



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Genesis Systems Corporation Genesis PSAP Monitor with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Genesis Systems Corporation Genesis PSAP Monitor application with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager.

Genesis PSAP Monitor interfaces with Avaya Aura® Application Enablement Services Device, Media and Call Control to provide real-time information on offered, active and completed calls for Public Safety Answer Points & Downstream Agencies.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

# 1. Introduction

These Application Notes describe the procedures for configuring Genesis Systems Corporation Genesis PSAP Monitor (Genesis PSAP Monitor) application with Avaya Aura® Application Enablement Services (Application Enablement Services) and Avaya Aura® Communication Manager (Communication Manager).

Genesis PSAP Monitor interfaces with Application Enablement Services to provide real-time information on offered, active and completed calls for Public Safety Answer Points & Downstream Agencies. The information collected from Application Enablement Services is formatted into Q-type records that are identical to the one in Avaya Communication Server 1000 (Communication Server 1000) system call detail records and then forwarded to the Public Safety Answer Points.

Genesis PSAP Monitor uses the Device, Media and Call Control (DMCC) interface to Application Enablement Services in order to retrieve the necessary fields for generating Q-type records that are similar to the ones seen in Communication Server 1000 call detail records.

From Avaya DMCC .NET Library the following fields are monitored by the Genesis PSAP Monitor application:

- getCallId
- getTrunkGroup
- getTrunkMember
- getDeviceId

The captured data is then formatted into a Q-type record format similar to the one found in Communication Server 1000, and can optionally send the data out via serial port or TCP/IP (as may be required by 911 controllers, depending on whether it supports serial or TCP/IP connection methods).

## 2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of Genesis PSAP Monitor with Avaya infrastructure consisting of Application Enablement Services and Communication Manager. This section also covers the test results.

The interoperability compliance test included feature and serviceability test. The feature test cases were performed manually. Calls were manually placed from the public switched telephone network (PSTN) directly to agents that were active in Communication Manager. For each successful or abandoned call, there is a Q-type call detail record generated. This generated call detail record was verified for accuracy to ensure that it has all the details that are required by the 911 controller.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the server hosting the Genesis PSAP Monitor application and rebooting the server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The general test approach was to make PSTN calls to agents that were active on Communication Manager. For all successful and abandoned calls, the application formatted the collected call detail records to Q-type record format. This Q-type record was then verified to make sure it has all the details that are required by a 911 controller.

### 2.2. Test Results

All test cases passed with the following observation:

- The DMCC service needs to be restarted whenever changes are made to GenesisPSAP.001 file. Refer to [Section 6.4](#).
- During compliance testing only TCP/IP connection of the Genesis PSAP Monitor was tested.

## 2.3. Support

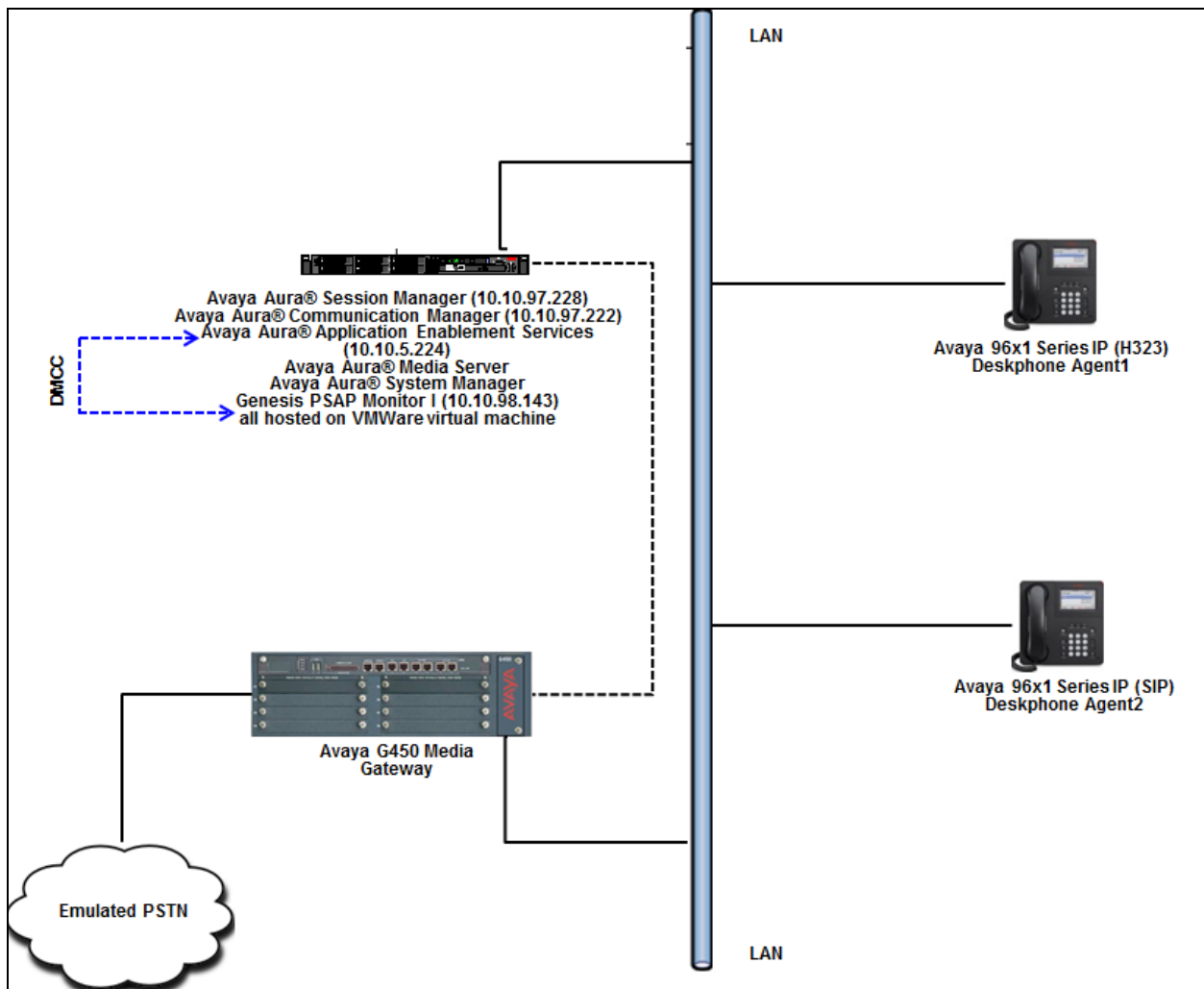
Information, Documentation and Technical support for Genesis products can be obtained at:

- Phone: 1 (888) 993-2288 or 1 (604) 530-9348
- Web: <http://www.buygenesis.com>
- Email: [support@buygenesis.com](mailto:support@buygenesis.com)

### 3. Reference Configuration

**Figure 1** illustrates the setup used to verify the Genesis PSAP Monitor with Application Enablement Services and Communication Manager. Genesis PSAP Monitor is installed and deployed on a Windows Server 2008R2 SP1 running on Virtual Environment. Avaya environment consisted of an Application Enablement Services, Communication Manager, Avaya Aura® Session Manager, Avaya Aura® System Manager, Avaya Aura® Media Server and Avaya G450 Media Gateway. Genesis PSAP Monitor application connected to Application Enablement Services via the DMCC interface.

Avaya environment also consisted of Avaya IP (H323 and SIP) Deskphones which were used by the agents to log in.



**Figure 1: Genesis Systems Corporation Genesis PSAP Monitor solution with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager**

## 4. Equipment and Software Validated

The following equipment and software were used for the reference configuration:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.0.1.2.0-FP1SP2
Avaya Aura® Application Enablement Services running on virtualized environment	7.0.1.0.3.15-0
Avaya Aura® Session Manager running on virtualized environment	7.0.1.2.701230
Avaya Aura® System Manager running on virtualized environment	7.0.1.2 SP2
Avaya Aura® Media Server running on virtualized environment	7.7.0.375
Avaya G450 Media Gateway	37.41.0/1
Avaya 96x1 Series IP Deskphones: <ul style="list-style-type: none"><li>• 9641GS (SIP)</li><li>• 9611G (H323)</li></ul>	7.0.1.1.5 6.6229
Genesis Systems Corporation Genesis PSAP Monitor running on Windows 2008 R2 x64 Standard SP1 on virtualized environment	3.7.2017
DMCC .NET SDK	7.0.0.0.38

## 5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration to support the network shown in [Figure 1](#).

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

### 5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y**. If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                               Page 4 of 12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y                               Audible Message Waiting? y
Access Security Gateway (ASG)? n                                   Authorization Codes? y
Analog Trunk Incoming Call ID? y                                   CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                           Change COR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                                           Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n                                     DCS (Basic)? y
ASAI Link Core Capabilities? y                                     DCS Call Coverage? y
ASAI Link Plus Capabilities? y                                     DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n                             Digital Loss Plan Modification? y
ATM WAN Spare Processor? n                                         DS1 MSP? y
ATMS? y                                                            DS1 Echo Cancellation? y
Attendant Vectoring? y

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

## 5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID (1)** was used in the test) is defined. Also ensure that on page 13 that **Send UCID to ASAI** is set to **y**.

```
change system-parameters features                               Page 5 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
                                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n      MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station  Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y   UCID Network Node ID: 1
```

```
change system-parameters features                               Page 13 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
                                Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? n
  Call Classification After Answer Supervision? n
                                Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```



### 5.3. Administer IP-Services for Application Enablement Services

Add an IP Services entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.

```
change ip-services                                     Page 1 of 4

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

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in [Section 6.1](#).
- In the **Enabled** field, type **y**.

```
change ip-services                                     Page 4 of 4

AE Services Administration

Server ID    AE Services      Password      Enabled      Status
            Server
1:           devvmaes        *             y            in use
```

### 5.4. Administer Computer Telephony Integration (CTI) Link

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type a valid extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 1                                       Page 1 of 3

CTI LINK

CTI Link: 1
Extension: 56000
Type: ADJ-IP
Name: DevvmAES                                     COR: 1
```

## 6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter <https://<ip-addr>> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure Genesis PSAP Monitor User
- Administer Device, Media and Call Control Port
- Restart Device, Media and Call Control Service

Welcome: User cust  
Last login: Fri Mar 10 14:45:49 2017 from 10.98.71  
Number of prior failed login attempts: 0  
HostName/IP: devvmaes/10.97.224  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.3.15-0  
Server Date and Time: Wed Mar 22 11:13:42 EDT 2017  
HA Status: Not Configured

Home Home | Help | Logout

AVAYA Application Enablement Services Management Console

Home

Home | Help | Logout

Navigation Panel:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

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

## 6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection (e.g. **DevvmCM**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in [Section 5.3](#) and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

### Connection Details - DevvmCM

Switch Password

Confirm Switch Password

Msg Period  Minutes (1 - 72)

Provide AE Services certificate to switch

Secure H323 Connection

Processor Ethernet

The display returns to the **Switch Connections** screen which shows that the **DevvmCM** switch connection has been added. This information is required when configuring the Genesis PSAP Monitor as mentioned in [Section 7.1](#).

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance  
Networking

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> DevvmCM	Yes	30	1

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN IP** Address(es). The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
 Communication Manager Interface  
 Switch Connections  
 Dial Plan  
 High Availability  
 Licensing  
 Maintenance

Edit Processor Ethernet IP - DevvmCM

Name or IP Address	Status
10.10.97.222	In Use

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN IP** Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
 Communication Manager Interface  
 Switch Connections  
 Dial Plan  
 High Availability  
 Licensing  
 Maintenance

Edit H.323 Gatekeeper - DevvmCM

Name or IP Address

10.10.97.222

## 6.2. Configure Genesis PSAP Monitor User

In the Navigation Panel, select **User Management** → **User Admin** → **Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list. This information is required by Genesis PSAP Monitor to connect to Application Enablement Services as mentioned in [Section 7.1](#).

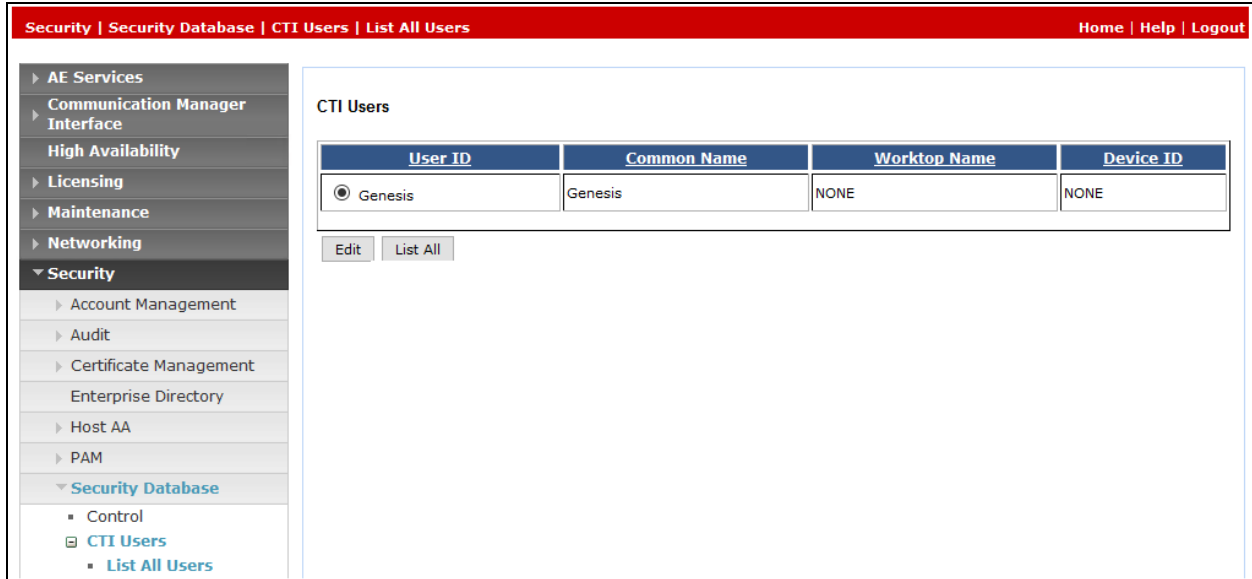
Click **Apply** (not shown) at the bottom of the pages to save the entry.

The screenshot shows a web interface for adding a user. The breadcrumb trail at the top reads "User Management | User Admin | Add User". On the right, there are links for "Home | Help | Logout". A left-hand navigation menu is expanded to "User Management", with "User Admin" and "Add User" selected. The main content area is titled "Add User" and contains the following fields:

- Fields marked with \* can not be empty.
- \* User Id: Text input containing "Genesis"
- \* Common Name: Text input containing "Genesis"
- \* Surname: Text input containing "Genesis"
- \* User Password: Password input (masked with dots)
- \* Confirm Password: Password input (masked with dots)
- Admin Note: Text input (empty)
- Avaya Role: Dropdown menu with "None" selected
- Business Category: Text input (empty)
- Car License: Text input (empty)
- CM Home: Text input (empty)
- Css Home: Text input (empty)
- CT User: Dropdown menu with "Yes" selected
- Department Number: Text input (empty)

If the Security Database (SDB) is enabled on Application Enablement Services, set the Genesis user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** and select the **Genesis** user and click **Edit**.



The screenshot shows a web interface for managing CTI Users. The breadcrumb navigation at the top reads "Security | Security Database | CTI Users | List All Users". On the left is a navigation menu with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Security Database. Under Security Database, "CTI Users" is expanded to show "List All Users". The main content area is titled "CTI Users" and contains a table with the following data:

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> Genesis	Genesis	NONE	NONE

Below the table are two buttons: "Edit" and "List All".

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown).

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

**Edit CTI User**

User Profile:	User ID	Genesis
	Common Name	Genesis
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>

---

Call and Device Control:	Call Origination/Termination and Device Status	None ▾
--------------------------	--	--------

---

Call and Device Monitoring:	Device Monitoring	None ▾
	Calls On A Device Monitoring	None ▾
	Call Monitoring	<input type="checkbox"/>

---

Routing Control:	Allow Routing on Listed Devices	None ▾
------------------	---------------------------------	--------

### 6.3. Administer Device, Media and Call Control Ports

From the Management console, navigate to **Networking** → **Ports**. The following highlighted configurations are needed in **DMCC Server Ports** section:

- **Unencrypted Port:** Enabled and enter the port **4721**. This port is used for Genesis PSAP Monitor server to connect to Application Enablement Services server as mentioned in [Section 7.1](#).

Click on **Apply Changes** and **Apply** (not shown) when finished.

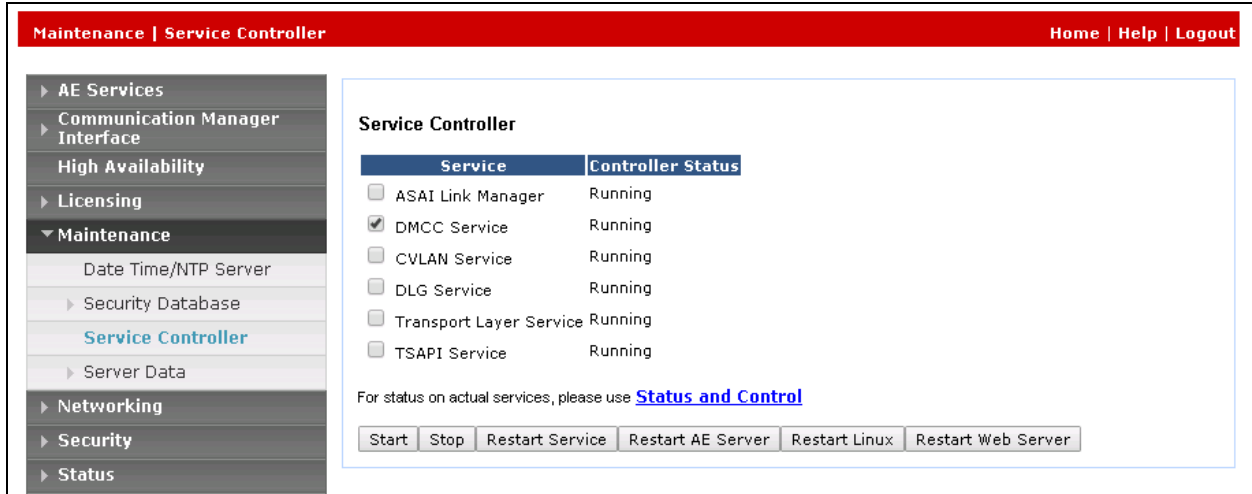
The screenshot shows the 'Networking | Ports' configuration page. The left sidebar contains a navigation menu with 'Ports' highlighted. The main content area is titled 'Ports' and is divided into three sections: CVLAN Ports, TSAPI Ports, and DMCC Server Ports. The DMCC Server Ports section is highlighted with a red box, showing the 'Unencrypted Port' set to 4721 and the 'Enabled' radio button selected. Other ports in the DMCC Server Ports section include 'Encrypted Port' (4722) and 'TR/87 Port' (4723).

Section	Port Name	Port Value	Enabled	Disabled
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted TCP Port	9998	<input type="radio"/>	<input checked="" type="radio"/>
DLG Port	TCP Port	5678		
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
DMCC Server Ports	Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
	Encrypted Port	4722	<input type="radio"/>	<input checked="" type="radio"/>
	TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>



## 6.4. Restart Device, Media and Call Control Service

DMCC service needs to be restarted for the changes to take effect. Navigate to **Maintenance** → **Service Controller**. Select the **DMCC Service** box and click **Restart Service** button to restart the service. This service also needs to be restarted when any changes are made to Genesis PSAP Monitor configuration.



The screenshot shows a web interface for the Service Controller. The top navigation bar is red and contains the text "Maintenance | Service Controller" on the left and "Home | Help | Logout" on the right. A left-hand sidebar menu lists various system components: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (highlighted in blue), Server Data, Networking, Security, and Status. The main content area is titled "Service Controller" and contains a table with two columns: "Service" and "Controller Status".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

Below the table, there is a note: "For status on actual services, please use [Status and Control](#)". At the bottom of the main content area, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

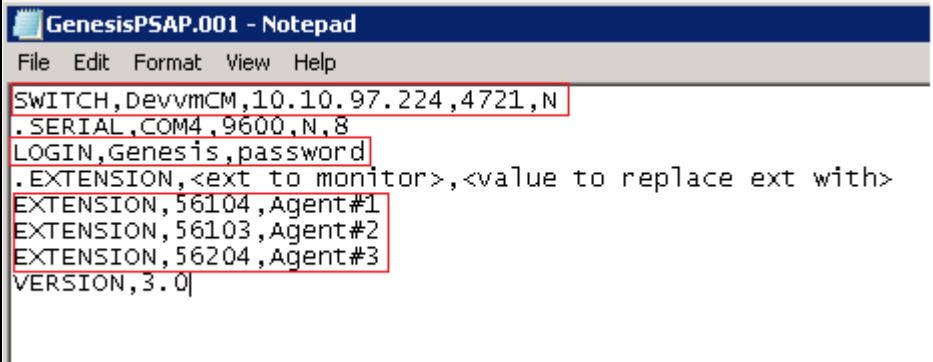
## 7. Configure Genesis Systems Corporation Genesis PSAP Monitor

This section describes the configuration of Genesis PSAP Monitor. It assumes that the application and all required software components have been installed and properly licensed. Genesis engineer or an approved installer will install and initially configure all server components. Details of the steps are beyond the scope of this document. For further documentation and references, refer to [Section 10](#).

### 7.1. Configure GenesisPSAP.001 File

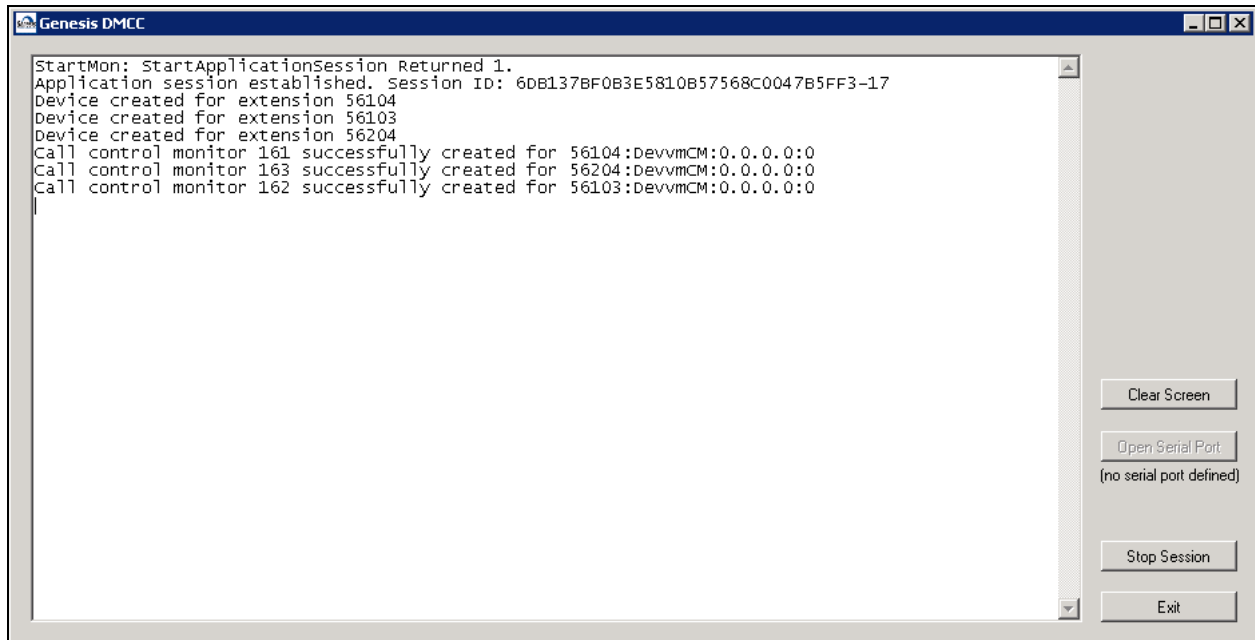
The **GenesisPSAP.001** file needs to be configured for Genesis PSAP Monitor to connect to Application Enablement Services. This file can be typically found in the installation folder, where the application is installed on the server. During compliance testing the file path for GenesisPSAP.001 was, **/Desktop/GenesisPSAP/**. Open the file in a notepad as shown below and configure the following:

- Name of the switch as configured in Application Enablement Services. During compliance testing **DevvmCM** was configured as mentioned in [Section 6.1](#).
- IP Address of Application Enablement Services.
- DMCC port of Application Enablement Services as mentioned in [Section 6.3](#).
- Specify if the connection is unsecure or secure. During compliance testing the connection was set to unsecure, which is **N**.
- Enter the user name and password of the Genesis user that was configured in Application Enablement Services in [Section 6.2](#).
- Enter the agent extensions that need to be monitored and assign a value for the same. During compliance testing extensions **56104**, **56103** and **56204** were monitored.



```
GenesisPSAP.001 - Notepad
File Edit Format View Help
SWITCH, DevvmCM, 10.10.97.224, 4721, N
.SERIAL, COM4, 9600, N, 8
LOGIN, Genesis, password
.EXTENSION, <ext to monitor>, <value to replace ext with>
EXTENSION, 56104, Agent#1
EXTENSION, 56103, Agent#2
EXTENSION, 56204, Agent#3
VERSION, 3.0
```

Run the **GenesisPSAP.exe** that is typically found in the installation folder, where the application is installed on the server. During compliance testing the file path for GenesisPSAP.exe was, **/Desktop/GenesisPSAP/**. Screen below shows the Genesis PSAP Monitor successfully connected to Application Enablement Services and monitoring the configured agent extensions.



## 8. Verification Steps

The following information verifies the integration between Genesis PSAP Monitor application and Application Enablement Services and also the accuracy of the Q-type call detail record generated.

Check status of connections from Genesis PSAP Monitor server to Application Enablement Services server by navigating to **Status** → **Status and Control** → **DMCC Service Summary**. The **DMCC Service Summary-Session Summary** window is displayed in the right pane as shown below. Verify the **User** column shows an active session with the CTI user name from **Section 6.2**, and that the **# of Associated Devices** column reflects the number of agent extensions that are being monitored as configured in **Section 7.1**.

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
- Alarm Viewer
- ▶ Log Manager
- ▶ Logs
- ▼ Status and Control
- CVLAN Service Summary
- DLG Services Summary
- DMCC Service Summary
- Switch Conn Summary
- TSAPI Service Summary
- ▶ User Management
- ▶ Utilities
- ▶ Help

### DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every  seconds

Session Summary [Device Summary](#)  
Generated on Wed Mar 22 16:05:10 EDT 2017

Service Uptime: 14 days, 4 hours 21 minutes

Number of Active Sessions: 3

Number of Sessions Created Since Service Boot: 18

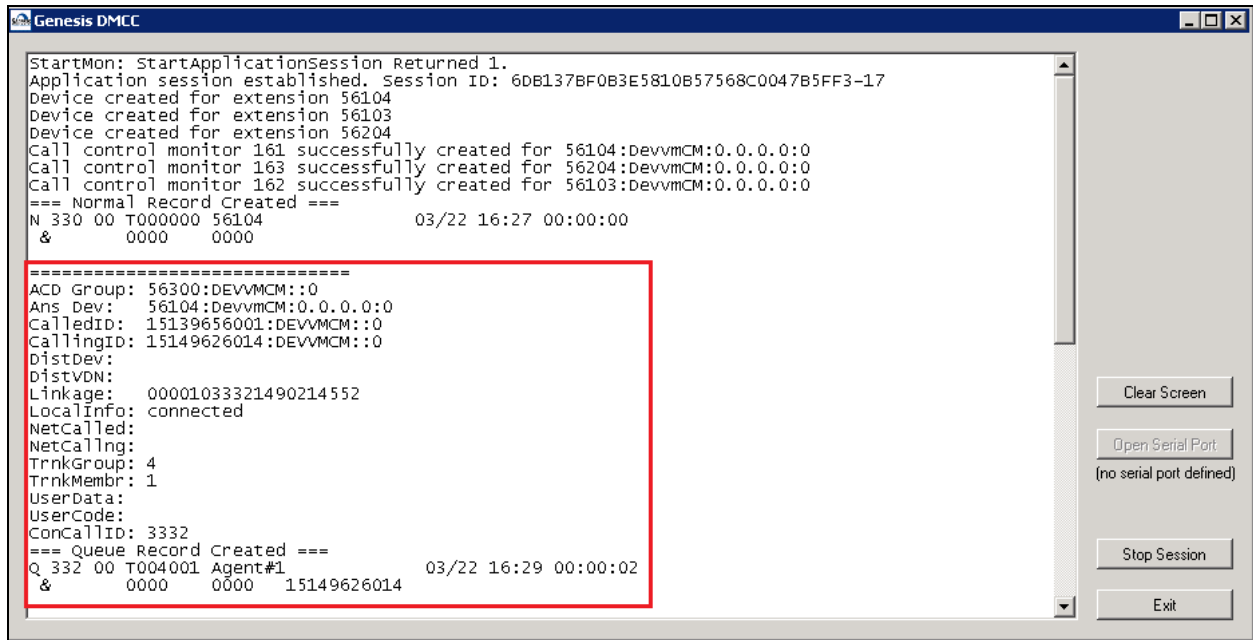
Number of Existing Devices: 15

Number of Devices Created Since Service Boot: 88

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	6DB137BF083E5810B 57568C0047B5FF3-17	Genesis	Genesis PSAP Monitor	10.10.98.143	XML Unencrypted	3

Item 1-3 of 3  
1  Go

Calls were made from PSTN to an active agent and call record details that was formatted in Q-type record were verified for accuracy. Screen below shows the information collected from Application Enablement Services being formatted into a Q-type call detail record.



## 9. Conclusion

These Application Notes describe the procedures required to configure Genesis Systems Corporation Genesis PSAP Monitor to interoperate with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to support the network shown in [Figure 1](#). Genesis Systems Corporation Genesis PSAP Monitor passed compliance testing with the observations noted in [Section 2.2](#).

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2 May 2016.
2. *Deploying Avaya Aura® System Manager*, Release 7.0.1, Issue 2 August 2016.
3. *Administering Avaya Aura® System Manager for Release 7.0.1*, Release 7.0.1, Issue 3 January 2017.
4. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, 03-300509, Issue 2.1 August 2016.
5. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0.1, 555-245-205, Issue 3 October 2016.
6. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*, Release 7.0.1 November 2016.
7. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016

Product documentation for Genesis PSAP Monitor may be obtained from Genesis Systems Corporation.

---

**©2017 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](mailto:devconnect@avaya.com).