Edit View Tools Actions Help

ACD STA Volume Park Unpark TTY Transfer Speed Dial Redial Rev. Calls Mute Keypad Hold Dr-Rup Cal-Rup Barge In Monitor

ANI: _____ ESN: _____ Phone Display: a=John Doe to PlantCML HotLin
 CPN: _____

Request All Release Call Answer Call Call History

9-1-1

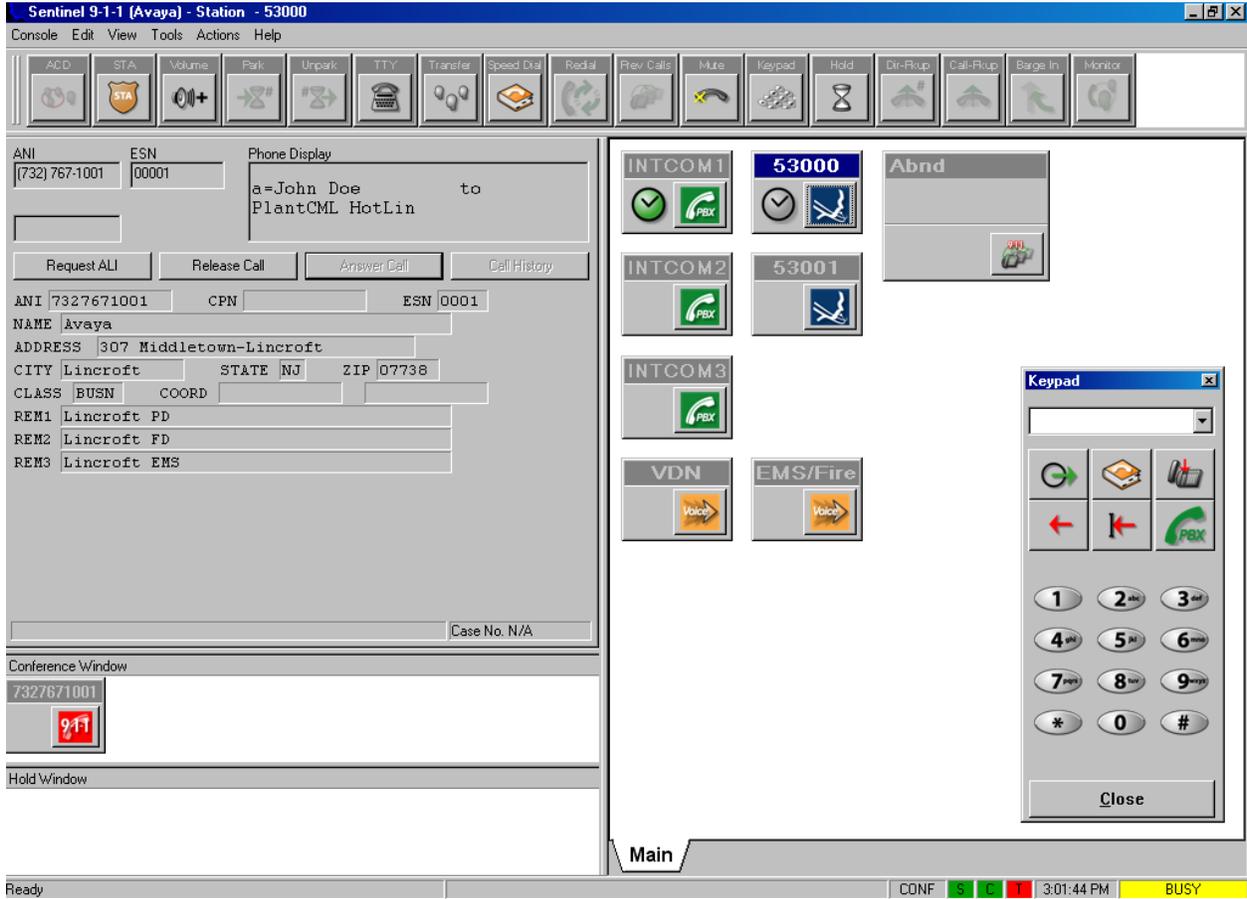
Conference Window

Hold Window

Main

Ready CONF 3:01:12 PM BUSY

Verify the agent is connected to the caller with two-way talk paths, and that the agent screen is populated with the caller ANI and ALI information, as shown below.

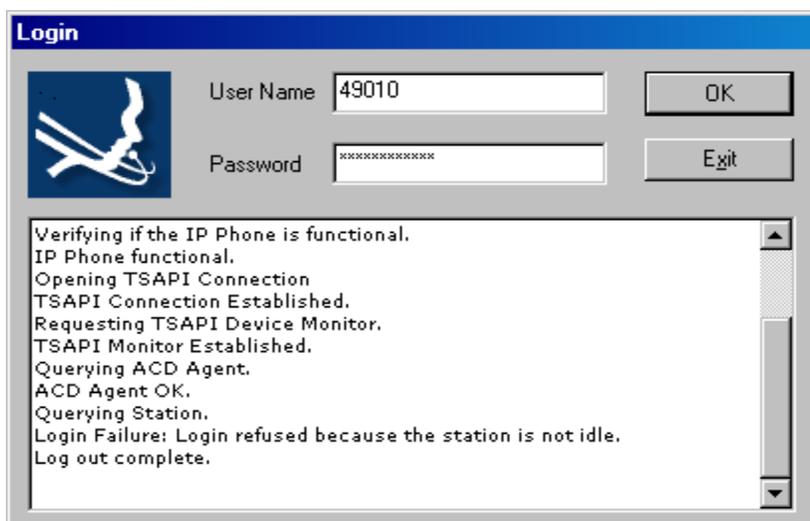


10. Troubleshooting

This section offers some common configuration mismatches to assist in troubleshooting.

10.1. Sentinel 9-1-1 Cannot Login

The 911 Agent cannot login to the Sentinel 9-1-1 Application if the station/agent is on an active call. Following Login Failure screen will appear.



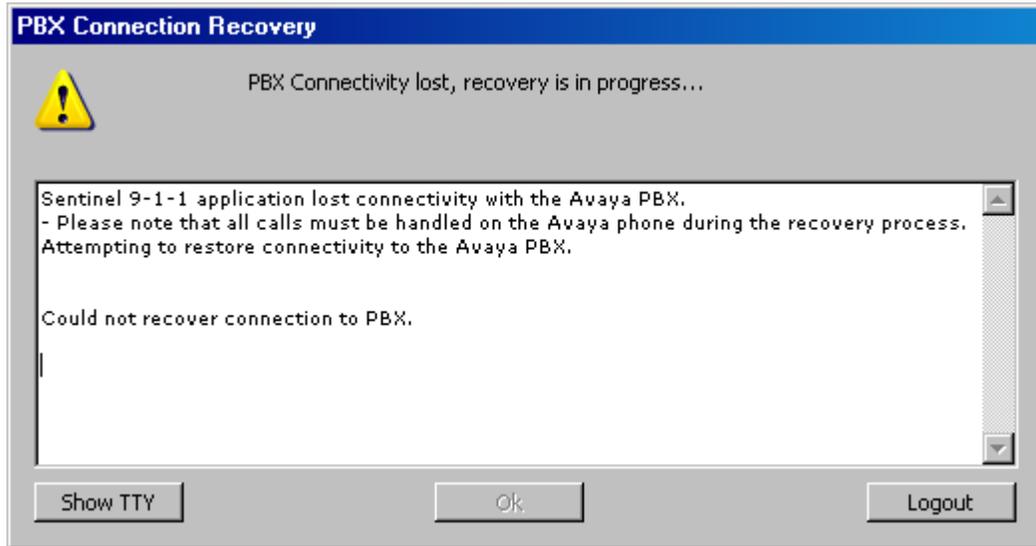
10.2. Incorrect User Name or Password

Following Login Failure screen will appear if incorrect User Name or Password is entered during the Sentinel 9-1-1 application login process. The **User Name** should match the “Agent Login ID” administered in **Section 4.11**. The **Password** should match “password” for the agent.

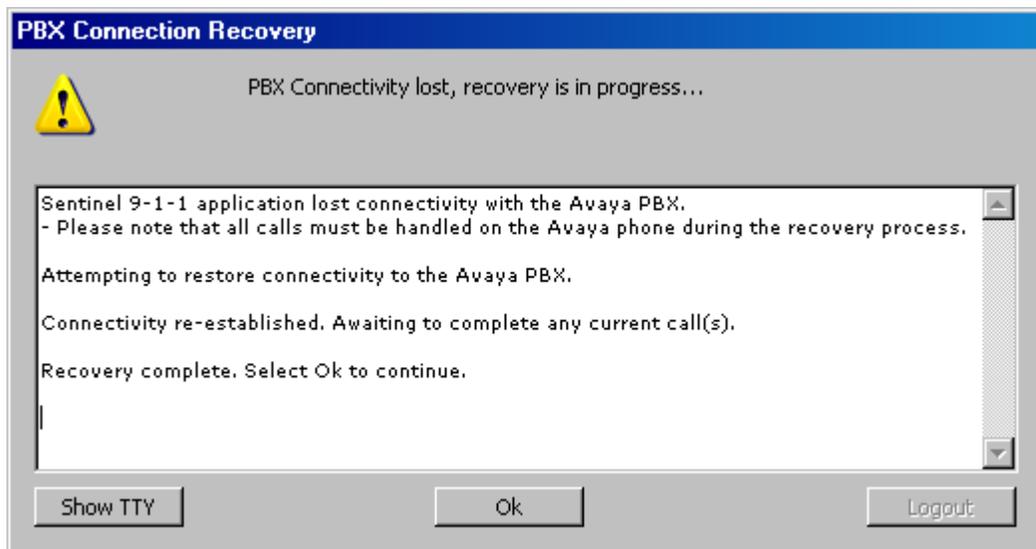


10.3. PBX Connectivity lost

When the Sentinel 9-1-1 Application loses PBX connectivity, a PBX Connection Recovery dialog box will appear. In some cases, the Sentinel 9-1-1 Application is not able to recover and will require the agent to log back into the Sentinel Application as shown below:



In other scenarios, the Sentinel 9-1-1 Application is able to recover and the agent will not have to log back into the Sentinel Application. Clicking Ok will enable the agent to continue, as shown below:



11. 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

12. Conclusion

These Application Notes describe the configuration steps required for PlantCML Sentinel to successfully interoperate with Avaya Communication Manager Release 5.1 and Avaya Application Enablement Services Release 4.2.1.

13. 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 555-230-716, 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. *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*.
6. *Application Notes for Raytheon JPS ACU-2000IP with Avaya Communication Manager and Avaya SIP Enablement Services Release 5.1*.
7. *Application Notes for PlantCML Sentinel CM Release 2.0 with Avaya Communication Manager with Local Survivable Processor and Avaya Application Enablement Services Release 4.2*.

©2009 Avaya Inc. All Rights Reserved.

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

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