



Application Notes for Valcom VE6025 Application Server Pro with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Valcom VE6025 Application Server Pro to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Valcom VE6025 Application Server Pro is a multi-purpose mass notification solution.

In the compliance testing, Valcom VE6025 Application Server Pro used the SNMP interface from Avaya Aura® Communication Manager, and the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to provide monitoring and on-site notification of emergency calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any 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 configuration steps required for Valcom VE6025 Application Server Pro (VE6025) to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. VE6025 is a multi-purpose mass notification solution.

In the compliance testing, VE6025 used the SNMP version 1 interface from Communication Manager, and the Device, Media, and Call Control (DMCC) Java interface from Application Enablement Services to provide monitoring and on-site notification of emergency calls.

The DMCC interface is used by VE6025 to register a virtual IP softphone to Communication Manager for monitoring of emergency call. The virtual IP softphone is configured with a crisis alert button, such that when a user on Communication Manager dials an emergency call, the virtual IP softphone will receive events associated with audible and visual alerts. VE6025 obtains the emergency caller name and extension from the DMCC interface, uses SNMP to obtain location information associated with the emergency caller, and sends alerts to audio and/or visual points that are connected to VE6025.

The supported alert points can include led display signage, IP speakers, email notifications, etc. In the compliance testing, two IP speakers were used for verification of emergency call alerts.

2. General Test Approach and Test Results

The feature test cases were performed manually. Emergency calls were placed manually from users on Communication Manager to the emulated PSTN.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the VE6025 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 interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on VE6025:

- Use of DMCC registration services to register and un-register virtual IP softphone.
- Use of DMCC physical devices services and monitoring services to obtain audio and visual alerts events for emergency calls.
- Use of SNMP interface to obtain emergency caller station building, floor, and room information.
- Proper alerting of emergency calls including user name, extension, dialed digits, building, room, and floor.
- Proper handling of emergency call scenarios involving emergency callers from different users, simultaneous emergency calls, and simultaneous notification to all alert points.

The serviceability testing focused on verifying the ability of VE6025 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the VE6025 server.

2.2. Test Results

All test cases were executed and verified. The following were observations on VE6025 from the compliance testing.

- The system setup information on the crisis alert tab may not be displayable after it has been configured. Even when non displayable, the configured information appeared to be retained with subsequent emergency calls alerted the alert points.
- When the Every User Responds parameter on the system-parameters crisis-alert form was disabled on Communication Manager, then the crisis alert notification got acknowledged by VE6025 via the virtual IP softphone and therefore cleared at all other user stations faster than the other user stations can view the crisis alert details. Therefore, the configuration of the Every User Responds parameter needs to take this observation into account.
- The current release of VE6025 assumes the same Communication Manager C-LAN interface is used for both SNMP and DMCC. Therefore, the DMCC H.323 gatekeeper must be configured to use the Processor C-LAN, as noted in **Section 6.3**.

2.3. Support

Technical support on VE6025 can be obtained through the following:

- **Phone:** (800) 825-2661
- **Email:** support@valcom.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of Communication Manager resources are not the focus of these Application Notes and will not be described.

In the compliance testing, two IP speakers were used for broadcast alert of all emergency calls.

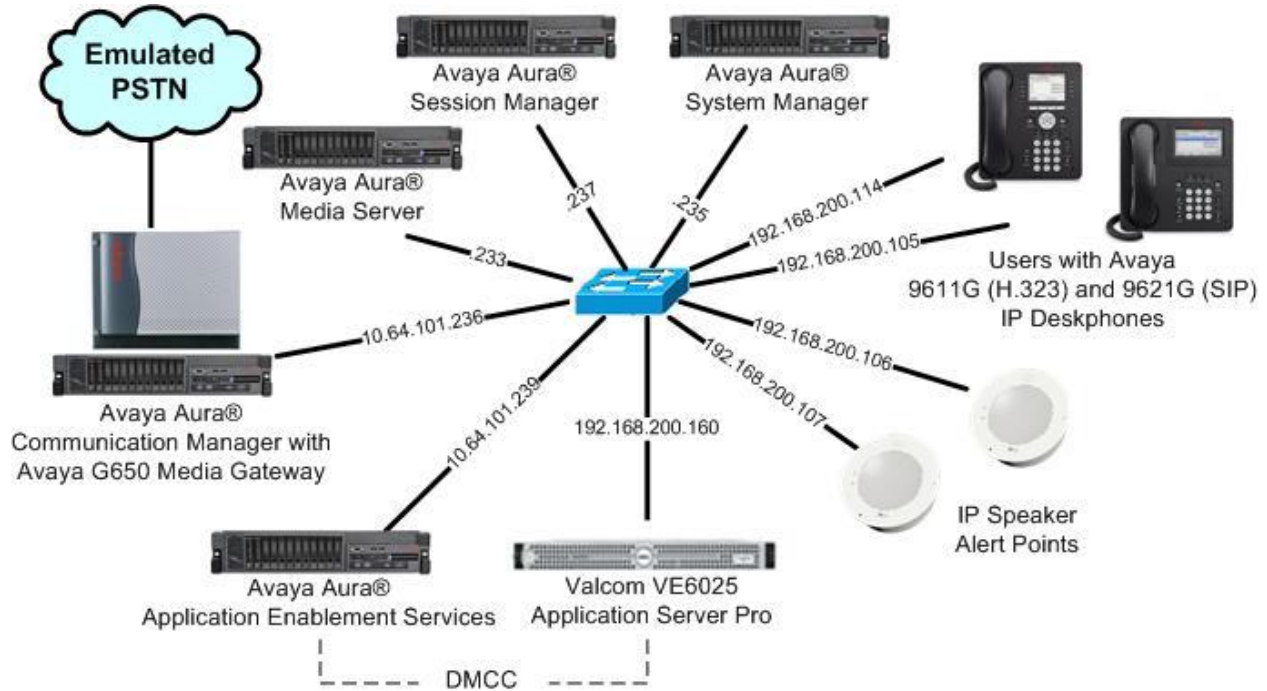


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0 .1 (7.0.1.0.701007)
Avaya Aura® System Manager in Virtual Environment	7.0 .1 (7.0.1.0.064859)
Avaya 9611G IP Deskphones (H.323)	6.6302
Avaya 9621G IP Deskphone (SIP)	7.0.1.2.9
Valcom VE6025 Application Server Pro on CentOS <ul style="list-style-type: none">Avaya DMCC Java SDK	4.8.0-201701170904-48e75ac 6.3 6.3.3.0.107

5. Configure Avaya Aura® Communication Manager

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

- Administer virtual IP softphone
- Administer ARS analysis
- Administer system parameters crisis alert
- Launch maintenance web interface
- Administer SNMP access

5.1. Administer Virtual IP Softphone

Log in to the System Access Terminal, and add a virtual IP softphone 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.

- **Extension:** The available extension number.
- **Type:** “9630”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **IP SoftPhone:** “y”

```
add station 65991                                     Page 1 of 5
                                                    STATION
Extension: 65991                                Lock Messages? n                BCC: 0
Type: 9630                                       Security Code: 123456          TN: 1
Port: IP                                           Coverage Path 1:                COR: 1
Name: VE6025 Virtual #1                          Coverage Path 2:                COS: 1
                                                    Hunt-to Station:                Tests: y

STATION OPTIONS
    Location:                                       Time of Day Lock Table:
    Loss Group: 19                                Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 65991
    Speakerphone: 2-way                            Mute Button Enabled? y
    Display Language: english                       Button Modules: 0
Survivable GK Node Name:
    Survivable COR: internal                        Media Complex Ext:
    Survivable Trunk Dest? y                       IP SoftPhone? y
                                                    IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? Y
```

Navigate to **Page 4**, and assign a “crss-alert” button for notification of emergency calls.

```

add station 65991                                     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:
2: call-appr                                       6:
3: call-appr                                       7:
4: crss-alert                                   8:

voice-mail
  
```

5.2. Administer ARS Analysis

Use the “change ars analysis n” command, where “n” is the applicable emergency call digit string, in this case “911”.

Locate the entry associated with the emergency call digit string, and make certain **Call Type** is set to “alrt”, which activates emergency notification.

```

change aar analysis 911                             Page 1 of 2
                                                    ARS DIGIT ANALYSIS TABLE
                                                    Location: all                               Percent Full: 1
Dialed      Total      Route      Call      Node      ANI
String      Min Max    Pattern   Type     Num      Reqd
911      3  3    911    alrt
  
```


5.3. Administer System Parameters Crisis Alert

Use the “change system-parameters crisis-alert” command, and set **Every User Responds** to the desired setting.

When the parameter is enabled, all users with crisis alert button are notified and must clear the alert for every emergency alert.

When the parameter is disabled, all users with crisis alert button are notified and only one user needs to acknowledge an alert. When the alert is acknowledged by one user, the alert is cleared at all other users except the one that acknowledged the alert.

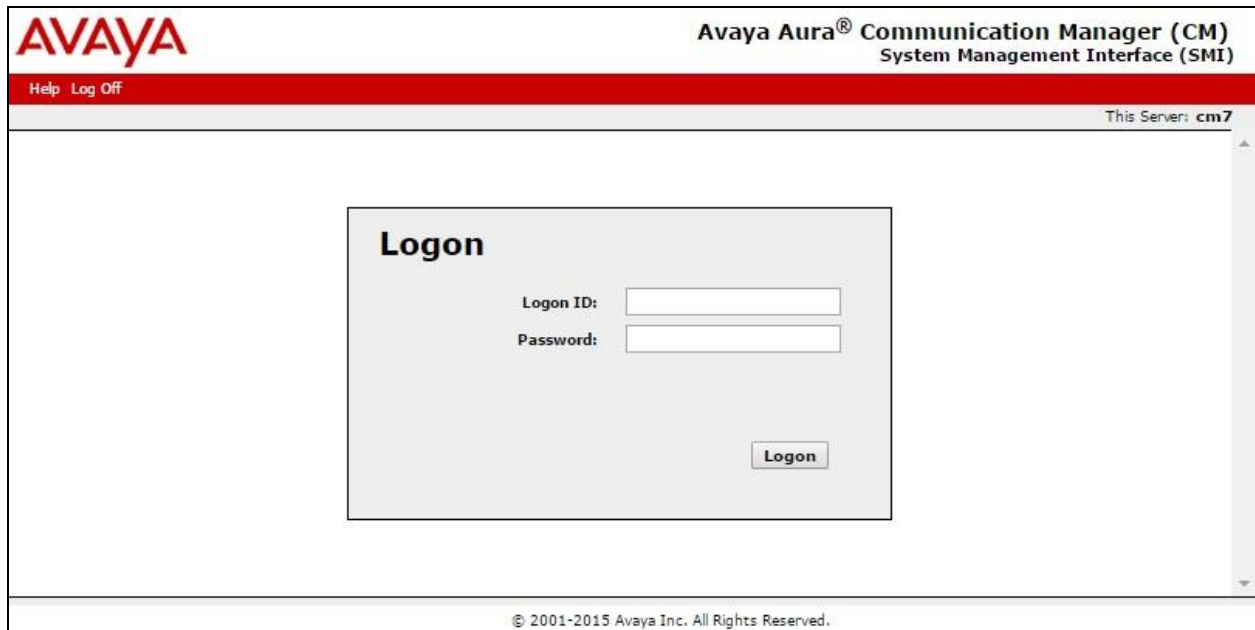
```
change system-parameters crisis-alert                               Page 1 of 1
                        CRISIS ALERT SYSTEM PARAMETERS

ALERT STATION
  Every User Responds? y

ALERT PAGER
  Alert Pager? n
```

5.4. Launch Maintenance Web Interface

Access the Communication Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of Communication Manager. Log in using the appropriate credentials.



In the subsequent screen, select **Administration → Server (Maintenance)** from the top menu, to display the **Server Administration** screen below.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm7. The top navigation bar includes 'Help Log Off' and 'Administration'. The left sidebar menu is expanded to 'Administration / Server (Maintenance)'. The main content area is titled 'Server Administration' and contains a welcome message: 'Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server. Please use the menu to the left for navigation.' The sidebar menu includes sections for Alarms, SNMP (with 'Agent Status' selected), Diagnostics, and Server.

5.5. Administer SNMP Access

Select **SNMP → Agent Status** from the left pane, to display the **Agent Status** screen. Click **Stop Master Agent**.

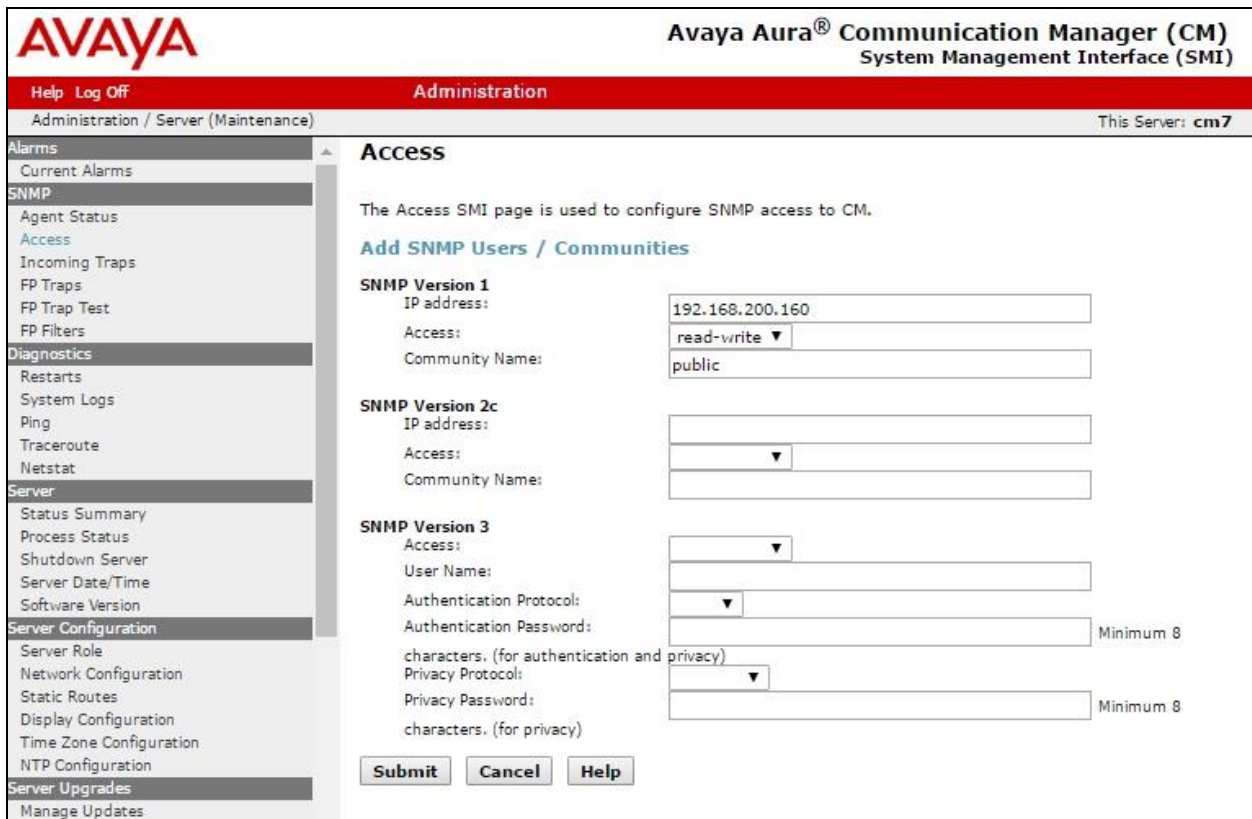
The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm7, displaying the 'Agent Status' screen. The top navigation bar includes 'Help Log Off' and 'Administration'. The left sidebar menu is expanded to 'Administration / Server (Maintenance)'. The main content area is titled 'Agent Status' and contains the following information: 'The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent. All of the Sub Agents are connected to the Master Agent. Master Agent status: UP'. Below this, there is a section for 'Sub Agent Status' with the following information: 'FP Agent status: UP', 'CMSubAgent status: UP', and 'Load Agent status: UP'. At the bottom of the main content area, there are two buttons: 'Stop Master Agent' and 'Help'. The sidebar menu includes sections for Alarms, SNMP (with 'Agent Status' selected), Diagnostics, and Server.

Select **SNMP** → **Access** from the left pane, to display the **Access** screen. Click **Add/Change**.



The **Access** screen is updated, as shown below. In the **SNMP Version 1** sub-section, enter the following values for the specified fields. Upon submittal, Master Agent will start automatically.

- **IP address:** IP address of the VE6025 server.
- **Access:** “read-write”
- **Community Name:** A desired string.



6. Configure Avaya Aura® Application Enablement Services

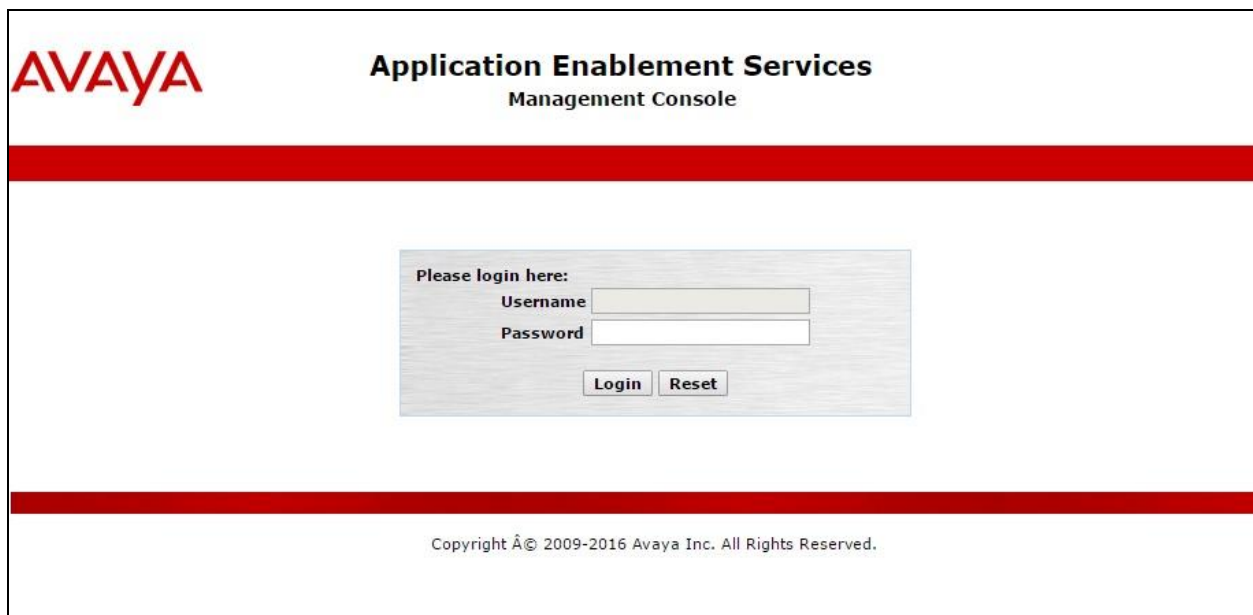
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer H.323 gatekeeper
- Administer VE6025 user
- Administer security database
- Administer ports
- Restart service

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services" and "Management Console". Below this is a red horizontal bar. The main content area contains a login form with the heading "Please login here:". The form includes two input fields: "Username" and "Password". Below the fields are two buttons: "Login" and "Reset". At the bottom of the page, there is a red horizontal bar and a copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Feb 21 09:51:47 2017 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Feb 21 10:37:07 EST 2017', and 'HA Status: Not Configured'. A red navigation bar at the top contains 'Home | Help | Logout'. On the left, a sidebar menu lists: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Welcome to OAM' and contains the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. A bulleted list follows: '• 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'. Below the list, it states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.'

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' page selected. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Feb 21 09:51:47 2017 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Feb 21 10:37:07 EST 2017', and 'HA Status: Not Configured'. A red navigation bar at the top contains 'Home | Help | Logout'. On the left, a sidebar menu lists: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing' (expanded to show 'WebLM Server Address', 'WebLM Server Access', and 'Reserved Licenses'), 'Maintenance', and 'Networking'. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:'. A bulleted list follows: '• WebLM Server Address'. Below that, it says: 'If you are importing, setting up and maintaining the license, you need to use the following:'. A bulleted list follows: '• WebLM Server Access'. Finally, it says: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:'. A bulleted list follows: '• Reserved Licenses'.

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there is sufficient license for **Device Media and Call Control**, as shown below.

Application Enablement (CTI) - Release: 7 - SID: 10503000 Standard

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: October 12, 2015 2:21:49 PM -05:00

License File Host IDs: V1-19-37-80-8F-BF

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20 LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AE CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnre CSI_T2_001, BasicUnrestricted, AdvancedUnre AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_00 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

6.3. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Feb 21 09:15:44 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Feb 21 09:19:07 EST 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	No	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, which is required by VE6025, and in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Feb 21 09:15:44 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Feb 21 09:19:07 EST 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit H.323 Gatekeeper - cm7

10.64.101.236 Add Name or IP

Name or IP Address

Delete IP Back

6.4. Administer VE6025 User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message and system information: "Welcome: User", "Last login: Tue Feb 21 09:51:47 2017 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Tue Feb 21 10:37:07 EST 2017", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "User Management | User Admin | Add User" on the left and "Home | Help | Logout" on the right.

The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management" (expanded), "Service Admin", "User Admin" (expanded), "Add User" (selected), "Change User Password", "List All Users", "Modify Default Users", "Search Users", "Utilities", and "Help".

The main content area is titled "Add User" and contains the following form fields:

- 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:

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that **Enable SDB for DMCC Service** is unchecked, as shown below.

In the event that the security database is used by the customer with the parameter already enabled, then follow reference [2] to configure access privileges for the VE6025 user from **Section 6.3**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a user information block: "Welcome: User", "Last login: Tue Feb 21 09:51:47 2017 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Tue Feb 21 10:37:07 EST 2017", and "HA Status: Not Configured".

The main navigation bar is red and contains "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

6.6. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user welcome message with login details. A red navigation bar contains "Networking | Ports" and "Home | Help | Logout". A left sidebar lists various configuration categories, with "Networking" expanded to show "Ports" selected. The main content area is titled "Ports" and is divided into several sections:

- CVLAN Ports:** Includes "Unencrypted TCP Port" (9999) and "Encrypted TCP Port" (9998), each with "Enabled" and "Disabled" radio buttons.
- DLG Port:** Includes "TCP Port" (5678).
- TSAPI Ports:** Includes "TSAPI Service Port" (450) with "Enabled" and "Disabled" radio buttons, and "Local TLINK Ports" with "TCP Port Min" (1024) and "TCP Port Max" (1039).
- Unencrypted TLINK Ports:** Includes "TCP Port Min" (1050) and "TCP Port Max" (1065).
- Encrypted TLINK Ports:** Includes "TCP Port Min" (1066) and "TCP Port Max" (1081).
- DMCC Server Ports:** Includes "Unencrypted Port" (4721), "Encrypted Port" (4722), and "TR/87 Port" (4723), each with "Enabled" and "Disabled" radio buttons.

The "H.323 Ports" section is partially visible at the bottom.

6.7. Restart Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service**, and click **Restart Service**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message for the user, including the last login time (Tue Feb 21 09:51:47 2017), the number of failed login attempts (0), the host name/IP (aes7/10.64.101.239), the server offer type (VIRTUAL_APPLIANCE_ON_VMWARE), the SW version (7.0.1.0.2.15-0), the server date and time (Tue Feb 21 10:37:07 EST 2017), and the HA status (Not Configured).

The main content area is titled "Service Controller" and contains a table with the following data:

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 page, there are several buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

7. Configure Valcom VE6025 Application Server Pro

This section provides the procedures for configuring VE6025. The procedures include the following areas:

- Launch web interface
- Administer system setup
- Administer audio editor
- Administer event editor
- Administer play list
- Administer text monitors

In the compliance testing, one set of audio file, event, play list, and text monitor was created for monitoring of all emergency calls. Whenever a user on Communication Manager dials an emergency call, both IP speakers were alerted by VE6025.

7.1. Launch Web Interface

Access the VE6025 web-based interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the VE6025 server. Log in using the appropriate credentials.



7.2. Administer System Setup

Select **Administration** → **System** → **Setup** from the left pane to display the **Vip Scheduler Setup** screen in the right pane. Select the **Crisis Alert** tab. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Crisis Alert enabled:** Check this field.
- **CM Software Version:** Select the radio button for **6.3.111 and later**.
- **CM Server IP:** The IP address of the H.323 gatekeeper from **Section 6.3**.
- **SNMP Community Name:** The SNMP community name from **Section 5.5**.
- **CM Extension:** The virtual IP softphone extension from **Section 5.1**.
- **CM Password:** The virtual IP softphone security code from **Section 5.1**.
- **CM Confirm Password:** The virtual IP softphone security code from **Section 5.1**.
- **AES Server IP:** IP address of the Application Enablement Services server.
- **AES Port:** The DMCC server unencrypted port from **Section 6.6**.
- **AE Server UserName:** The VE6025 user credentials from **Section 6.4**.
- **AE Server Password:** The VE6025 user credentials from **Section 6.4**.
- **AE Confirm Password:** The VE6025 user credentials from **Section 6.4**.
- **Text Monitor Port:** An available port, in this case “560”.
- **Text Monitor Protocol:** Select the desired protocol, in this case **TCP**.

The screenshot shows the 'Vip Scheduler Setup' application window. The left pane contains a 'Menu' with a tree view showing 'Administration' > 'System' > 'Setup'. The right pane displays the 'Crisis Alert' configuration tab. The configuration fields are as follows:

Crisis Alert enabled:	<input checked="" type="checkbox"/>
CM Software Version:	<input checked="" type="radio"/> 6.3.111 and later <input type="radio"/> 6.3.xx and earlier
CM Server IP:	10.64.101.236
SNMP Community Name:	public
CM Extension:	65991
CM Password:	*****
CM Confirm Password:	
AE Server IP:	10.64.101.239
AE Port:	4721
AE Server UserName:	ve6025
AE Server Password:	*****
AE Confirm Password:	*****
Text Monitor Port:	560
Text Monitor Protocol:	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Text Monitor Example:	name=firstname lastname,ext=extension,building=bui

7.3. Administer Audio Editor

Select **Editors** → **Audio Editor** from the left pane to display the **Audio Editor** tab in the right pane. Select **New TTS File**.

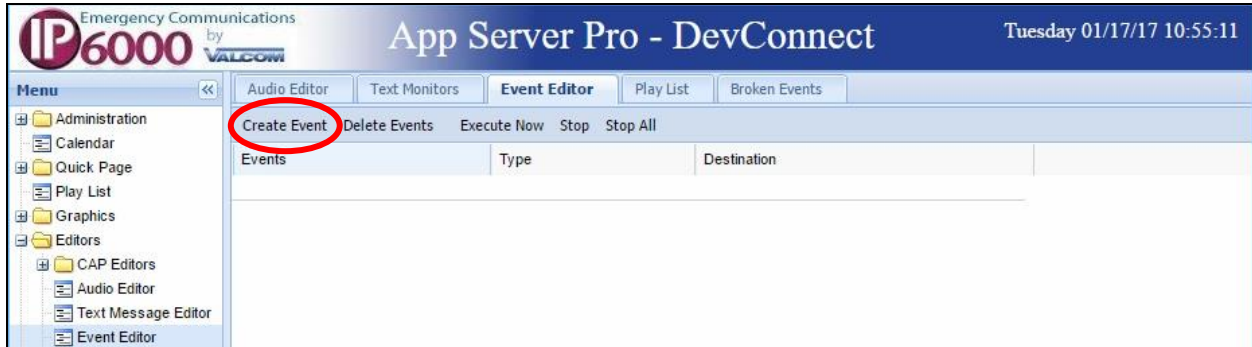


The **New Audio TTS File** screen is displayed. For **File Description**, enter a desired description. For **Category**, select an applicable pre-configured category, in this case "Avaya". For **Text**, follow reference [3] to enter desired text to be spoken for emergency call alert. Retain the default values in the remaining fields.



7.4. Administer Event Editor

Select **Editors** → **Event Editor** from the left pane to display the **Event Editor** tab in the right pane. Select **Create Event**. Select **Audio File** in the subsequent pop-up box (not shown below).



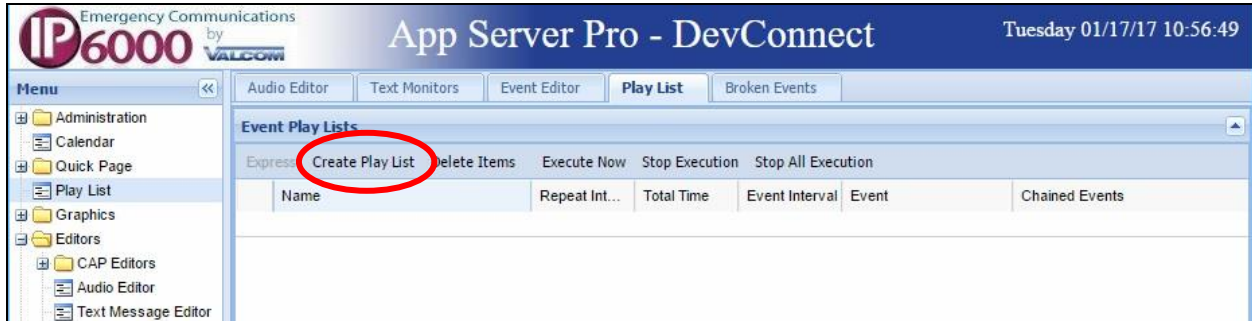
The **Create New Audio File Event** screen is displayed. For **Event Name**, enter a desired name. For **Audio File**, select the audio file from **Section 7.3**. For **Selected Codes**, select desired codes from the **Available Codes** column. Retain the default values in the remaining fields.

In the compliance testing, the “900 Alert All” code entry corresponded to the two IP speakers shown in **Section 3**.

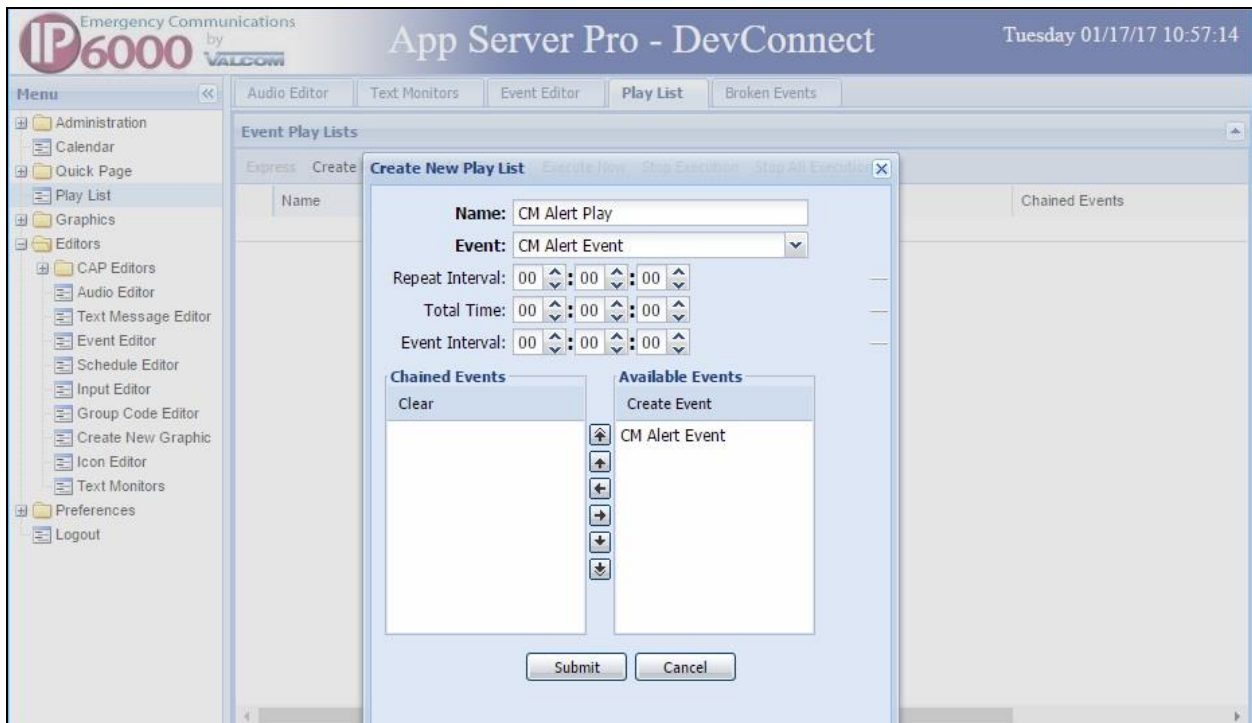


7.5. Administer Play List

Select **Play List** from the left pane to display the **Play List** tab in the right pane. Select **Create Play List**.



The **Create New Play List** screen is displayed. For **Name**, enter a desired name. For **Event**, select the event name from **Section 7.4**. Retain the default values in the remaining fields.



7.6. Administer Text Monitors

Select **Editors** → **Text Monitors** from the left pane to display the **Text Monitors** tab in the right pane. Select **Create Text Monitor**.



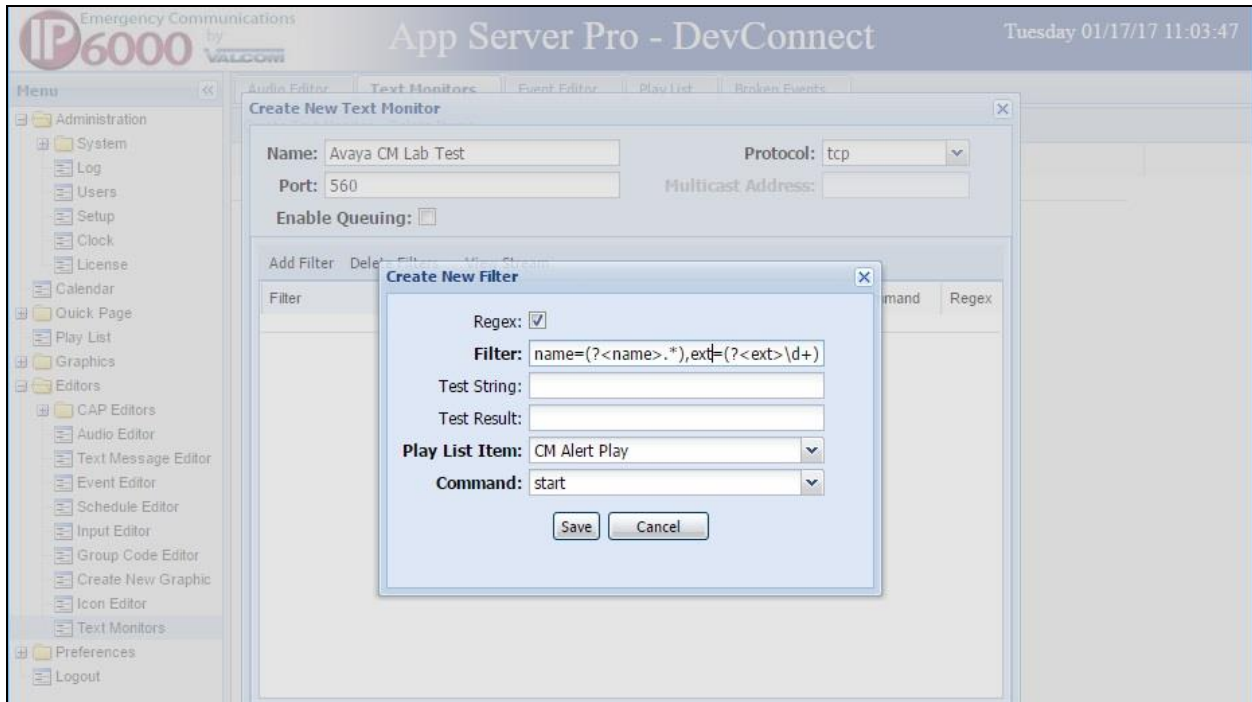
The **Create New Text Monitor** screen is displayed. For **Name**, enter a desired name. For **Protocol** and **Port**, select and enter the text monitor protocol and port values from **Section 7.2** respectively.

Select **Add Filter**, as shown below.



The **Create New Filter** screen is displayed. For **Filter**, follow reference [3] to enter a desired filter to match crisis alert and SNMP emergency call events from Application Enablement Services and Communication Manager. In the compliance testing, the **Filter** was set to “name=(?<name>.*),ext=(?<ext>\d+)(,building=(?<bldg>[^\,]*)?)(,floor=(?<floor>[^\,]*)?)(,room=(?<room>.*))?”.

For **Play List Item**, select the play list from **Section 7.5**. For **Command**, select “start”, as shown below.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and VE6025.

8.1. Verify Avaya Aura® Communication Manager


On Communication Manager, verify registration status of the virtual IP softphone by using the “list registered-ip-stations” command. Verify that the virtual IP softphone from **Section 5.1** is displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Skt	Station IP Address/ Gatekeeper IP Address		
65000	9641 1	IP_Phone 6.6302	tls	192.168.200.186 10.64.101.236		
65001	9611 1	IP_Phone 6.6302	tls	192.168.200.114 10.64.101.236		
65991	9630 1	IP_API_A 3.2040	tcp	10.64.101.239 10.64.101.236		

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC connection by selecting **Status → Status and Control → DMCC Service Summary** (not shown below) from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed. Verify that the **User** column shows an active session with the VE6025 user name from **Section 6.4**.



Application Enablement Services Management Console

Welcome: User
Last login: Wed Feb 22 11:13:54 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Thu Feb 23 10:23:11 EST 2017
HA Status: Not Configured

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**

DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every seconds

Session Summary [Device Summary](#)
Generated on Thu Feb 23 10:22:40 EST 2017

Service Uptime: 22 days, 16 hours 34 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 26

Number of Existing Devices: 1

Number of Devices Created Since Service Boot: 33

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
E26ADB727970DC954 81169A982CA1E72-34	ve6025	cmapiApplication	192.168.200.160	XML Unencrypted	1

[Terminate Sessions](#) | [Show Terminated Sessions](#)

8.3. Verify Valcom VE6025 Application Server Pro

Establish an emergency 911 call from a Communication Manager user with the PSTN.

Verify that the relevant IP speakers from **Section 7.4** received and played a call alert, with alert broadcast containing proper values for parameters such as the user extension, name, building, floor, and room, as defined in **Section 7.2**.

As an example from the compliance testing, the broadcast associated with an emergency 911 call from Communication Manager user with extension “65001”, name “CM7 Station 1”, building “Thorton”, floor “Floor5”, and room “RmMain” was announced as follows:

“An emergency 911 call has been placed from extension 65001, user CM 7 Station 1 in building Thorton, floor floor5, room RmMain”.

9. Conclusion

These Application Notes describe the configuration steps required for Valcom VE6025 Application Server Pro to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *IP6000 VE6025 Application Server Pro Overview*, Rev 2017-1.02, available at <http://www.valcomes.com>.

©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.