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

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.

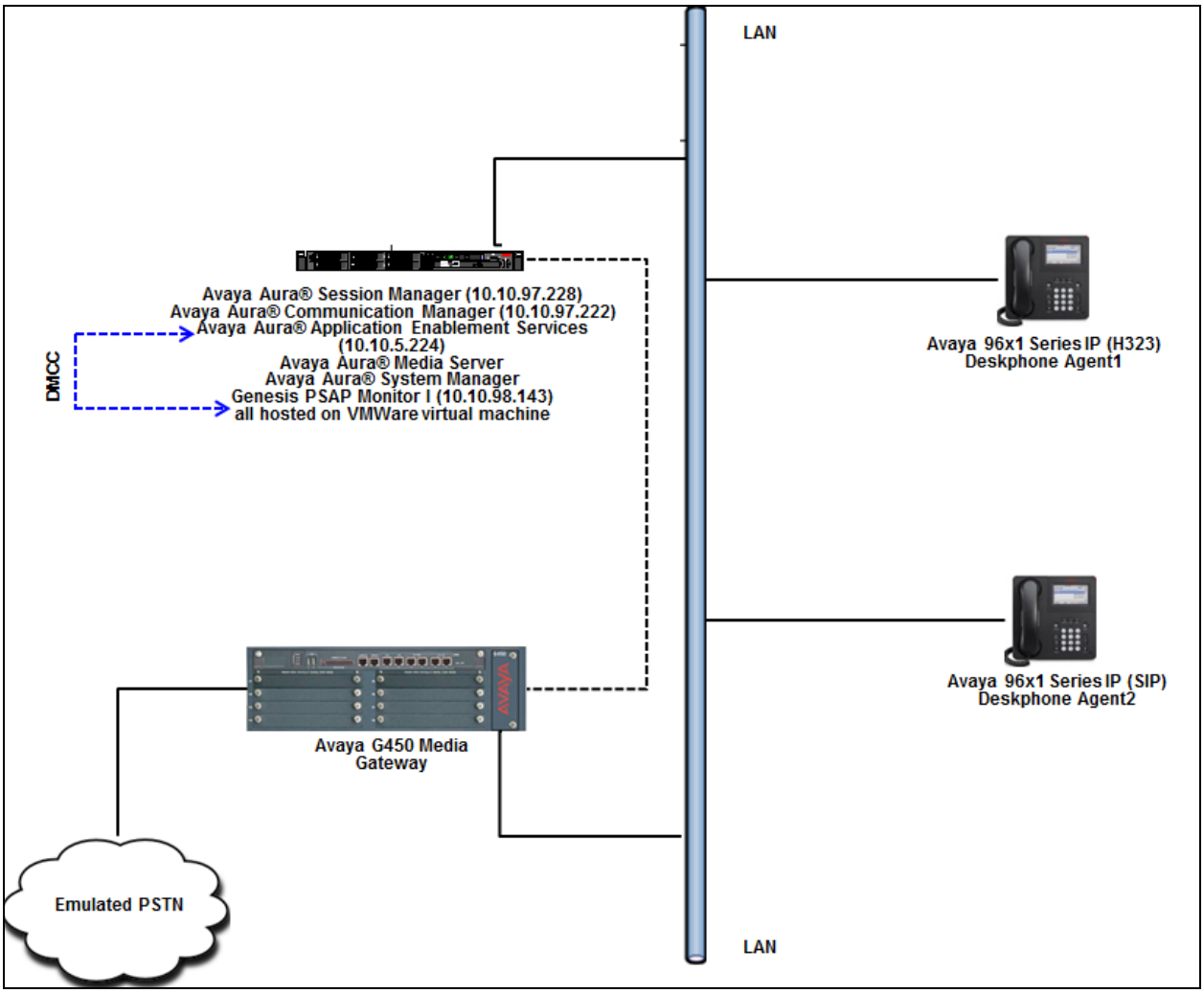


Figure 1: Genesis Systems Corporation Genesis PSAP Monitor solution with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager

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: • 9641GS (SIP) • 9611G (H323)	 7.0.1.1.5 6.6229
Genesis Systems Corporation Genesis PSAP Monitor running on Windows 2008 R2 x64 Standard SP1 on virtualized environment DMCC .NET SDK	3.7.2017 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 UUI 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

                                    IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         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.

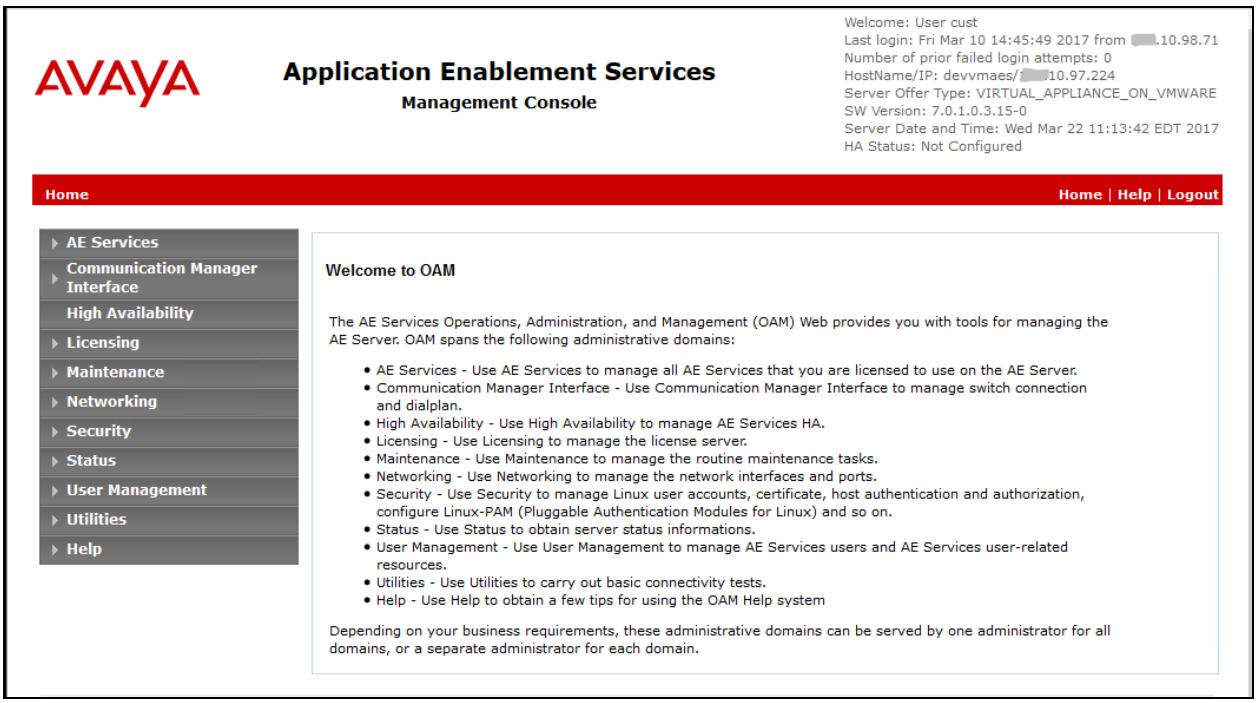
```
add cti-link 1                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 56000
     Type: ADJ-IP
                                                                      COR: 1
     Name: DevvmAES
```

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.

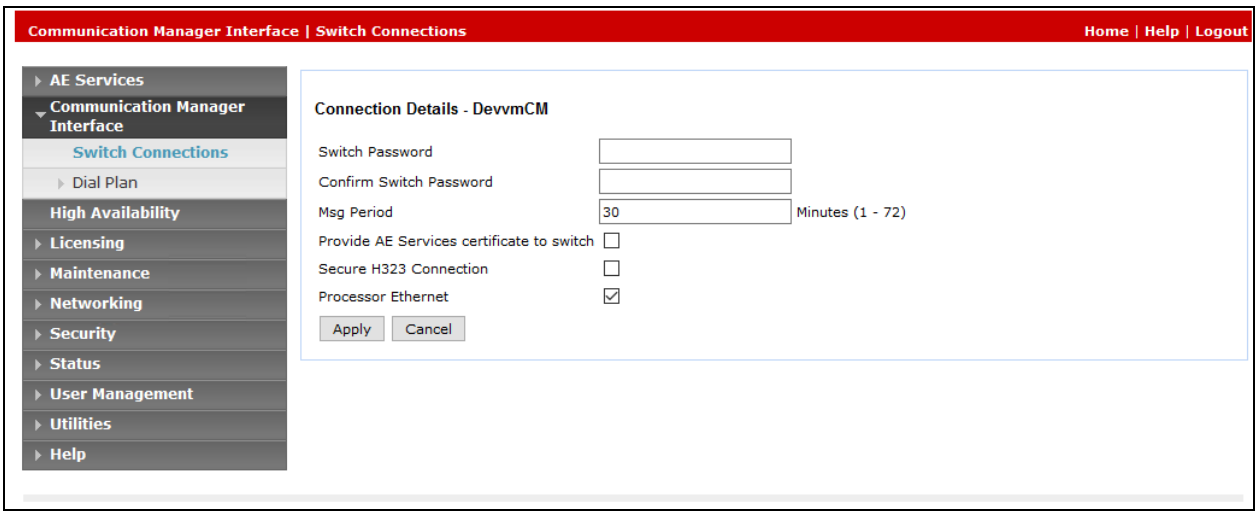
The procedures fall into the following areas:

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

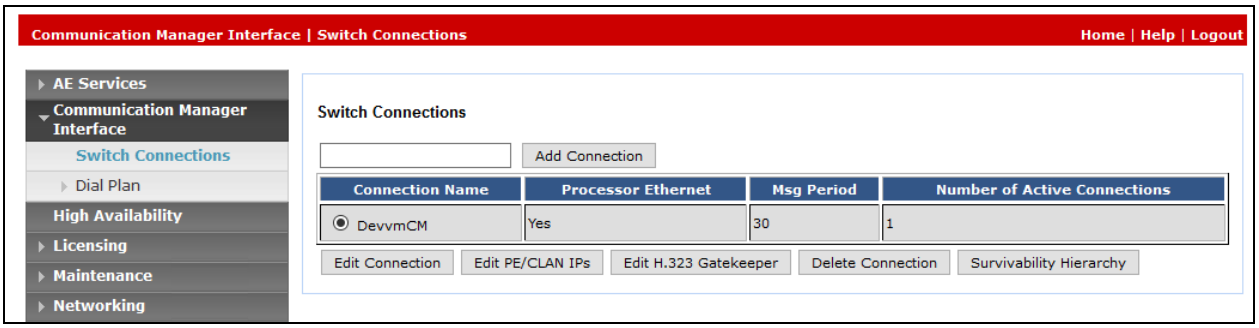


6.1. Configure Communication Manager Switch Connections

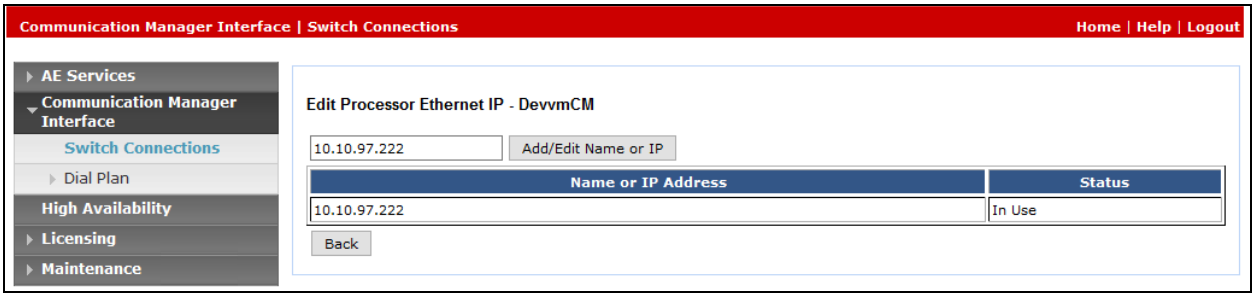
To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **DevvmCM**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password**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



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**.



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.

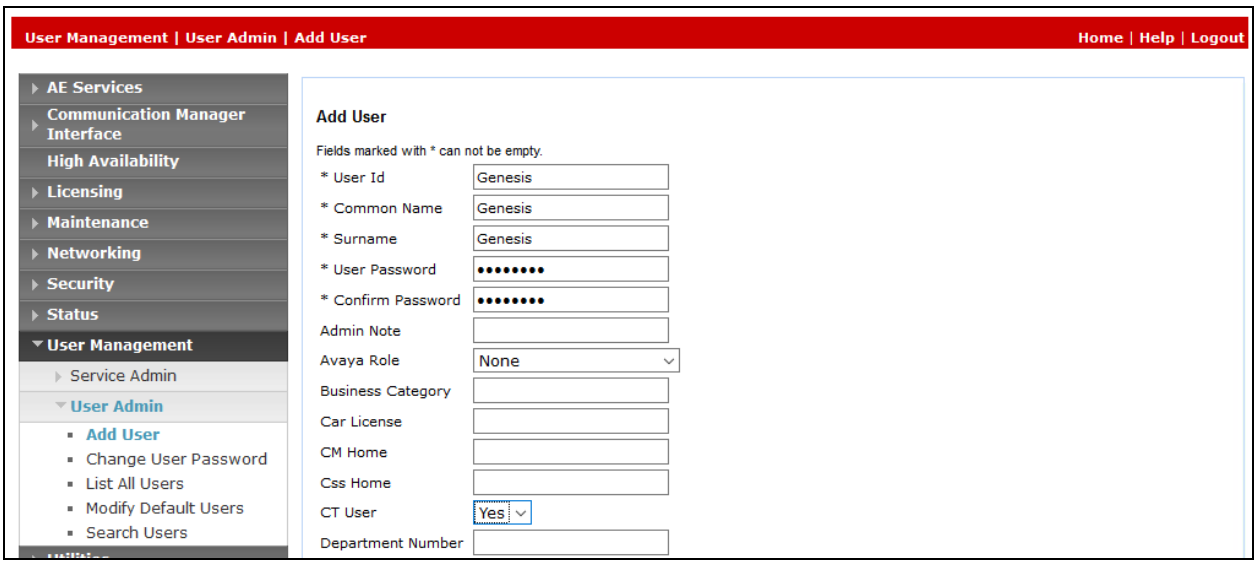


Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

6.2. Configure Genesis PSAP Monitor User

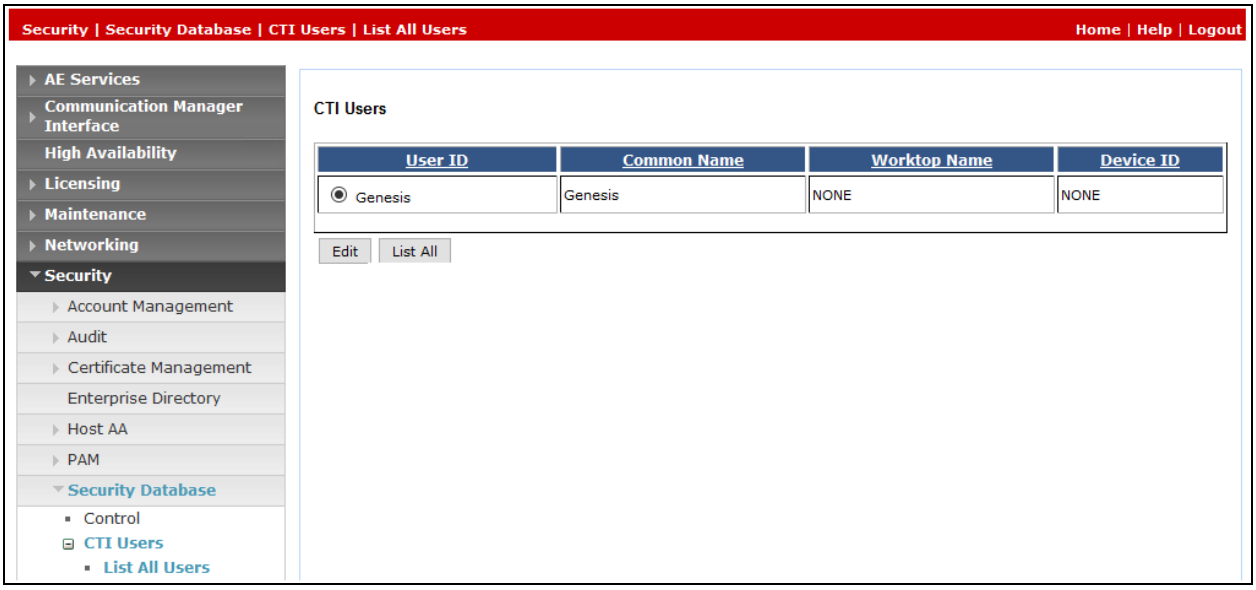
In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list. This information is required by Genesis 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.

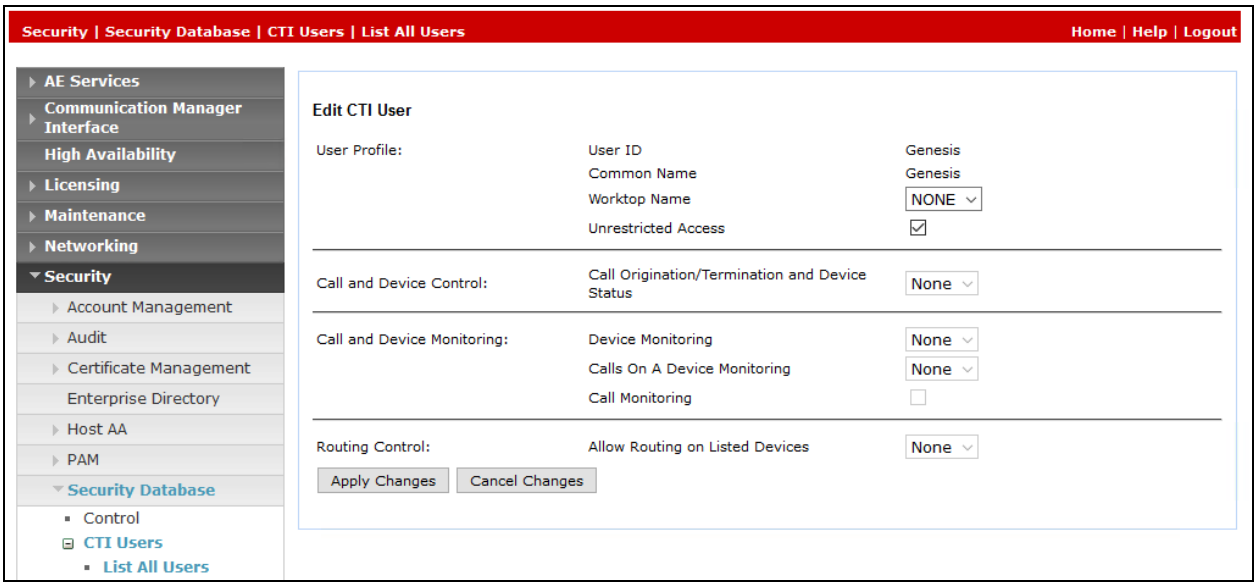


If the Security Database (SDB) is enabled on Application Enablement Services, set the Genesis user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

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



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).

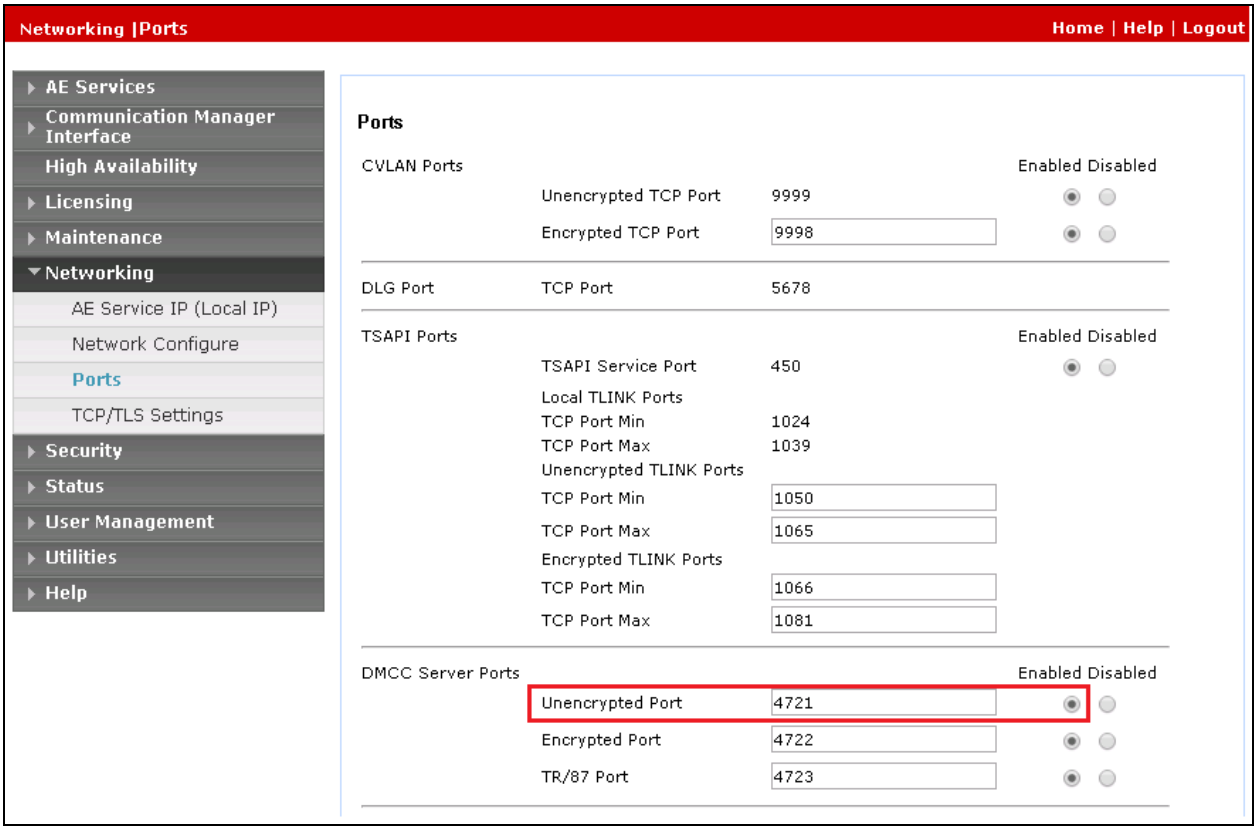


6.3. Administer Device, Media and Call Control Ports

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

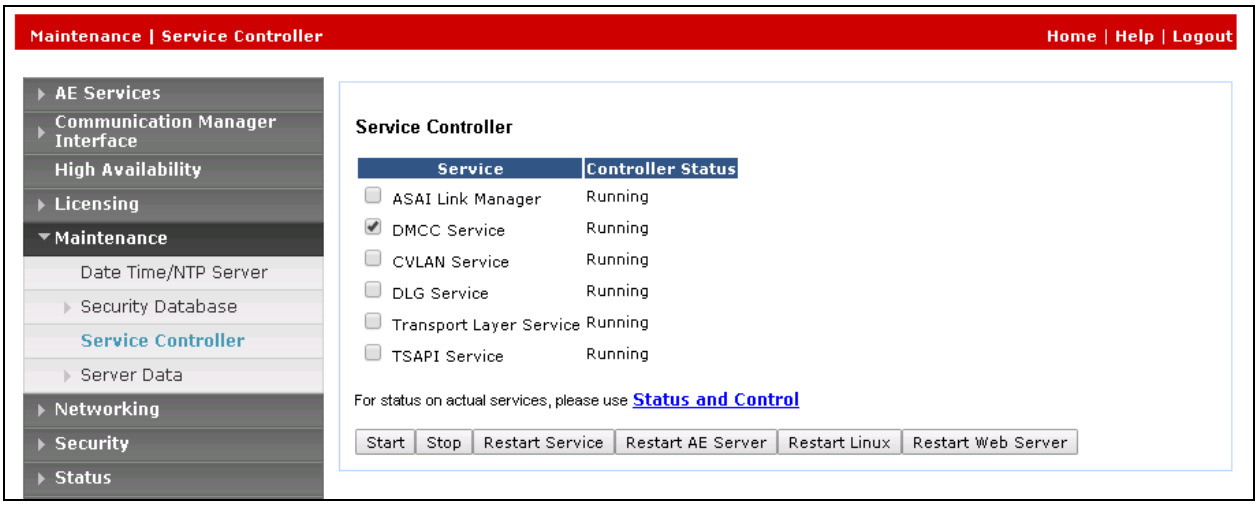
- **Unencrypted Port**: Enabled and enter the port **4721**. This port is used for Genesis PSAP Monitor server to connect to Application Enablement Services server as mentioned in **Section 7.1**.

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



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.



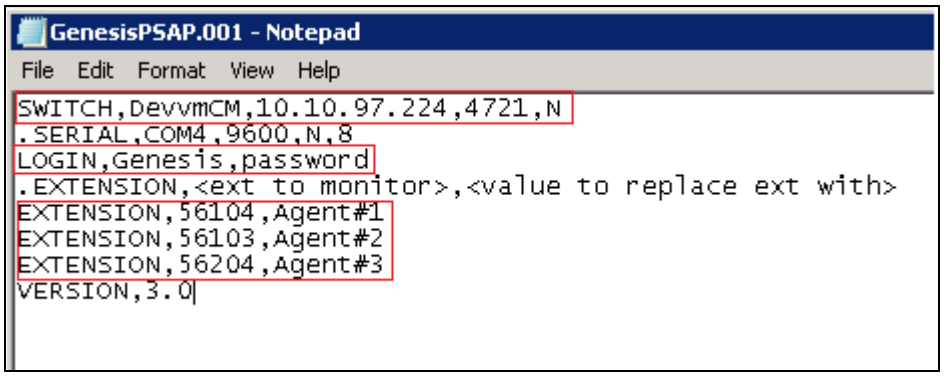
7. Configure Genesis Systems Corporation Genesis PSAP Monitor

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**.

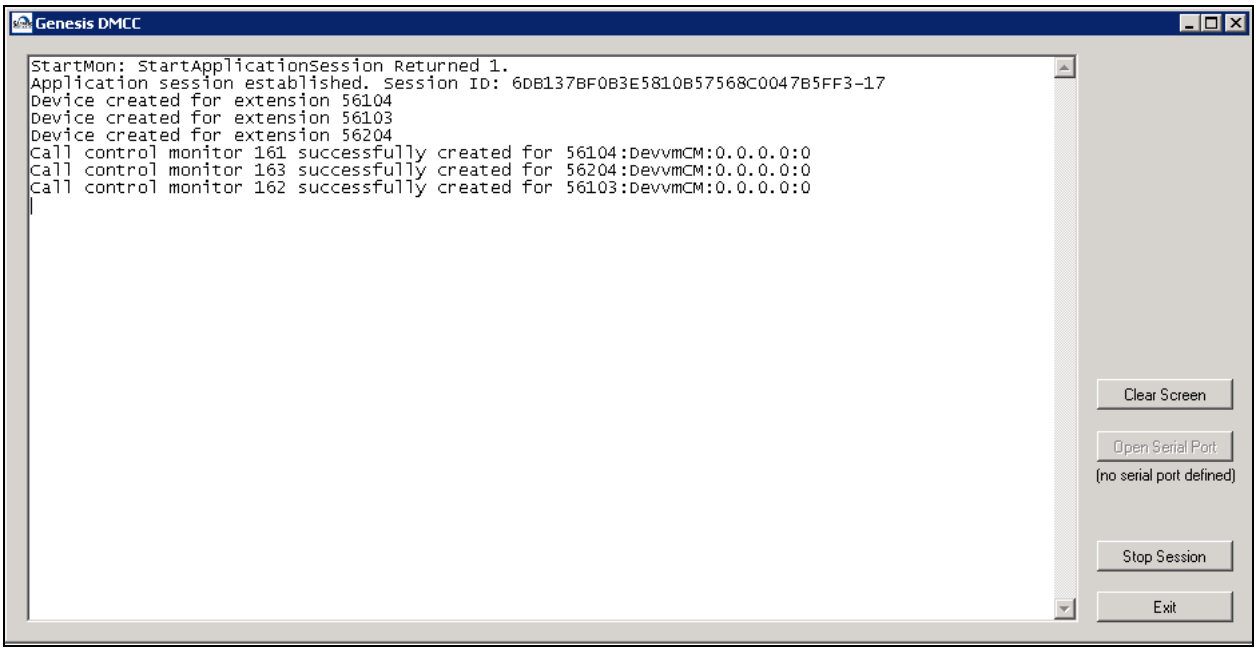
7.1. Configure GenesisPSAP.001 File

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.



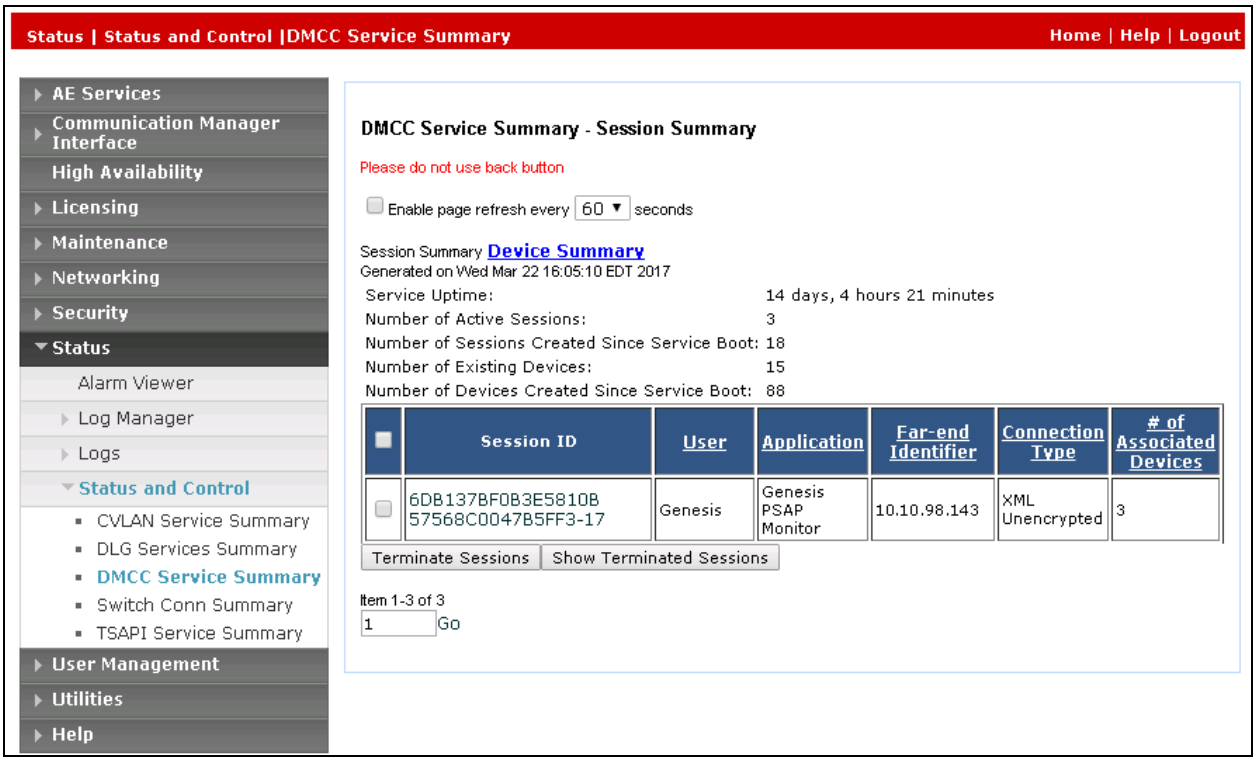
Run the **GenesisPSAP.exe** that is typically found in the installation folder, where the application is installed on the server. During compliance testing the file path for GenesisPSAP.exe was, **/Desktop/GenesisPSAP/**. Screen below shows the Genesis PSAP Monitor successfully connected to Application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



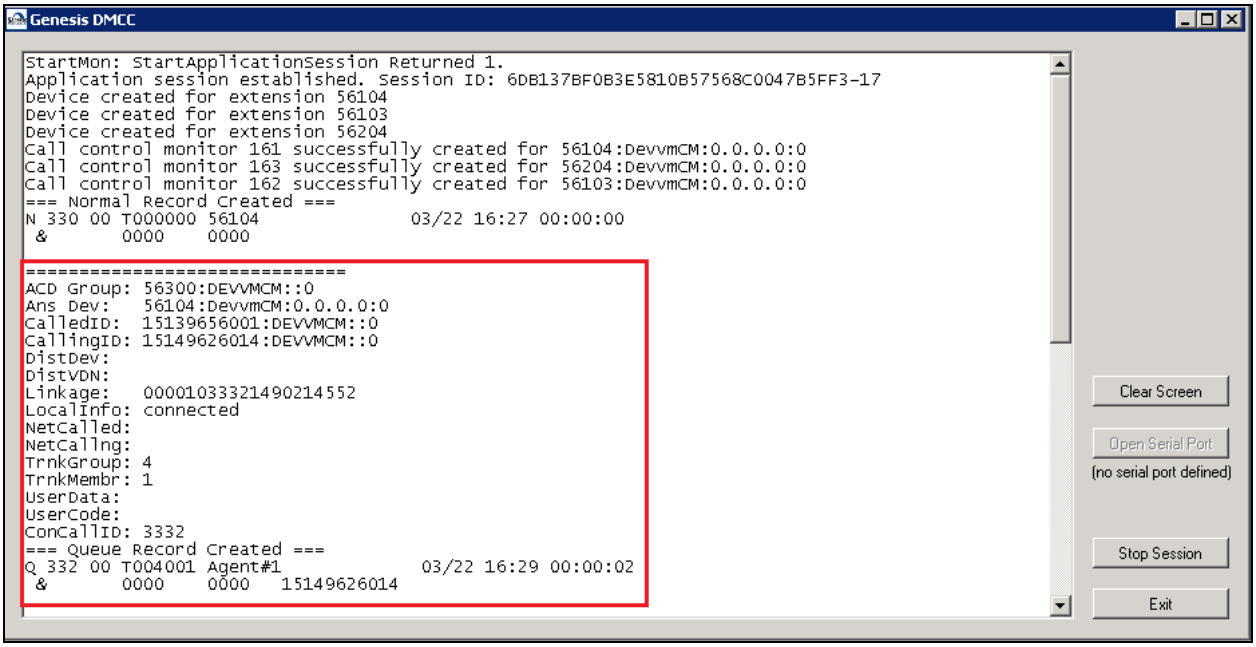
8. Verification Steps

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.**



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.

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.