



Avaya Solution & Interoperability Test Lab

Application Notes for 911inform Connected Building with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3 using Crisis Alert – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for 911inform Connected Building to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3 using Crisis Alert. 911inform Connected Building is an emergency notification and management application.

In the compliance testing, 911inform Connected Building used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services and the Crisis Alert feature to provide monitoring 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 911inform Connected Building to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3 using Crisis Alert. Connected Building is an emergency notification and management application.

In the compliance testing, Connected Building used the Device, Media, and Call Control (DMCC) interface from Application Enablement Services and the Crisis Alert feature to provide monitoring of emergency calls.

Connected Building is a 911inform offer that consists of the DMCC-CA package running on a local enterprise server to interface with Application Enablement Services using the DMCC Java method and communicates with the 911inform Cloud Service on the public cloud hosted on Amazon Web Services.

The DMCC interface is used by Connected Building to register a virtual IP softphone with Communication Manager for monitoring of emergency calls. The virtual IP softphone is configured with a Crisis Alert feature button, such that when a Communication Manager user dials an emergency call, the virtual IP softphone receives events associated with audible and visual alerts.

Upon notified of an emergency call via DMCC, Connected Building sends the emergency call information including caller extension along with pre-assigned organizational ID to the Cloud Service. The Cloud Service then sends emergency notification to pre-configured notification users' email and/or SMS destinations, and provides browser access for viewing of applicable building and location map associated with the organizational ID along with highlighting of room associated with the emergency caller extension.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Connected Building application, the application automatically used DMCC to register the virtual IP softphone. Emergency calls were placed manually from users on Communication Manager to the simulated SIP Service Provider.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to Connected Building.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Application Enablement Services and Connected Building did not include use of any specific encryption features as requested by 911inform.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Connected Building:

- 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.
- Proper handling of emergency call scenarios involving emergency callers from different users, simultaneous emergency calls, and simultaneous emergency notifications.

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

2.2. Test Results

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

- When the Every User Responds parameter on the system-parameters crisis-alert form was disabled on Communication Manager in **Section 5.3**, then the Crisis Alert notification was acknowledged by Connected Building via the virtual IP softphone and cleared at all other user stations faster than the other user stations can view the crisis alert details. Therefore, the configuration of the parameter needs to take this observation into account.

2.3. Support

Technical support on Connected Building can be obtained through the following:

- **Phone:** (833) 333-1911
- **Email:** support@911inform.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 is not the focus of these Application Notes and will not be described.

The user extensions used in the compliance testing and their associated rooms are shown in the table below.

User Extensions	Room
65001 (H.323), 66002 (SIP)	301
65002 (H.323), 66007 (SIP)	302

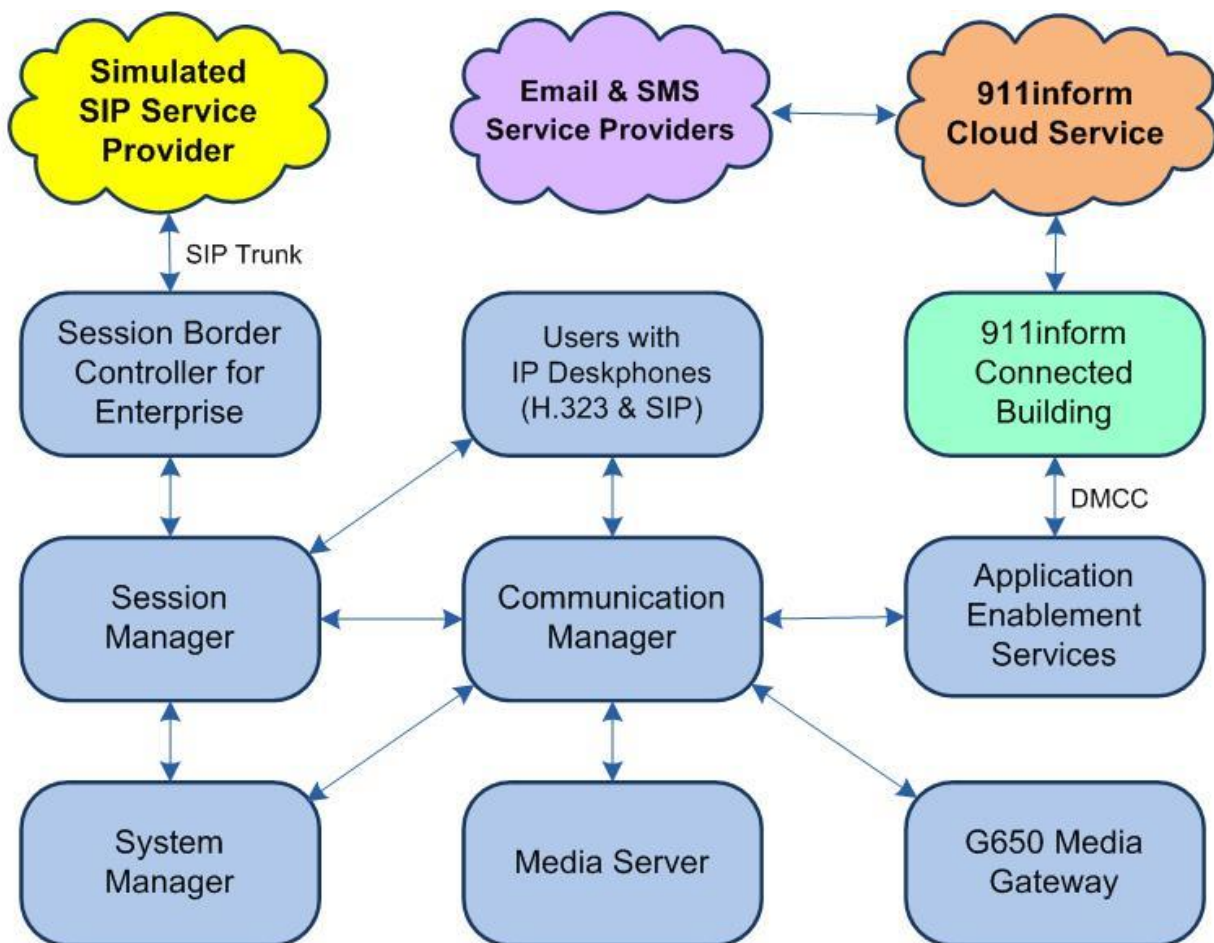


Figure 1: Compliance Testing Configuration

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	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3 (8.1.3.0.0.25-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.1 (8.1.1.0-19390)
Avaya 9611G & J159 IP Deskphone (H.323)	6.8502
Avaya 9641G IP Deskphone (SIP)	7.1.11.0.8
Avaya J169 IP Deskphone (SIP)	4.0.7.1.5
911inform Connected Building on Ubuntu <ul style="list-style-type: none">• DMCC-CA• Avaya DMCC Java	NA 18.04.5 LTS 1.2.1 8.1.0.0.9
911inform Cloud Service	4.0.0

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

5.1. Administer Virtual IP Softphone

Add a virtual 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.

- **Type:** “9630”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **IP SoftPhone:** “y”

add station 65991		Page 1 of 6
STATION		
Extension: 65991	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: 911inform DMCC	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 65991	
Display Language: English	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
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:crss-alert
  2:call-appr                         6:
  3:call-appr                         7:
  4:                                  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”. Note that the actual dialed string can vary depending on customer configuration. In the compliance testing, “911” was dialed and matches as is to the ARS dialed string entry “911” as part of the ARS/AAR Dialing without FAC feature.

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

change ars 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		n	

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
```

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 911inform 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 "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar menu lists various services: 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 provides an overview of the OAM web interface, listing administrative domains and their functions. A welcome message and system information are displayed in the top right corner.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Home | Help | Logout

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.

6.2. Verify License

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

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the sidebar. The main content area is titled "Licensing" and provides instructions for setting up and maintaining the WebLM, including steps for WebLM Server Address, WebLM Server Access, and Reserved Licenses. The top header and navigation bar are consistent with the previous screenshot.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- 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.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a navigation tree with the following structure:

- WebLM Home
- Install license
- Licensed products
 - APPL_ENAB
 - Application_Enablement (expanded)
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
 - ASBCE
 - Session_Border_Controller_E_AE
 - Avaya_Proactive_Contact
 - ContactCenter
 - CCTR
 - ContactCenter
 - COMMUNICATION_MANAGER

The right pane displays the **Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license)** screen. It includes the following information:

- You are here: Licensed Products > Application_Enablement > View by Feature
- License installed on: August 8, 2019 4:43:51 PM -05:00
- License File Host IDs: VE-83-02-2D-26-52-01

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

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**.

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

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

Switch Connections

[Add Connection](#)

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	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 a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

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

Edit H.323 Gatekeeper - cm7

[Add Name or IP](#)

Name or IP Address

[Delete IP](#) [Back](#)

6.4. Administer 911inform 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id911inform

* Common Name911inform

* Surname911inform

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

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 both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the 911inform user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including login details and system information. The main navigation bar is red and contains links for "Security", "Security Database", and "Control". The left sidebar lists various management categories, with "Security" expanded to show "Security Database" and "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
▼ Security
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
 ▼ Security Database
 ■ Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

Enabled Disabled

TR/87 Port4723

Enabled Disabled

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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Jan 27 13:06:36 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 09:47:18 EST 2021
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

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

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

7. Configure 911inform Connected Building

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

- Administer config.properties
- Launch web interface
- Administer users
- Administer room extensions

The configuration of Connected Building is typically performed by the 911inform Project Management team. The procedural steps are presented in these Application Notes for informational purposes.

Prior to configuration, an administrator account along with organizational ID, building and room layouts are assumed to have been created.

7.1. Administer config.properties

Log in to the Linux shell of Connected Building. Navigate to the **~/DMCC-Crisis-Alert-Dist/resources** directory and open the **config.properties** file with a text editor such as **vim**.

```
[xxxx@ubuntu:~$  
[xxxx@ubuntu:~$ cd ~/DMCC-Crisis-Alert-Dist/resources  
[xxxx@ubuntu:~/DMCC-Crisis-Alert-Dist/resources$ sudo vim config.properties
```

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

- **aesIP:** IP address of Application Enablement Services.
- **cmIP:** IP address of the H.323 gatekeeper from **Section 6.3**.
- **username:** The 911inform user credentials from **Section 6.4**.
- **password:** The 911inform user credentials from **Section 6.4**.
- **apiKey:** The pertinent api key value provided by 911inform.
- **orgId:** The pertinent organizational ID value provided by 911inform.
- **source:** Unique location IP address if used with 911inform, else “255.255.255.255”.
- **caExt:** The virtual IP softphone extension from **Section 5.1**.
- **caPass:** The virtual IP softphone security code from **Section 5.1**.


```
aesIP=10.64.101.239
aesPort=4721
cmIP=10.64.101.236
username=911inform
password=911Inform#
apiKey=xxxxxx
orgId=yyyyy
source=255.255.255.255
caExt=65991
caPass=123456
```

7.2. Launch Web Interface

Access the Cloud Service web interface by using the URL <https://inform.911inform.com> in a browser window to display the screen below. Select **LOGIN**.



The **Welcome to 911inform** screen below is displayed. Enter the administrator credentials provided by 911inform, and click **Log In**.



Welcome to 911inform

911inform is the latest technology for school and building emergencies. This software can handle all types of emergency situations including 911 calls, lockdowns, health emergencies, shelter in places and more.


911inform is tied directly to the police and emergency personnel. It works with your existing phone system and has apps that run on any computer or mobile device. This technology gives the police and emergency personnel situational awareness of the emergencies going on in your school or building.

To order this software or see a demonstration please call
(833) 333-1911.

Existing Customers Log In Here

Email address

Password

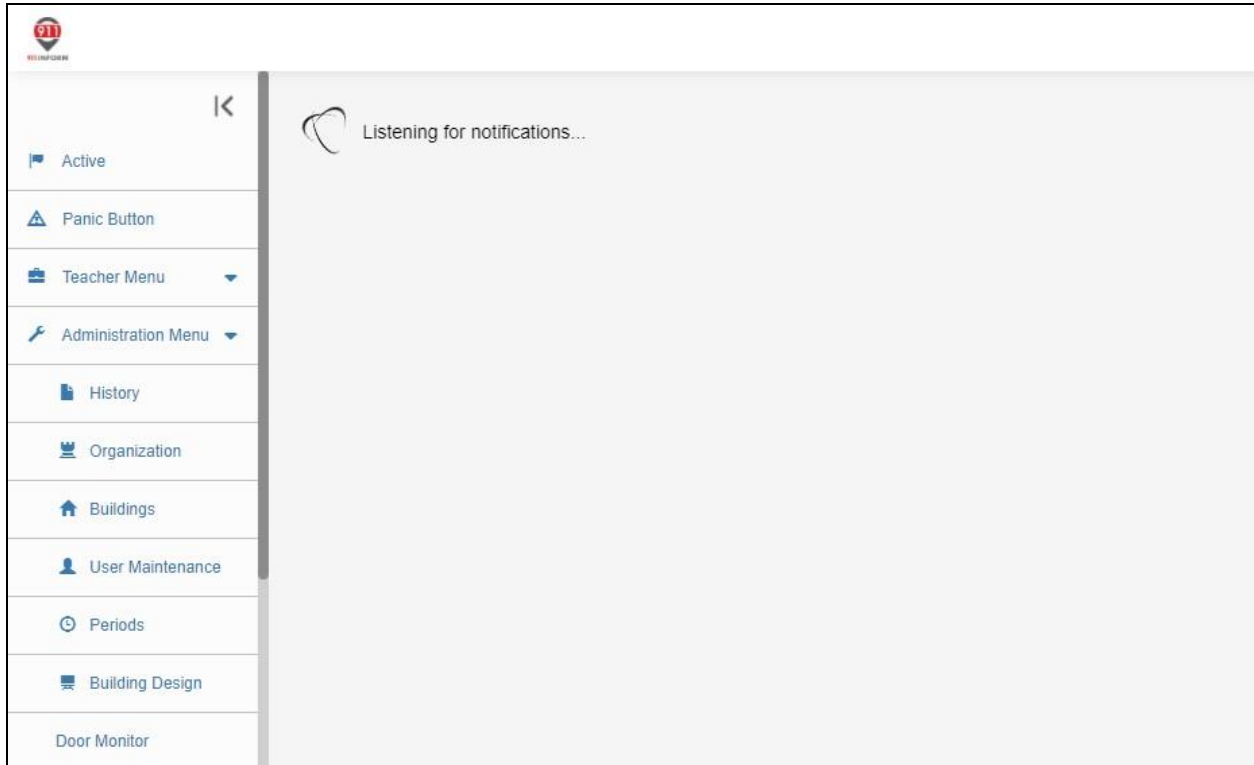
[Forgot Password?](#)

☒ Remember me

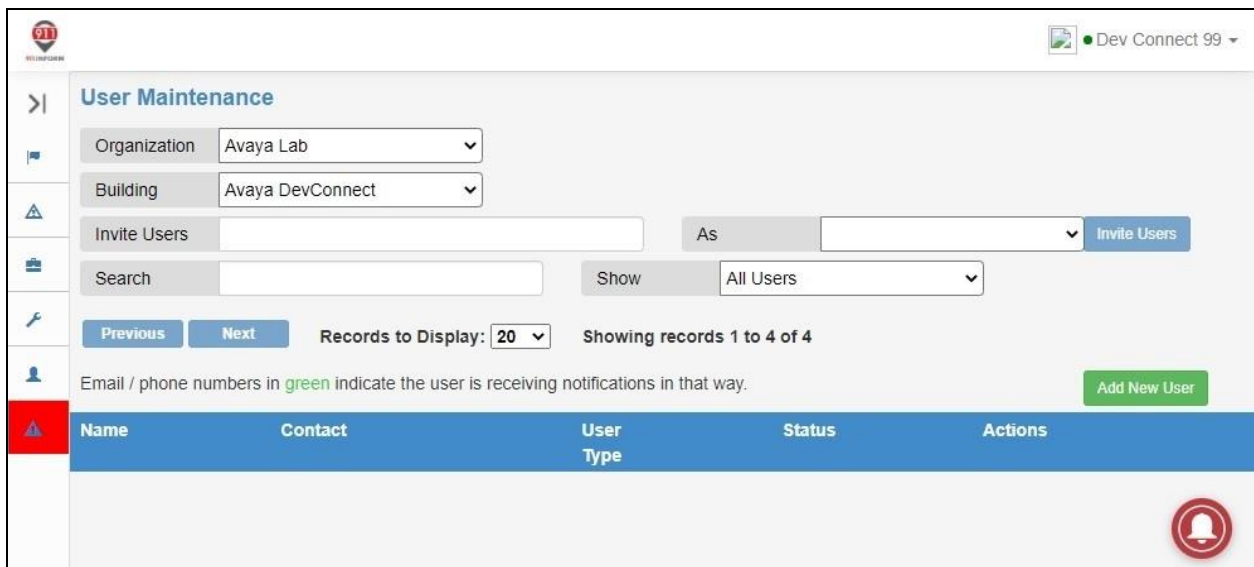
Log In

7.3. Administer Users

The screen below is displayed next. Select **Administration Menu → User Maintenance** to add users for emergency notifications.



The **User Maintenance** screen is displayed. Retain the default values and select **Add New User**.



The screen below is displayed next. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Email:** The user email address.
- **First Name:** The user first name.
- **Last Name:** The user last name.
- **Phone:** The user mobile number.
- **Password:** The desired password.
- **User Type:** “Default User”
- **Notifications:** Select the desired notifications, in this case “Text & Email”.

User Maintenance / Avaya Lab / Avaya DevConnect

Email: devconnect11@gmail.com Active? ☒

First Name: Dev 11 Last Name: Avaya

Phone: (111) 222-3333 Phone 2:

Position: ID:

Password: test123

Extensions:

Receive Location Registration Requests Via:

User Type: Default User Notifications: Text & Email LDS Only? ☐

Save User

Repeat this section to create the desired number of users to receive notification of emergency calls. Below were the users created for the compliance testing with masked email and mobile numbers for security purposes.

Email / phone numbers in green indicate the user is receiving notifications in that way.

Name	Contact	User Type	Status	Actions
Avaya, Dev 11	devconnect11@gmail.com (111) 222-3333	Default User	Offline	
Avaya, Dev 22	devconnect22@gmail.com (777) 888-9999	Default User	Online	
Avaya, Dev 33	devconnect33@gmail.com (333) 333-3333	Default User	Offline	
Avaya, Dev 99	devconnect999@gmail.com (555) 555-5555	Administration User	Offline	

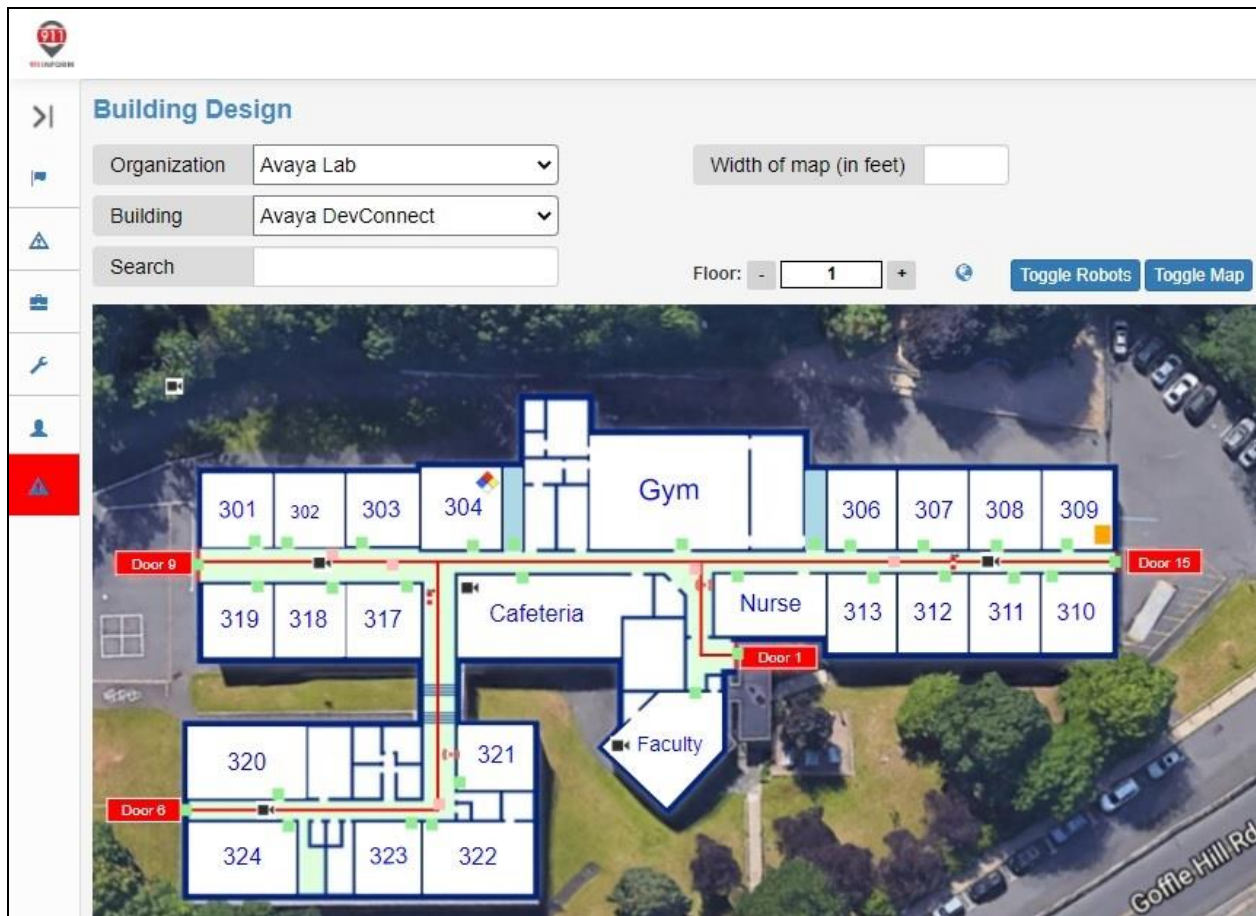
Add New User

7.4. Administer Room Extensions

From the expanded left pane shown in **Section 7.3**, select **Administration Menu → Building Design** to map user extensions to rooms.

Note that user extensions to rooms mapping can be accomplishing by import of CSV file or by manual configuration. The compliance testing used the manual configuration method.

The **Building Design** screen is displayed. Select the first room from **Section 3** to map extensions to, in this case “301”.



The **Building Design** screen is updated as shown below. For **Extension(s)**, enter the associated user extensions and/or extension ranges from **Section 3**, separated by commas.

Repeat this section to map all user extensions to rooms from **Section 3**. In the compliance testing, user extensions 65001 and 66002 were mapped to room 301, and user extensions 65002 and 66007 were mapped to room 302, as shown below.


Building Design / Avaya DevConnect / 301

Name	301	Floor	1
Description	Math Room	Type	Room
Extension(s)	65001,66002		

360 Image
Name: 5c07f90964a4e937ccd5ef30.jpg

Rectangle Circle Polygon Safety Area Entry Position

Object X 75 Y 116 W 48 H 50
Text - X 11 Y 30 Size 16



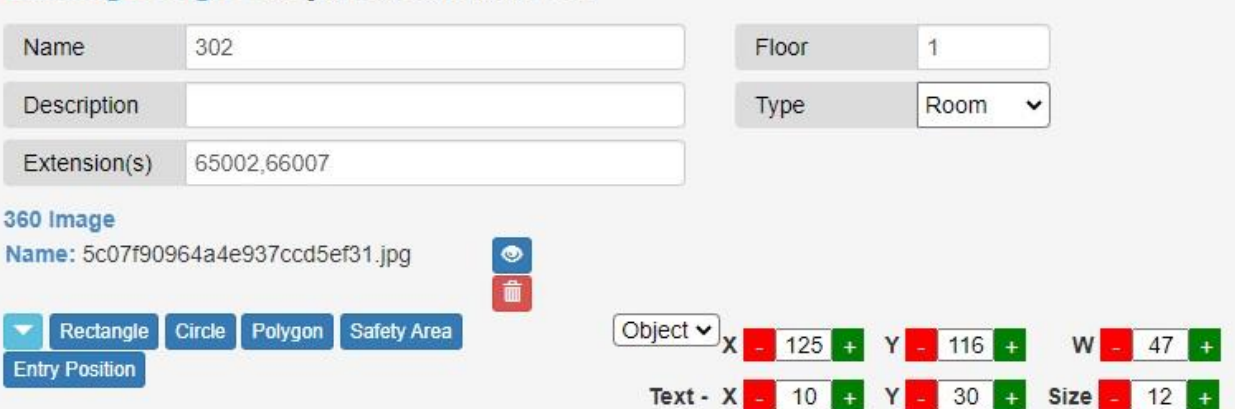
Building Design / Avaya DevConnect / 302

Name	302	Floor	1
Description		Type	Room
Extension(s)	65002,66007		

360 Image
Name: 5c07f90964a4e937ccd5ef31.jpg

Rectangle Circle Polygon Safety Area Entry Position

Object X 125 Y 116 W 47 H 50
Text - X 10 Y 30 Size 12



8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager


On Communication Manager, verify registration status of 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 IP address of the Application Enablement Services server, as shown below.

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

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65001	9611	IP_Phone	192.168.200.217
tls	1	6.8502	10.64.101.236
65002	9611	IP_Phone	192.168.200.179
tls	1	6.8502	10.64.101.236
65991	9630	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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 911inform user from **Section 6.4**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Feb 2 12:09:59 2021 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: 8.1.3.0.0.25-0
Server Date and Time: Tue Feb 02 12:25:11 EST 2021
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Feb 02 12:25:01 EST 2021

Service Uptime: 0 days, 0 hours 8 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 2

Number of Existing Devices: 1

Number of Devices Created Since Service Boot: 2

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	4340916579AE2E345 2F6011E8B6824DD-2	911inform	cmapiApplication	10.64.101.202	XML Unencrypted	1

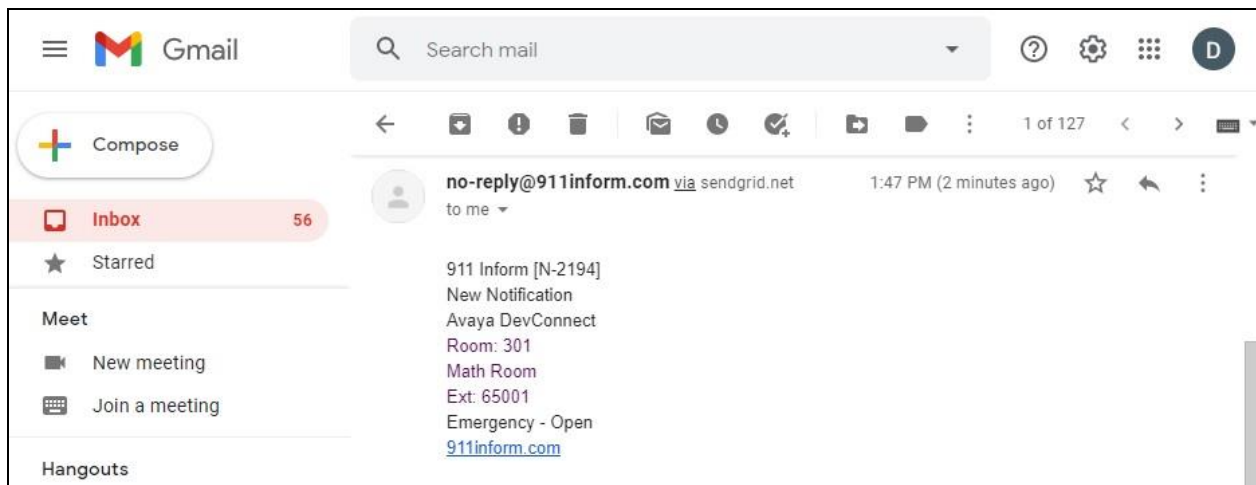
Terminate Sessions Show Terminated Sessions

8.3. Verify 911inform Connected Building

Make an emergency call from a Communication Manager user from **Section 3**. Verify that all emergency notification users configured in **Section 7.3** receive proper email and/or SMS notifications, and that the users can log into the Cloud Service to review details.

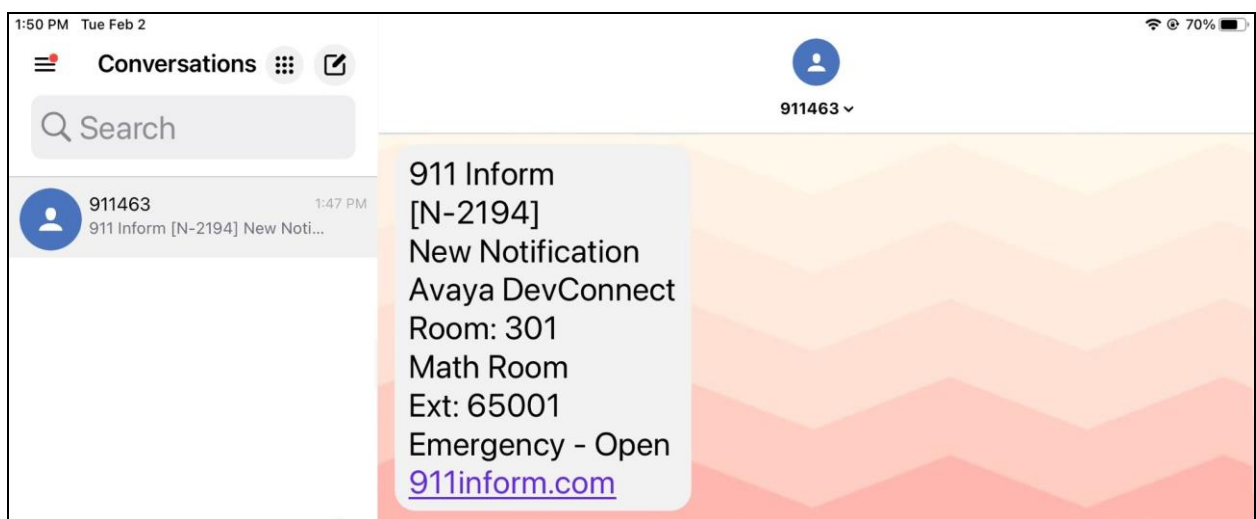
8.3.1. Verify Email Notification

Log a notification user into his/her email application. Verify that there is email notification for the emergency call as shown below, where “65001” is the extension of the emergency call originator obtained from DMCC and “301” is the room mapped to the user extension from **Section 7.4**.



8.3.2. Verify SMS Notification

Log a notification user into his/her SMS application or mobile phone. Verify that there is SMS notification with similar emergency call information from **Section 8.3.1** as shown below.



8.3.3. Verify Cloud Service

Click on the **911inform.com** link provided in the email notification from **Section 8.3.1** or the SMS notification from **Section 8.3.2** to open a browser connection to the Cloud Service web interface. The same 911inform screen from **Section 7.2** is displayed (not shown). Enter the notification user credentials to log in.

Verify that the active emergency is displayed, along with the emergency call originator extension “65001” and highlight of mapped room number from **Section 7.4**, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for 911inform Connected Building to successfully interoperate with Avaya Aura® Communication Manager 8.1.3 using Avaya Aura® Application Enablement Services 8.1.3. 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 8.1.x, Issue 8, November 2020, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at <http://support.avaya.com>.
3. *Connected Building Solution CM Integration Guide*, available upon request to 911inform Support.
4. *911inform User Manual Administrator*, available upon request to 911inform Support.

©2021 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.