Avaya Solution & Interoperability Test Lab

Application Notes for 911inform Location Discovery Solution with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for 911inform Location Discovery Solution to interoperate with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3. 911inform Location Discovery Solution is a VoIP user location tracking and management application.

In the compliance testing, 911inform Location Discovery Solution used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor H.323 user registrations, and the Element Manager Web Service interface from Avaya Aura® Session Manager to monitor SIP user registrations.

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 Location Discovery Solution (LDS) to interoperate with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3. LDS is a VoIP user location tracking and management application.

In the compliance testing, LDS used the Device, Media, and Call Control (DMCC) interface from Application Enablement Services to monitor H.323 user registrations, and the Element Manager Web Service interface from Session Manager to monitor SIP user registrations.

LDS requires the basic DMCC-CA package as part of the Connected Building offer, and these Application Notes assume the basic DMCC-CA package is already in place and will not be described. For more information on Connected Building, refer to reference **[4]**.

LDS is a 911inform offer that consists of an optional DMCC-911inform package for tracking of H.323 user registrations and an optional ASM package for tracking of SIP user registrations. The DMCC-911inform and ASM packages run on the same local enterprise server that hosts the required DMCC-CA package and communicates with 911inform Cloud Service on the public cloud hosted on Amazon Web Services.

The DMCC-911inform package interfaces with Application Enablement Services using the DMCC Java method to monitor registration events associated with H.323 users, and the ASM package interfaces with Session Manager using the Element Manager Web Service interface to query registration information associated with SIP users.

Upon detecting a change in the IP and/or MAC address from the registration information associated with a H.323 or SIP user, LDS sends the registration information including user extension along with pre-assigned organizational ID to the Cloud Service. The Cloud Service then sends registration notification to pre-configured email and/or SMS destinations associated with the user extension and provides URL for the user to update his/her location information.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the LDS application, the application automatically used DMCC to monitor H.323 user registrations and Element Manager Web Service to query SIP user registrations. The IP and/or MAC address changes were made manually from the user telephones.

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

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 interfaces with LDS included the encrypted Element Manager Web Service connection with Session Manager, and non-encrypted DMCC connection with Application Enablement Services 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 LDS:

- Use of DMCC monitoring services to monitor H.323 user registration information.
- Use of Element Manager Web Service to query SIP user registration information.
- Proper handling of registration notification and location setting scenarios involving H.323 users, SIP users, registration, un-registration, IP and/or MAC address changes.

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

2.2. Test Results

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

- By design, LDS automatically refreshes the DMCC session and all H.323 user monitors by a configurable refresh interval with default value set to 180 minutes.
- After a restart of Communication Manager, the H.323 user monitors were not re-established by LDS until after the next DMCC session refresh. The impact is that any potential H.323 user IP and/or MAC change will not be detected by LDS until the next DMCC session refresh.

2.3. Support

Technical support on LDS 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, Application Enablement Services, Session Manager, and System Manager are not the focus of these Application Notes and will not be described.

The VoIP user extensions used in the compliance testing are shown in the table below.

User Extensions	Type
65001, 65002	H.323
66002, 66007	SIP

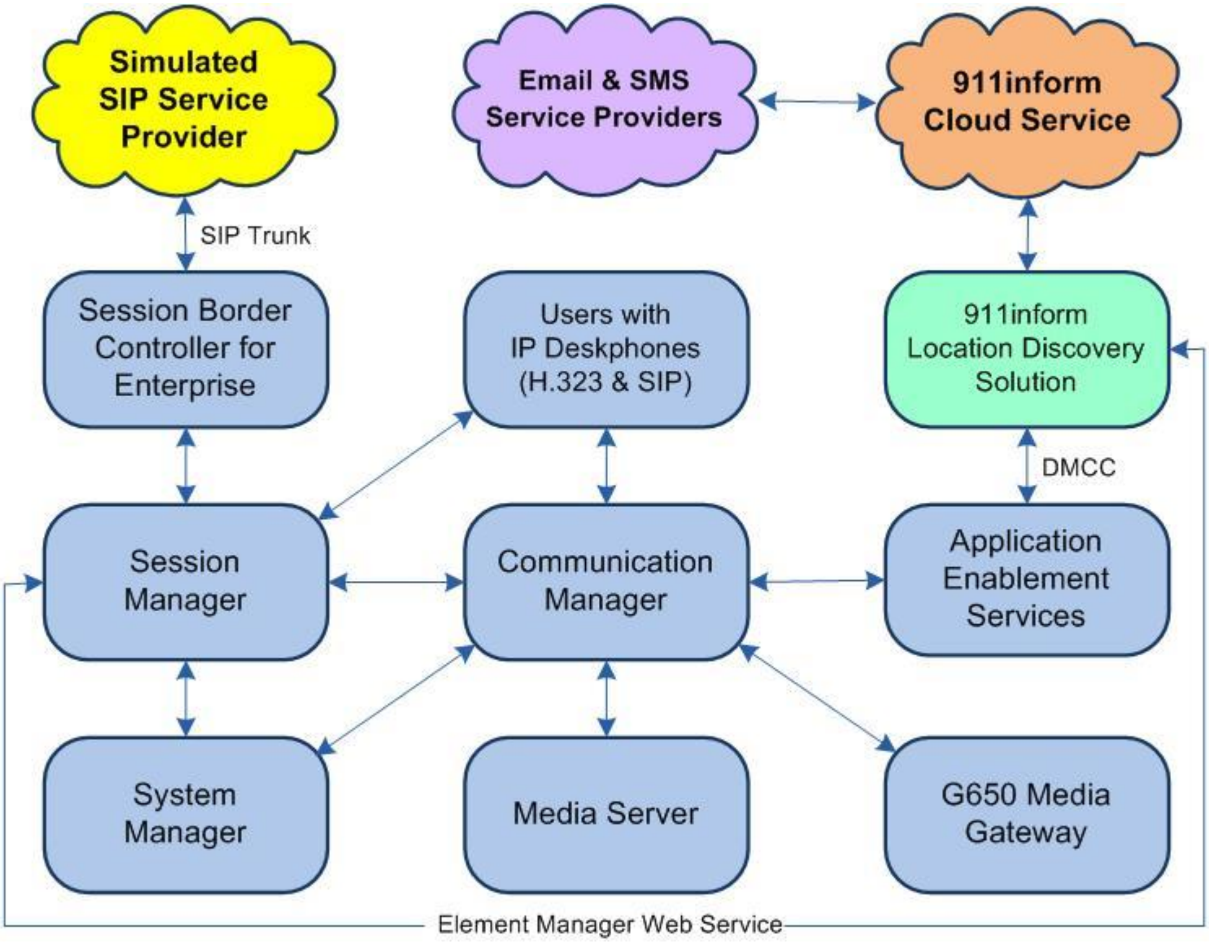

Simulated SIP Service Provider
Email & SMS Service Providers
911inform Cloud Service
SIP Trunk
Session Border Controller for Enterprise
Users with IP Deskphones (H.323 & SIP)
911inform Location Discovery Solution
DMCC
Session Manager
Communication Manager
Application Enablement Services
System Manager
Media Server
G650 Media Gateway
Element Manager Web Service

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 & J179 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 Location Discovery Solution on Ubuntu • DMCC-911inform • ASM • Avaya DMCC Java	NA 18.04.5 LTS 1.2.1 1.0.2 8.1.0.0.0.9
911inform Cloud Service	4.0.1

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "y" on **Page 4**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   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? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
```

5.2. Administer CTI Link

Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                   Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 60111
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES CTI Link
Unicode Name? n
```

6. Configure Avaya Aura® Application Enablement Services

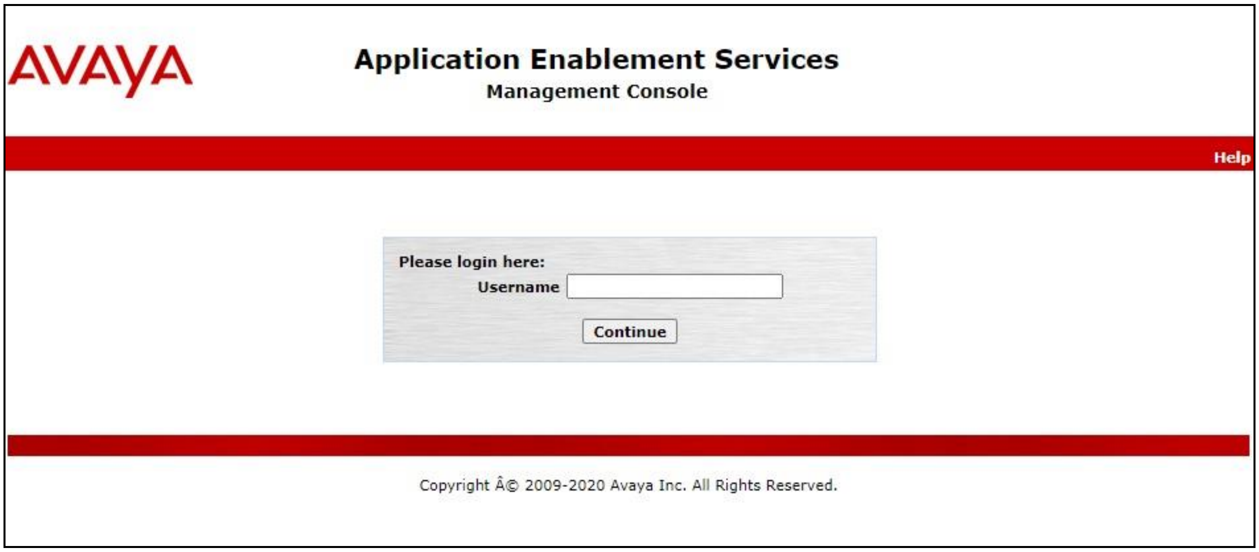
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer H.323 gatekeeper
- Administer TSAPI link
- Administer 911inform user
- Administer security database
- Administer ports
- Restart services

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.

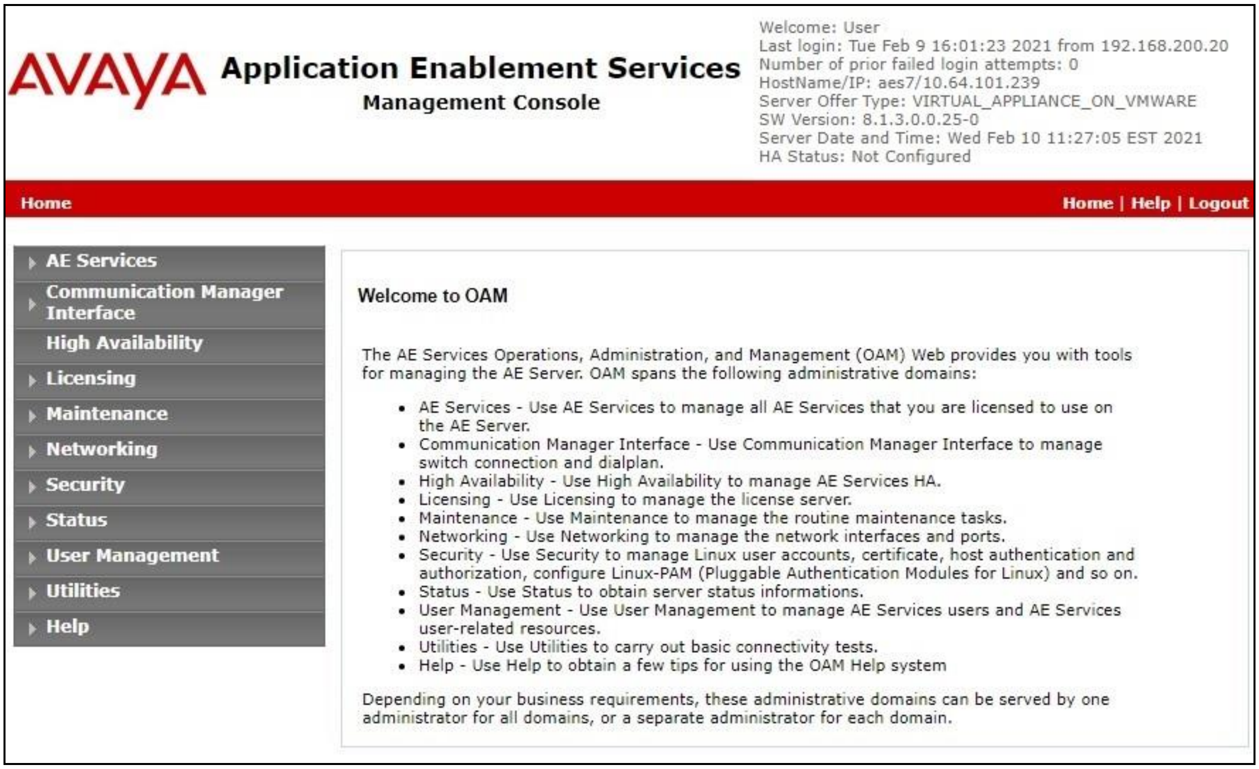


Application Enablement Services
Management Console

Please login here:
Username

Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Welcome to OAM

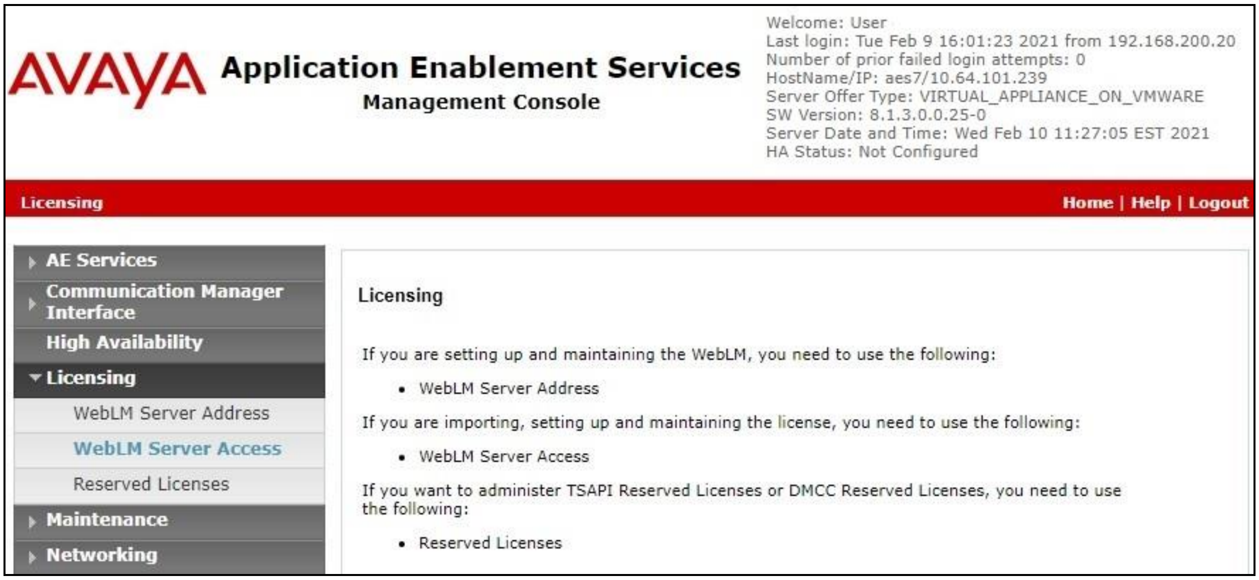
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

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:

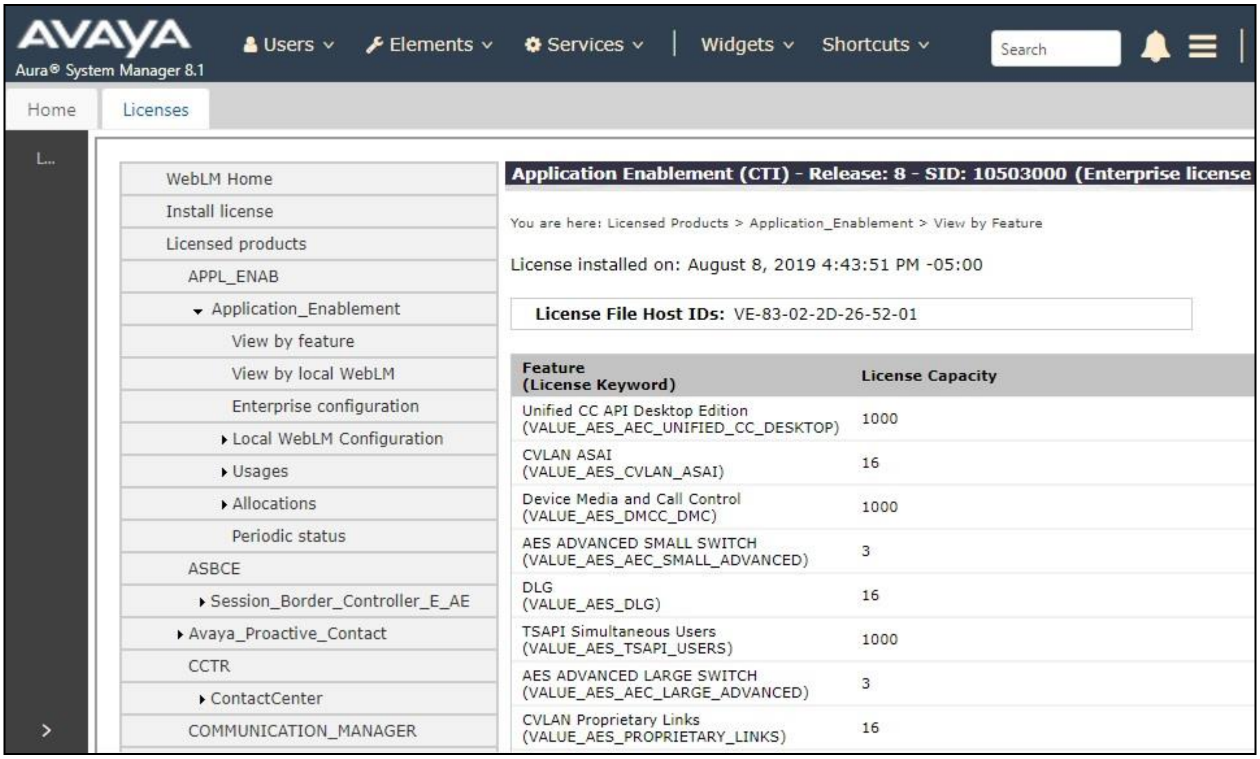
- WebLM Server Access

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 are sufficient licenses for **TSAPI Simultaneous Users** as shown below. Note that the TSAPI license is used for device monitoring via DMCC, and that no specific DMCC license is required for integration with LDS.



Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: August 8, 2019 4:43:51 PM -05:00

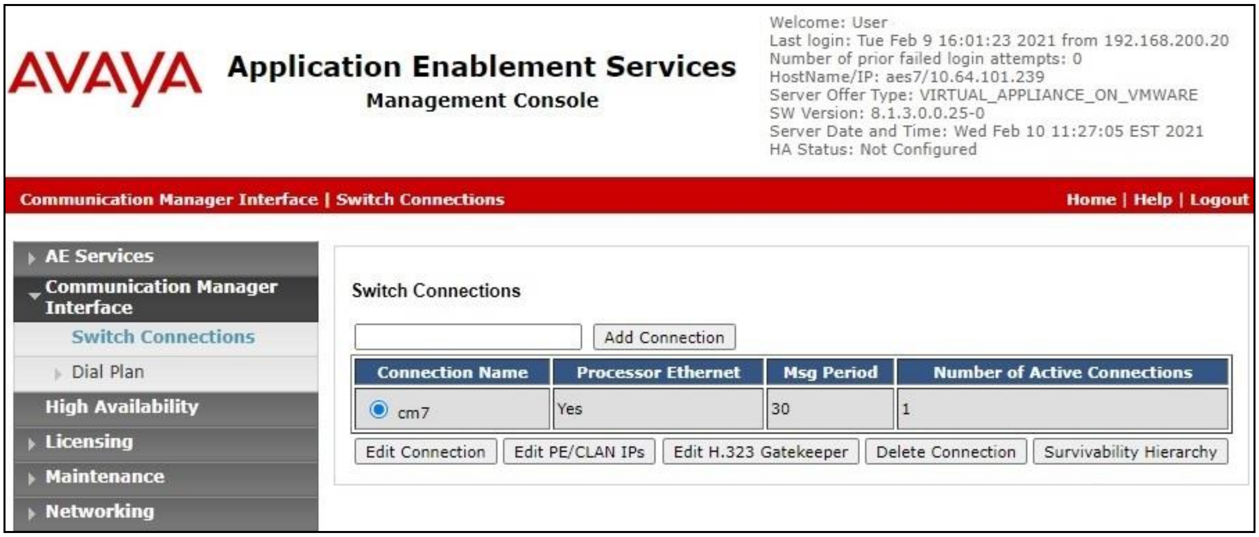
License File Host IDs: VE-83-02-2D-26-52-01

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**.

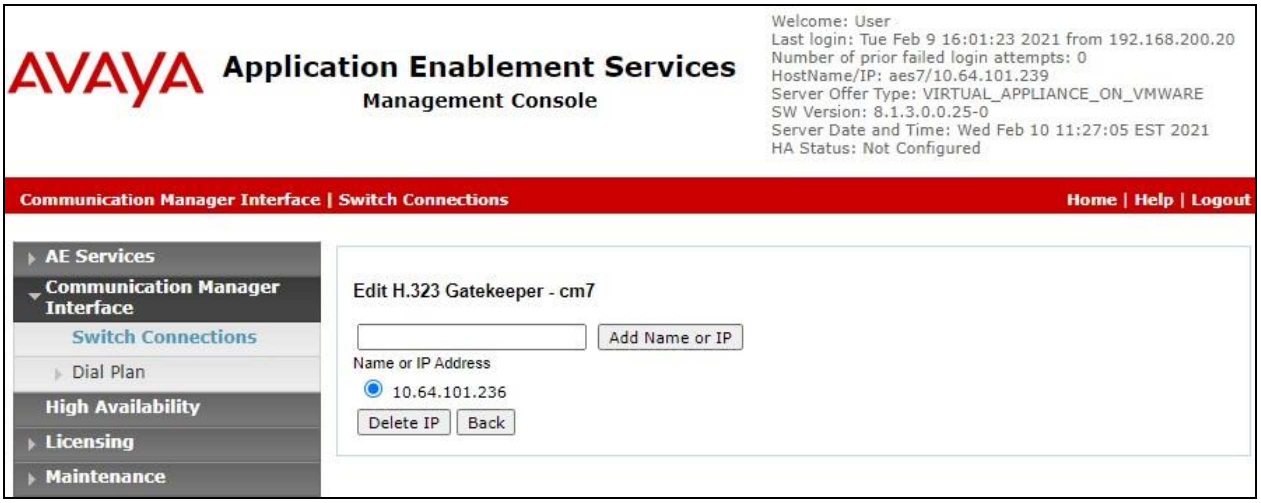


Welcome: User
Last login: Tue Feb 9 16:01:23 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Make a note of the H.323 gatekeeper IP address, which was created as part of the Connected Building integration documented in reference **[4]** and will be used later to configure LDS.



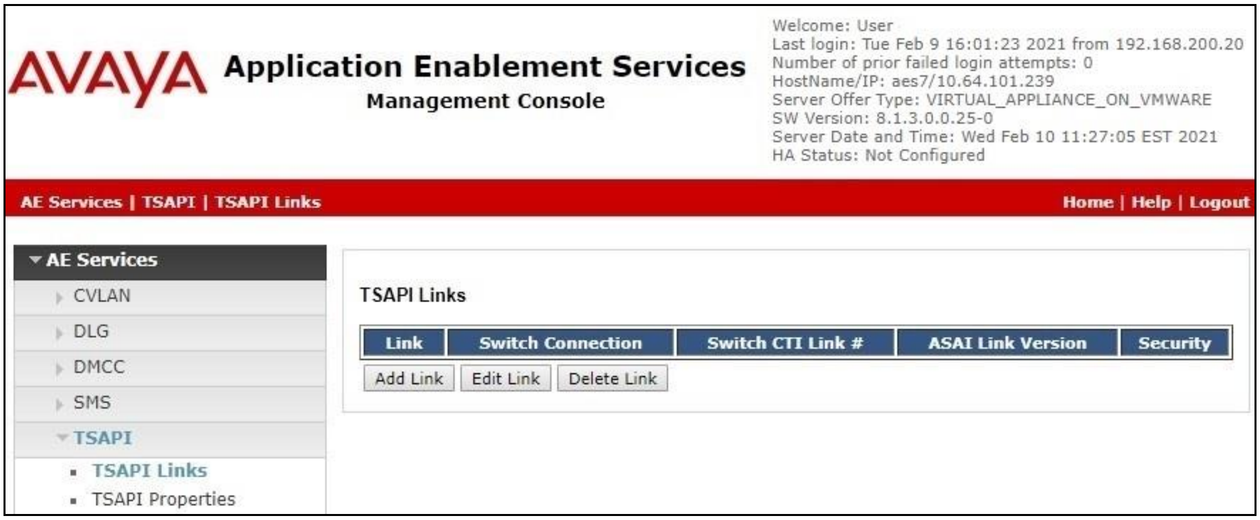
Welcome: User
Last login: Tue Feb 9 16:01:23 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Edit H.323 Gatekeeper - cm7

Name or IP Address
● 10.64.101.236

6.4. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



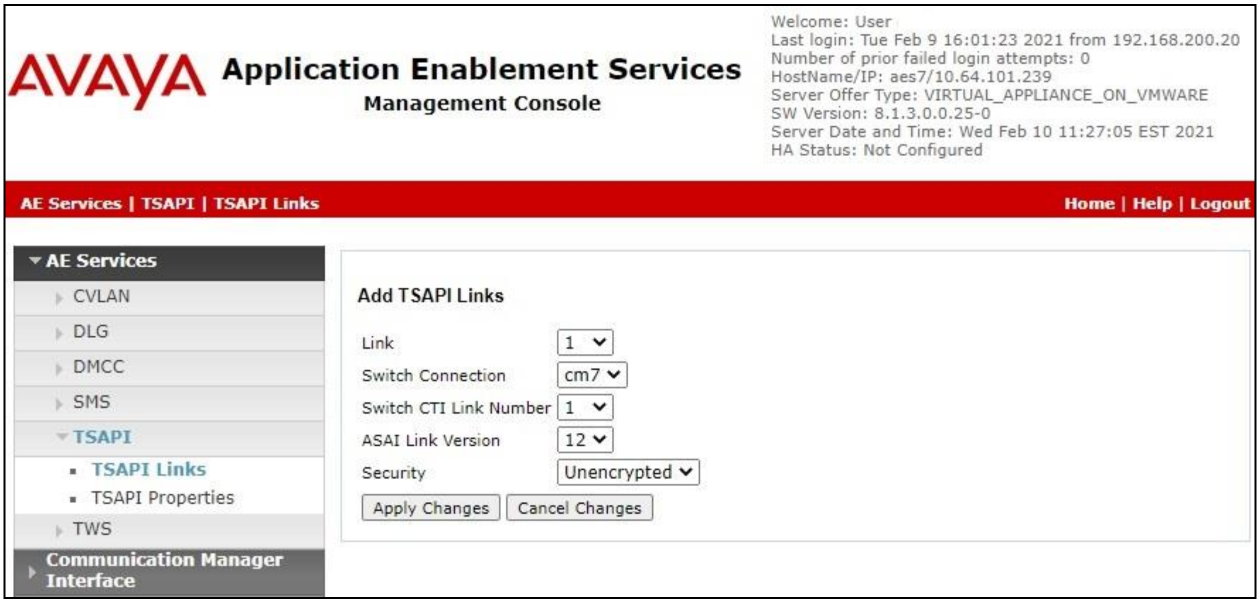
Welcome: User
Last login: Tue Feb 9 16:01:23 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Add TSAPI Links

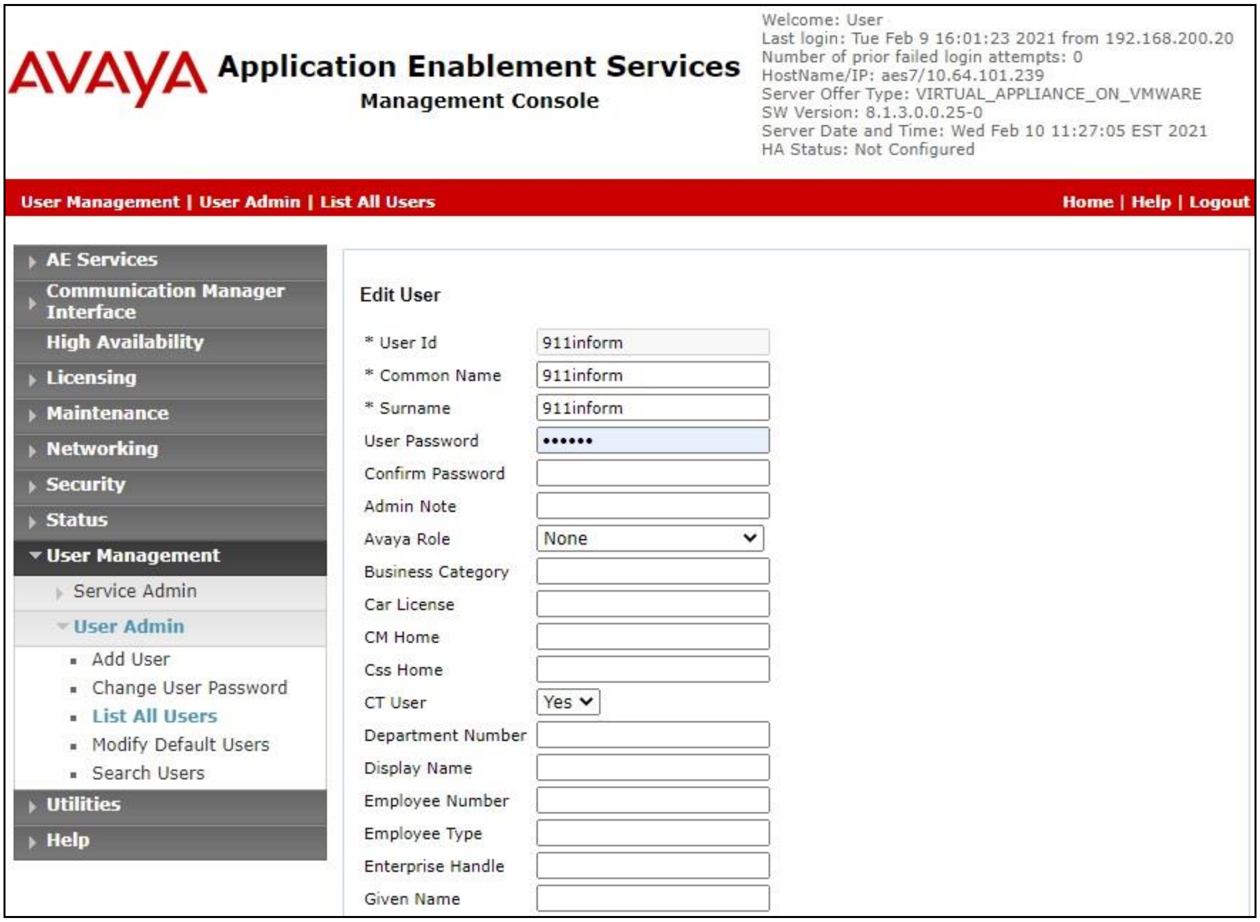
Link	1
Switch Connection	cm7
Switch CTI Link Number	1
ASAI Link Version	12
Security	Unencrypted

6.5. Administer 911inform User

Select **User Management → User Admin → Add User** from the left pane, to display the **Add User** screen in the right pane (not shown).

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.

Either a new CTI user can be created for the DMCC connection with LDS, or the existing CTI user created for Connected Building as part of reference **[4]** can be used. In the compliance testing, the same CTI user from reference **[4]** was used, as shown below.



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

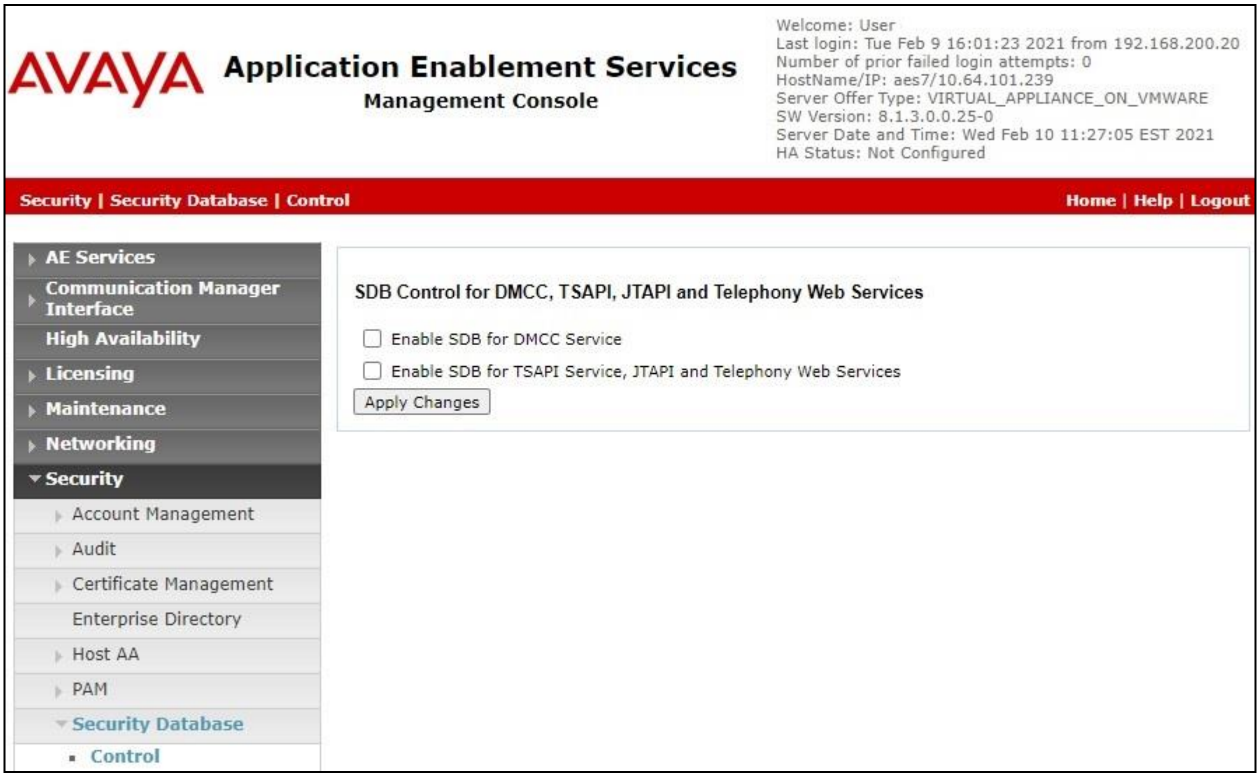
Edit User

* User Id	911inform
* Common Name	911inform
* Surname	911inform
User Password	••••••
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	

6.6. 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 6.5**.



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

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

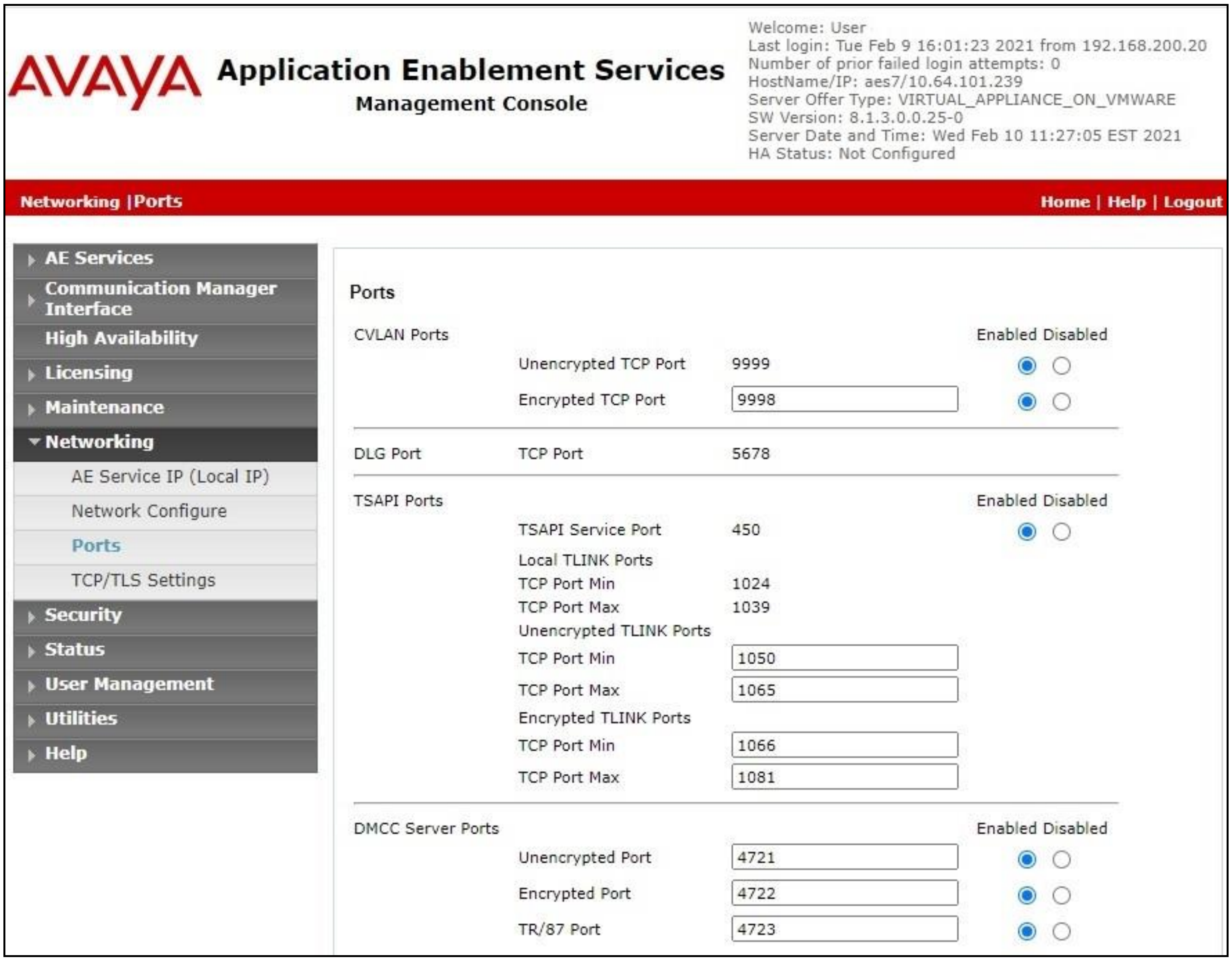
□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.7. Administer Ports

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

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



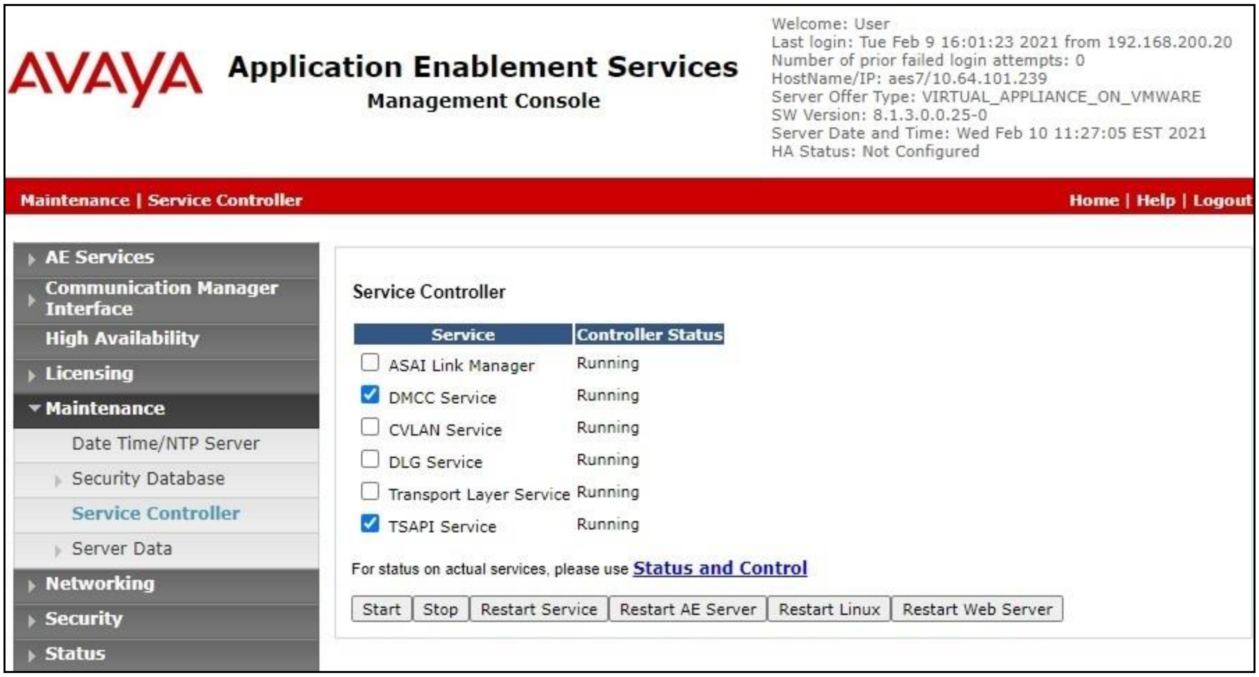
Welcome: User
Last login: Tue Feb 9 16:01:23 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.8. Restart Services

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



Welcome: User
Last login: Tue Feb 9 16:01:23 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: Wed Feb 10 11:27:05 EST 2021
HA Status: Not Configured

Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

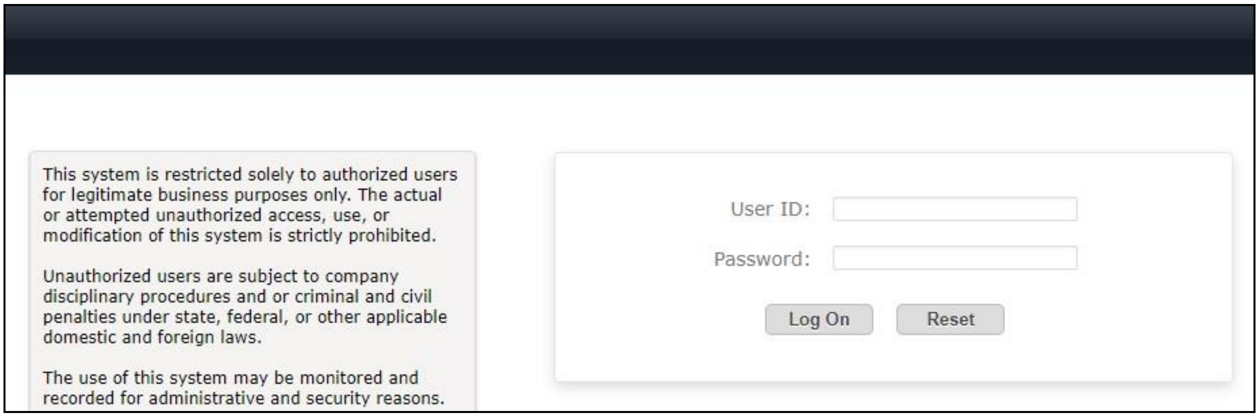
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer administrators
- Obtain CA certificate

7.1. Launch System Manager

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



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

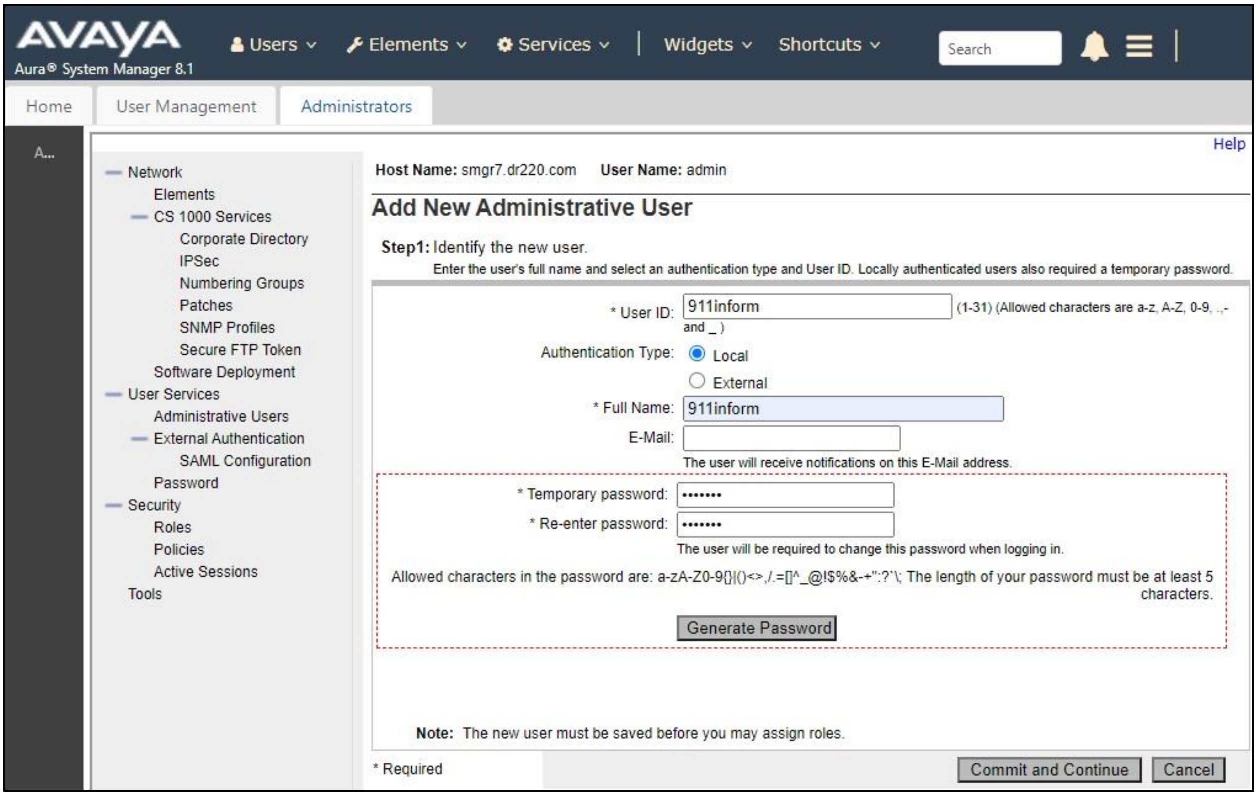
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

7.2. Administer Administrators

Select **Users → Administrators → Administrative Users** from the top menu to display a list of existing administrative users (not shown). Select **Add** (not shown) from the right pane to add a new administrative user for LDS for Element Manager Web Service access.

Enter desired **User ID**, **Full Name**, **Temporary password**, and **Re-enter password** as shown below. For **Authentication Type**, select "Local". Click **Commit and Continue**.



Host Name: smgr7.dr220.com **User Name:** admin

Add New Administrative User

Step1: Identify the new user.

Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

* User ID: 911inform (1-31) (Allowed characters are a-z, A-Z, 0-9, .,- and _)

Authentication Type: ● Local ○ External

* Full Name: 911inform

E-Mail:

The user will receive notifications on this E-Mail address.

* Temporary password: •••••••

* Re-enter password: •••••••

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`\; The length of your password must be at least 5 characters.

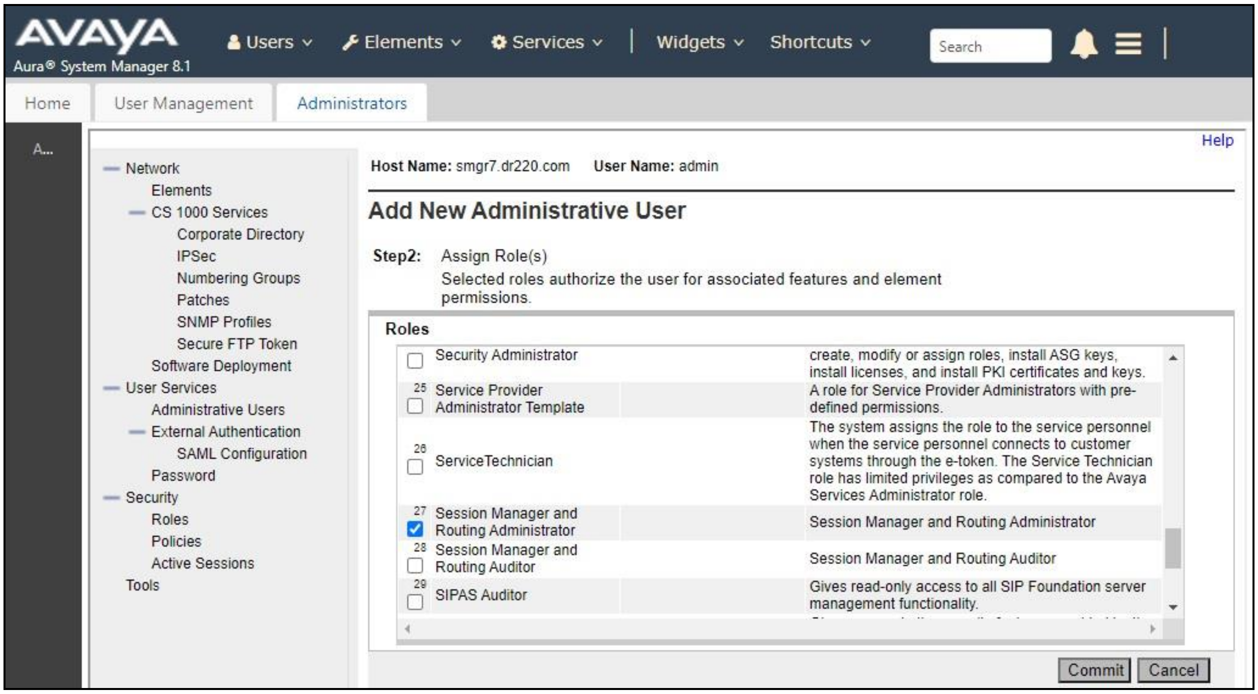
Generate Password

Note: The new user must be saved before you may assign roles.

* Required

Commit and Continue Cancel

The screen below is displayed next for assigning role(s) to the new administrative user. Scroll the right pane as necessary to locate and check **27 Session Manager and Routing Administrator** as shown below.



Host Name: smgr7.dr220.com **User Name:** admin

Add New Administrative User

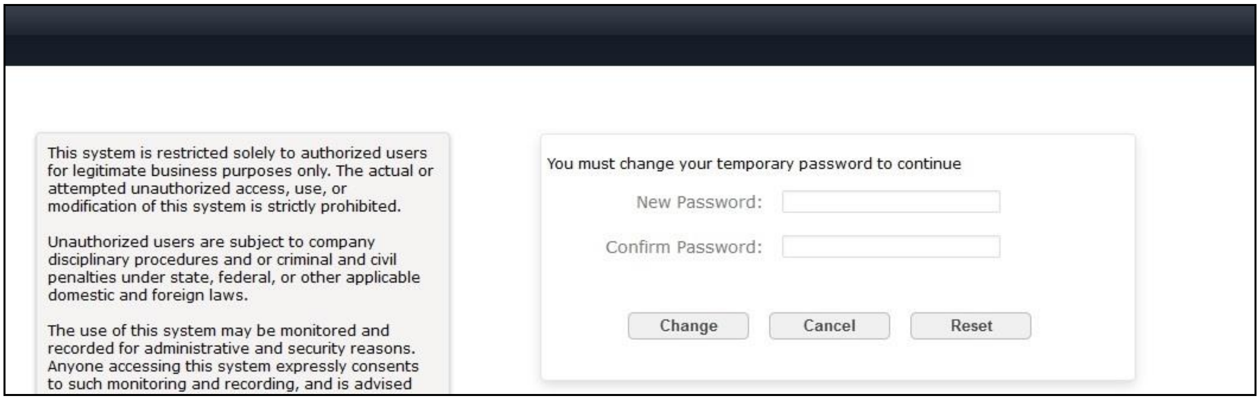
Step2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.

Roles

	□ Security Administrator	create, modify or assign roles, install ASG keys, install licenses, and install PKI certificates and keys.
25	□ Service Provider Administrator Template	A role for Service Provider Administrators with pre-defined permissions.
26	□ ServiceTechnician	The system assigns the role to the service personnel when the service personnel connects to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.
27	☑ Session Manager and Routing Administrator	Session Manager and Routing Administrator
28	□ Session Manager and Routing Auditor	Session Manager and Routing Auditor
29	□ SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.

Note that the new administrative user is required to change the temporary password upon initial log in, therefore log off as the existing user from the web interface and log back into System Manager using the new administrator credentials created in this section.

The screen below is displayed upon successful log in. Enter desired password for **New Password** and **Confirm Password**. Click **Change**.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised

You must change your temporary password to continue

New Password:

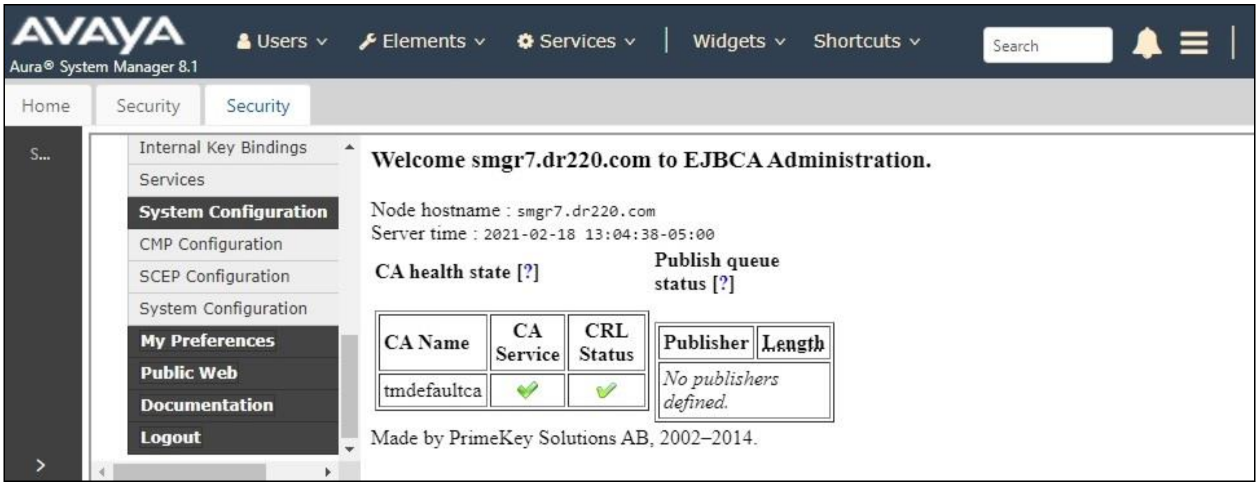
Confirm Password:

7.3. Obtain CA Certificate

The LDS connection with Session Manager Element Manager Web Service is encrypted and the Certification Authority (CA) certificate pertaining to the customer network needs to be obtained from the customer and installed on LDS.

In the compliance testing, the System Manager was used as the CA and the procedure to download the CA certificate from System Manager is described below.

From the System Manager web interface, select **Services → Security → Certificates → Authority** from the top menu to display the **Welcome** screen below. Select **Public Web** from the left pane.



Welcome smgr7.dr220.com to EJBCA Administration.

Node hostname : smgr7.dr220.com
Server time : 2021-02-18 13:04:38-05:00

CA health state [?]

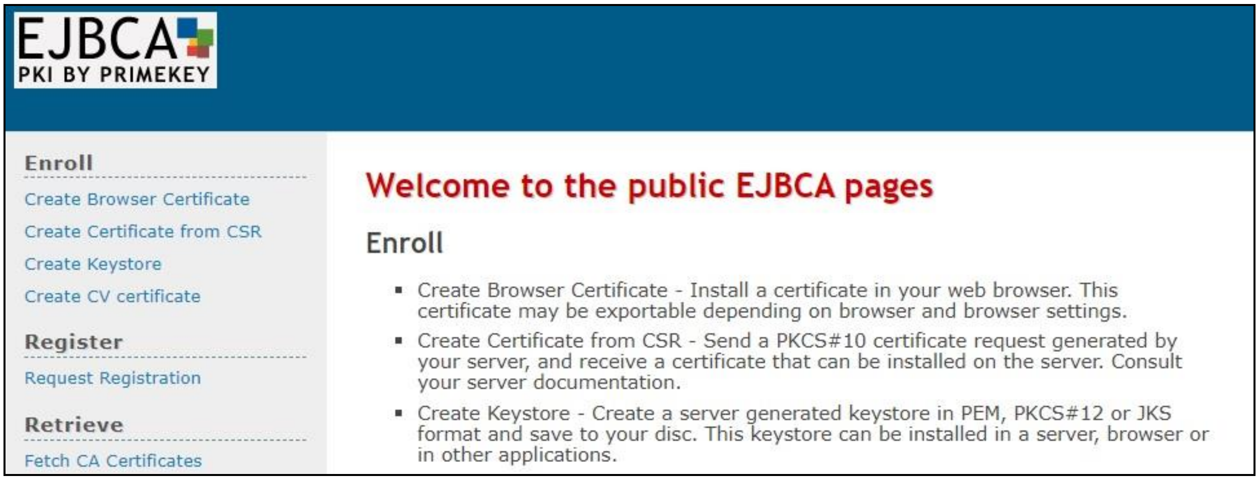
CA Name	CA Service	CRL Status
tmdefaultca	✓	✓

Publish queue status [?]

Publisher	Length
No publishers defined.	

Made by PrimeKey Solutions AB, 2002–2014.

The **Welcome to the public EJBCA pages** screen below is displayed next. Select **Retrieve → Fetch CA Certificates** from the left pane.



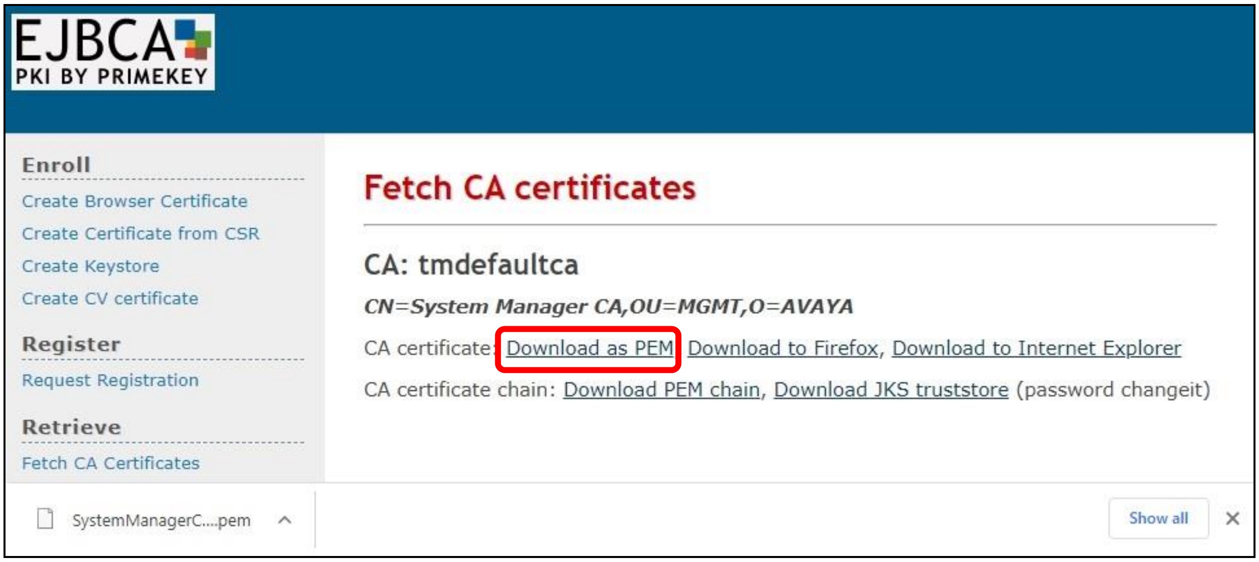
Welcome to the public EJBCA pages

Enroll

- Create Browser Certificate - Install a certificate in your web browser. This certificate may be exportable depending on browser and browser settings.
- Create Certificate from CSR - Send a PKCS#10 certificate request generated by your server, and receive a certificate that can be installed on the server. Consult your server documentation.
- Create Keystore - Create a server generated keystore in PEM, PKCS#12 or JKS format and save to your disc. This keystore can be installed in a server, browser or in other applications.

The **Fetch CA certificates** screen is displayed. Select **Download as PEM** to download the CA certificate.

After downloading, rename the downloaded CA certificate from the **pem** suffix to **der**, which is the extension type needed by LDS. In the compliance testing, the downloaded **SystemManagerCA.pem** file was renamed to **SystemManagerCA.der**, and will be used later to install on LDS.



Fetch CA certificates

CA: tmdefaultca

CN=System Manager CA,OU=MGMT,O=AVAYA

CA certificate: Download as PEM, Download to Firefox, Download to Internet Explorer

CA certificate chain: Download PEM chain, Download JKS truststore (password changeit)

8. Configure 911inform Location Discovery Solution

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

- Administer DMCC config.properties
- Administer ASM config.properties
- Install CA certificate
- Launch web interface
- Administer users

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

Prior to configuration, Connected Building configuration as documented in reference **[4]** is assumed to be in place along with enablement of the IP and MAC address change detection system parameter on Cloud Service.

After configuration, it is assumed that an initial registration request is sent by the Cloud Service to every configured registration notification user, and that the user's location address information is properly set via the link provided in the initial registration request.

8.1. Administer DMCC config.properties

Log in to the Linux shell of LDS. Navigate to the **~/DMCC-911inform-Dist/resources** directory and open the **config.properties** file with a text editor such as **vim**.

```
[xxxx@ubuntu:~$
[xxxx@ubuntu:~$ cd ~/DMCC-911inform-Dist/resources
[xxxx@ubuntu:~/DMCC-911inform-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**.
- **extensions:** The H.323 extensions and/or ranges from **Section 3**, separated by commas.
- **username:** The 911inform user credentials from **Section 6.5**.
- **password:** The 911inform user credentials from **Section 6.5**.
- **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”.
- **emgCodes:** The dialed digits for emergency calls, in this case “911”.
- **emgTypes:** “emergency”

```
aesIP=10.64.101.239
aesPort=4721
cmIP=10.64.101.236
extensions=65001-65002
username=911inform
password=911Inform#
cleanup=0
duration=180
apiKey=xxxxx
orgId=yyyyy
source=255.255.255.255
emgCodes=911
emgTypes=emergency
refreshTimer=180
```

8.2. Administer ASM config.properties

Navigate to the **~/ASM-Dist/resources** directory and open the **config.properties** file with a text editor such as **vim**.

```
xxxx@ubuntu:~$
xxxx@ubuntu:~$ cd ~/ASM-Dist/resources
xxxx@ubuntu:~/ASM-Dist/resources$ sudo vim config.properties
```

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

- **fqdn:** The fully qualified domain name of System Manager.
- **user:** The new administrative user credentials from **Section 7.2**.
- **password:** The new administrative user credentials from **Section 7.2**.
- **orgId:** The pertinent organizational ID value provided by 911inform.

```
fqdn=smgr7.dr220.com
user=911inform
password=test456
orgId=yyyyy
timeBetweenCalls=60
```

8.3. Install CA Certificate

Use a tool such as WinSCP to copy the CA certificate from **Section 7.3** to the LDS server. From the Linux shell of LDS, navigate to the directory containing the CA certificate.

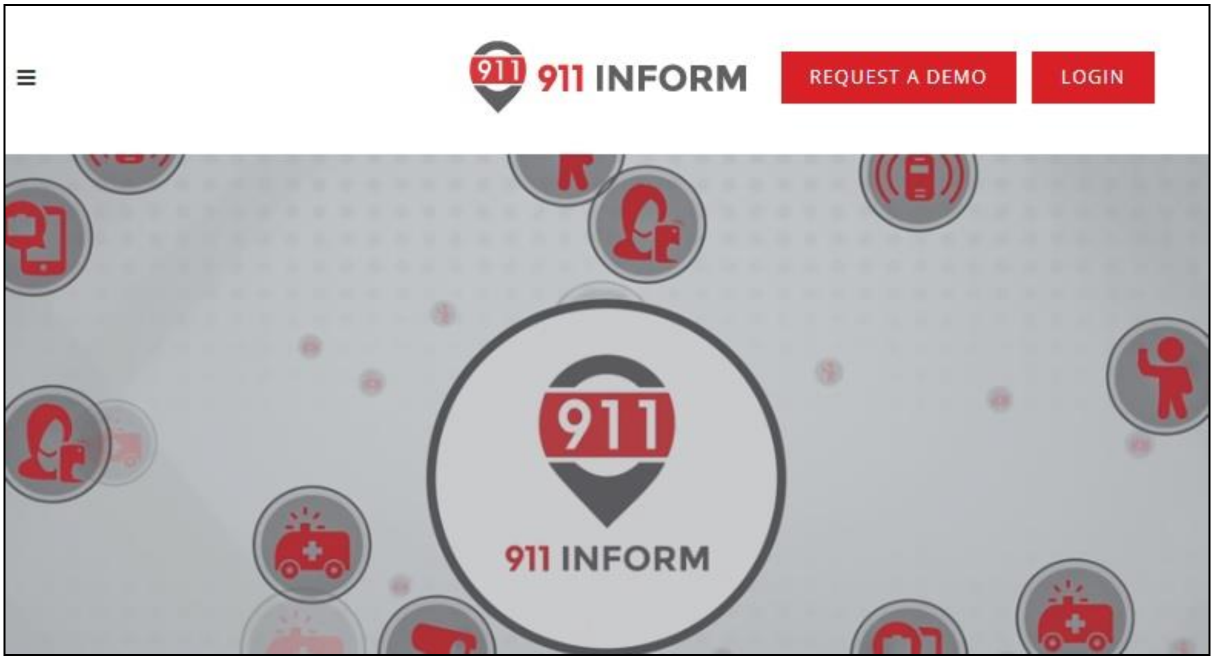
Use the **keytool** command shown below to install the CA certificate, where **ASM** is the alias and **SystemManagerCA.der** is the name of the CA certificate file.

When prompted, enter the pertinent keystore password, and make certain that the certificate is added to the keystore successfully, as shown below.

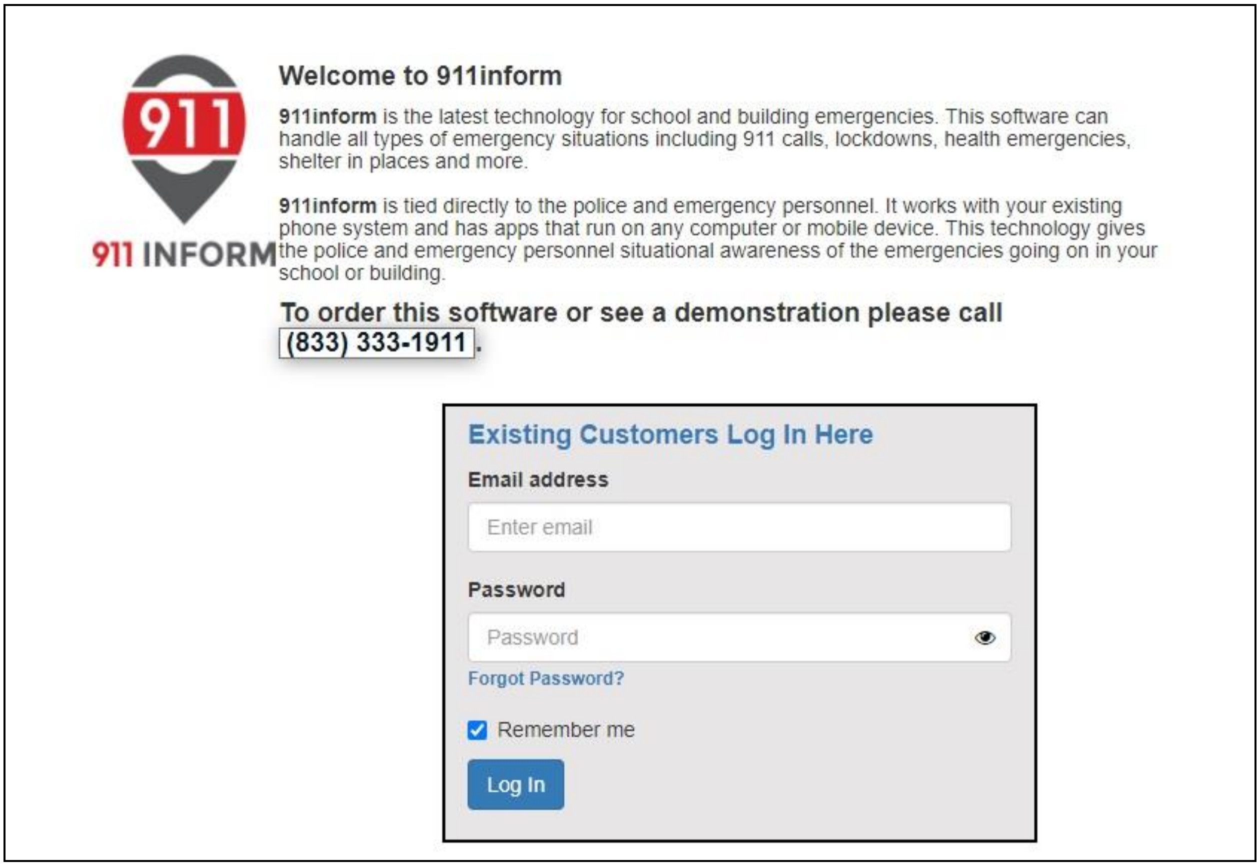
```
xxxx@ubuntu:~$
xxxx@ubuntu:~$ cd
xxxx@ubuntu:~$ ls
ASM-Dist  DMCC-911inform-Dist  DMCC-Crisis-Alert-Dist  SystemManagerCA.der
xxxx@ubuntu:~$
xxxx@ubuntu:~$ sudo keytool -import -alias ASM -keystore /etc/ssl/certs/java/cacerts -
file SystemManagerCA.der
Warning: use -cacerts option to access cacerts keystore
Enter keystore password:
Certificate was added to keystore
```

8.4. 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

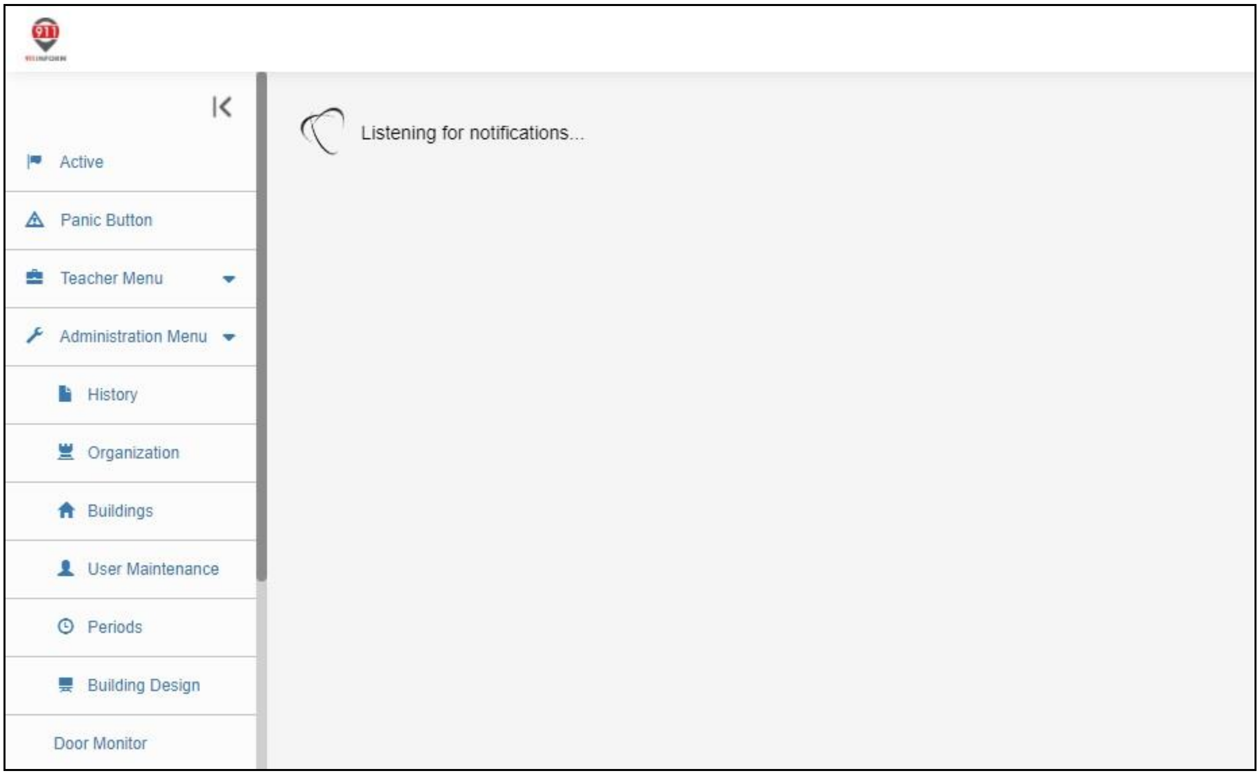
911inform is the latest technology for school and building emergencies. This software can handle all types of emergency situations including 911 calls, lockdowns, health emergencies, shelter in places and more.

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.

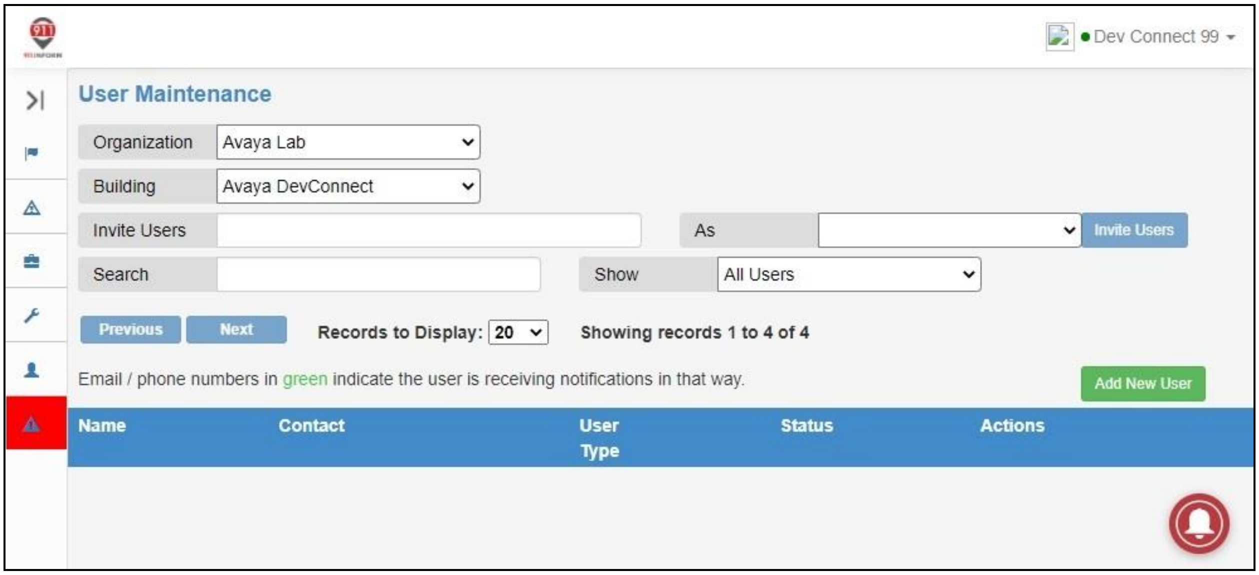
To order this software or see a demonstration please call (833) 333-1911.

8.5. Administer Users

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



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



Organization	Avaya Lab
Building	Avaya DevConnect
Invite Users	
As	
Search	
Show	All Users

Records to Display: 20 Showing records 1 to 4 of 4

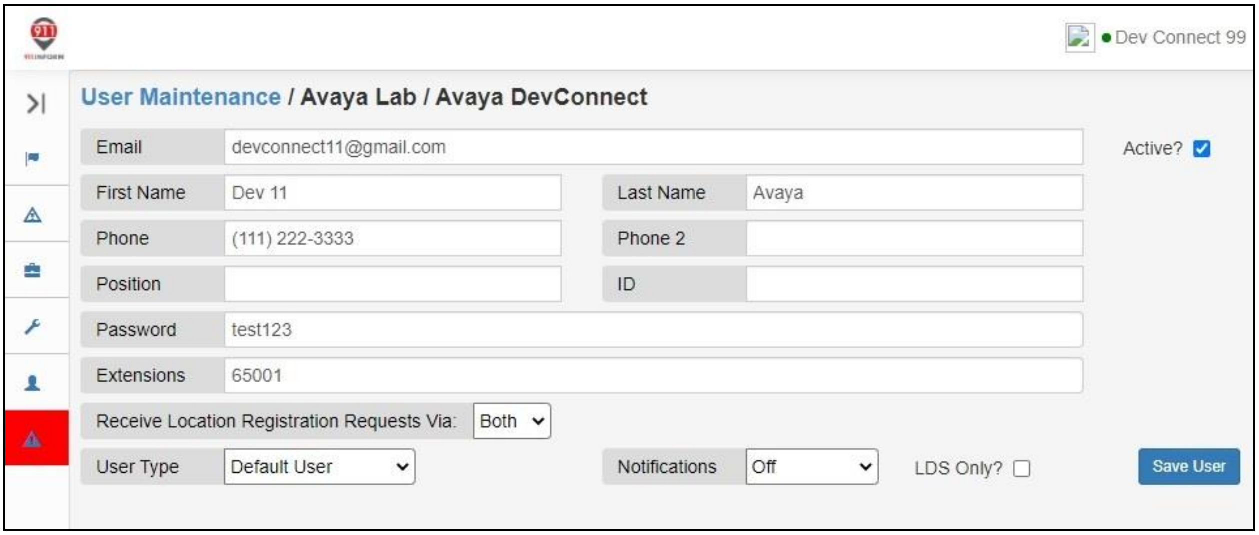
Email / phone numbers in green indicate the user is receiving notifications in that way.

Name	Contact	User Type	Status	Actions

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.
- **Extensions:** The pertinent user extension from **Section 3**.

For **Receive Location Registration Requests Via**, select the desired notifications, in this case "Both".

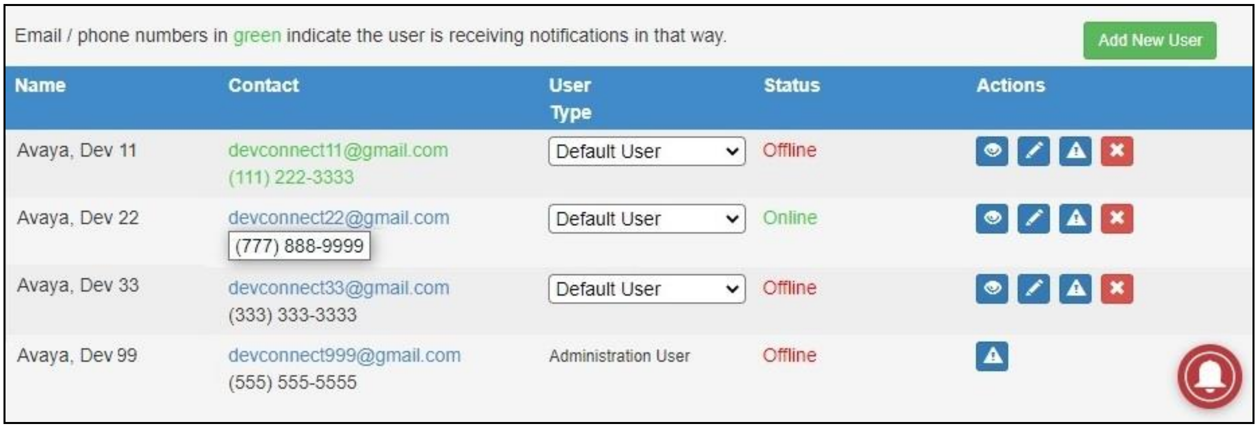


User Maintenance / Avaya Lab / Avaya DevConnect

Email	devconnect11@gmail.com	Active?	☑
First Name	Dev 11	Last Name	Avaya
Phone	(111) 222-3333	Phone 2	
Position		ID	
Password	test123		
Extensions	65001		
Receive Location Registration Requests Via:	Both		
User Type	Default User	Notifications	Off

LDS Only? ☐

Repeat this section to create an entry for each user extension from **Section 3** to receive registration notification upon a change in IP or MAC address. Below were the users used in 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	

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

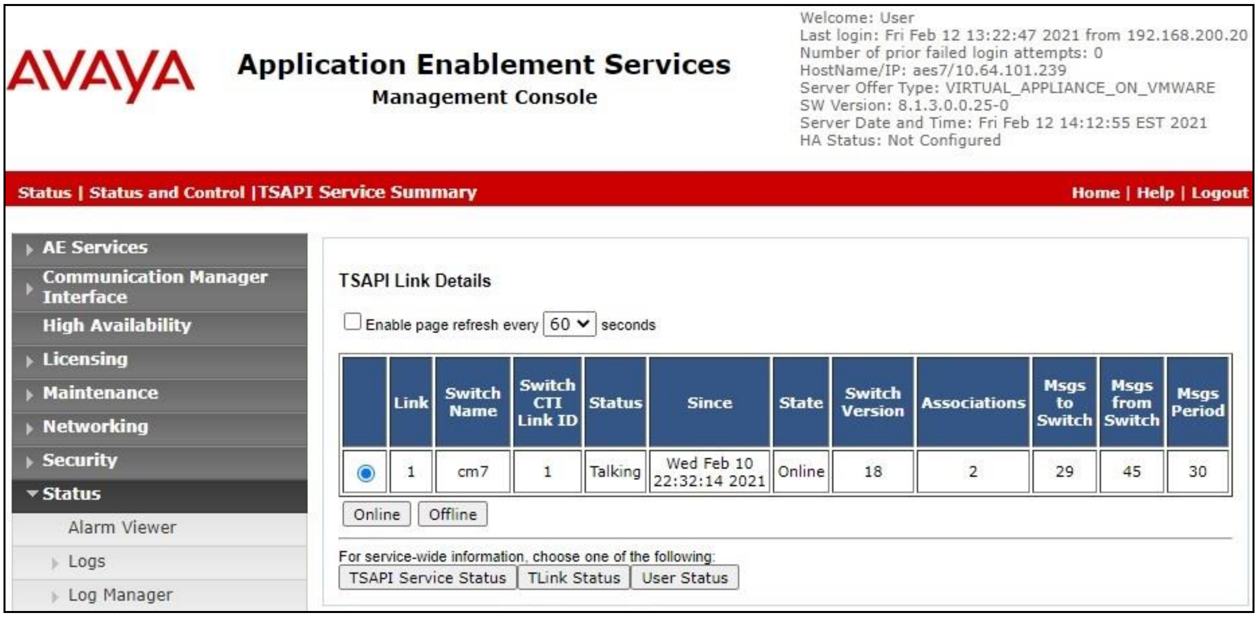
On Communication Manager, verify status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12       no    aes7             established   45       29
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane (not shown). The **TSAPI Link Details** screen is displayed.

Verify that **Status** is "Talking" for the TSAPI link administered in **Section 6.4**, and that the **Associations** column reflects the total number of monitored H.323 users from **Section 3**, in this case "2".



Welcome: User
Last login: Fri Feb 12 13:22:47 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: Fri Feb 12 14:12:55 EST 2021
HA Status: Not Configured

TSAPI Link Details

□ Enable page refresh every 60 seconds

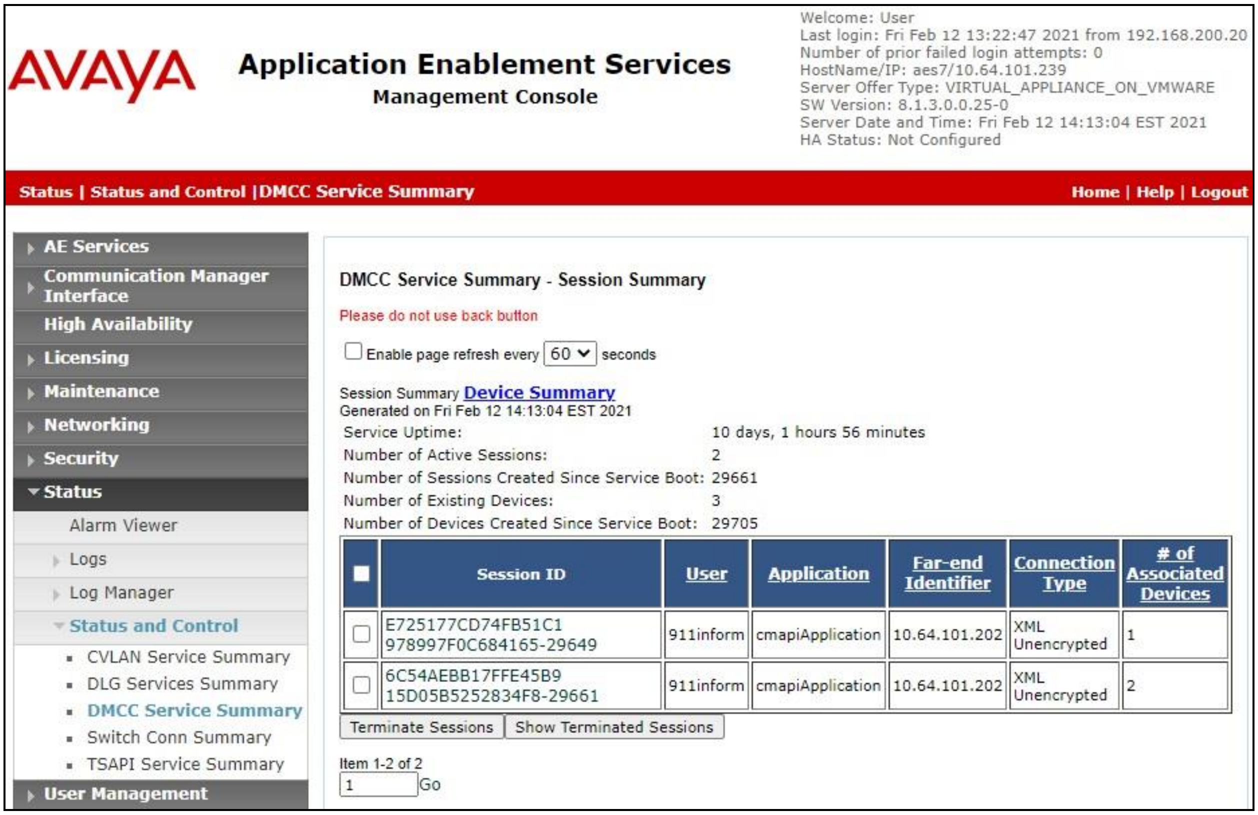
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Wed Feb 10 22:32:14 2021	Online	18	2	29	45	30

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

Verify status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the 911inform user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of monitored H.323 users from **Section 3**.

Note that the other active DMCC session shown below with the 911inform user is part of the Connected Building integration with Application Enablement Services as detailed in reference **[4]**.



Welcome: User
Last login: Fri Feb 12 13:22:47 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: Fri Feb 12 14:13:04 EST 2021
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Fri Feb 12 14:13:04 EST 2021

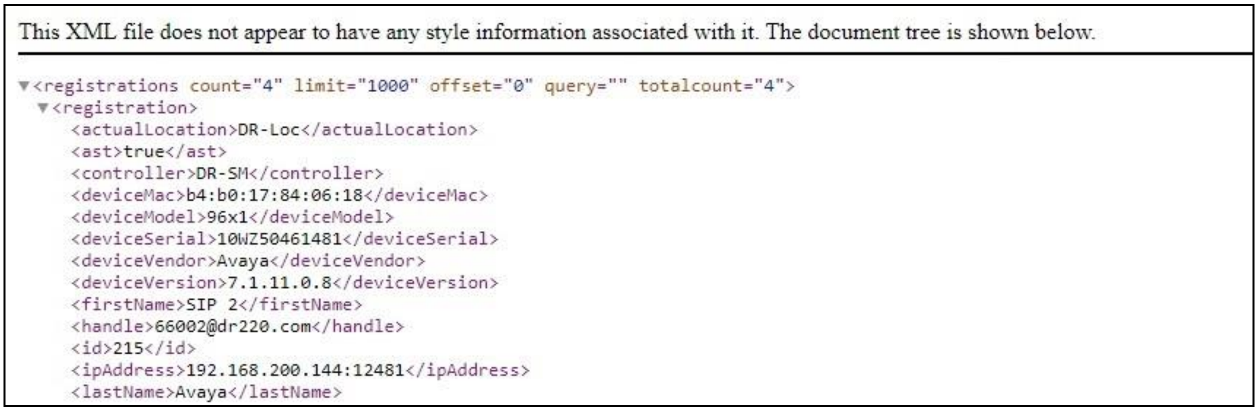
Service Uptime: 10 days, 1 hours 56 minutes
Number of Active Sessions: 2
Number of Sessions Created Since Service Boot: 29661
Number of Existing Devices: 3
Number of Devices Created Since Service Boot: 29705

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	E725177CD74FB51C1 978997F0C684165-29649	911inform	cmapiApplication	10.64.101.202	XML Unencrypted	1
□	6C54AEBB17FFE45B9 15D05B5252834F8-29661	911inform	cmapiApplication	10.64.101.202	XML Unencrypted	2

Item 1-2 of 2
1 Go

9.3. Verify Avaya Aura® Session Manager

Open an Internet browser window and enter the URL “https://ip-address/ASM/ws/registration”, where “ip-address” is the IP address of System Manager. Sign in with the updated administrative user credentials from **Section 7.2**. Verify that the registration status of SIP users is displayed, as partially shown below.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<registrations count="4" limit="1000" offset="0" query="" totalcount="4">
  ▼<registration>
     <actualLocation>DR-Loc</actualLocation>
     <ast>true</ast>
     <controller>DR-SM</controller>
     <deviceMac>b4:b0:17:84:06:18</deviceMac>
     <deviceModel>96x1</deviceModel>
     <deviceSerial>10WZ50461481</deviceSerial>
     <deviceVendor>Avaya</deviceVendor>
     <deviceVersion>7.1.11.0.8</deviceVersion>
     <firstName>SIP 2</firstName>
     <handle>66002@dr220.com</handle>
     <id>215</id>
     <ipAddress>192.168.200.144:12481</ipAddress>
     <lastName>Avaya</lastName>
```

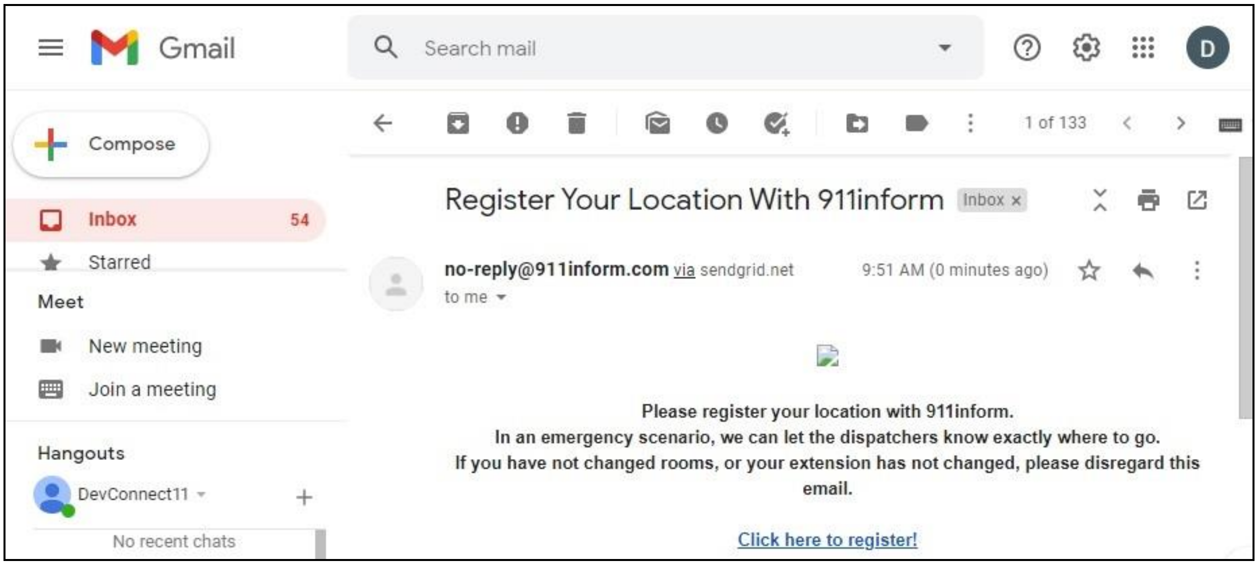
9.4. Verify 911inform Location Discovery Solution

Make an IP and/or MAC address change for a H.323 user and a SIP user from **Section 3**. Verify that the corresponding users configured in **Section 8.5** receive proper email and/or SMS notification and that the users can use the provided link to update his/her location information.

9.4.1. Verify Email Notification

Log the H.323 user into his/her email application. Verify that there is registration notification as shown below.

Repeat this section to verify email registration notification for the SIP user.



Register Your Location With 911inform

no-reply@911inform.com via sendgrid.net 9:51 AM (0 minutes ago)

to me

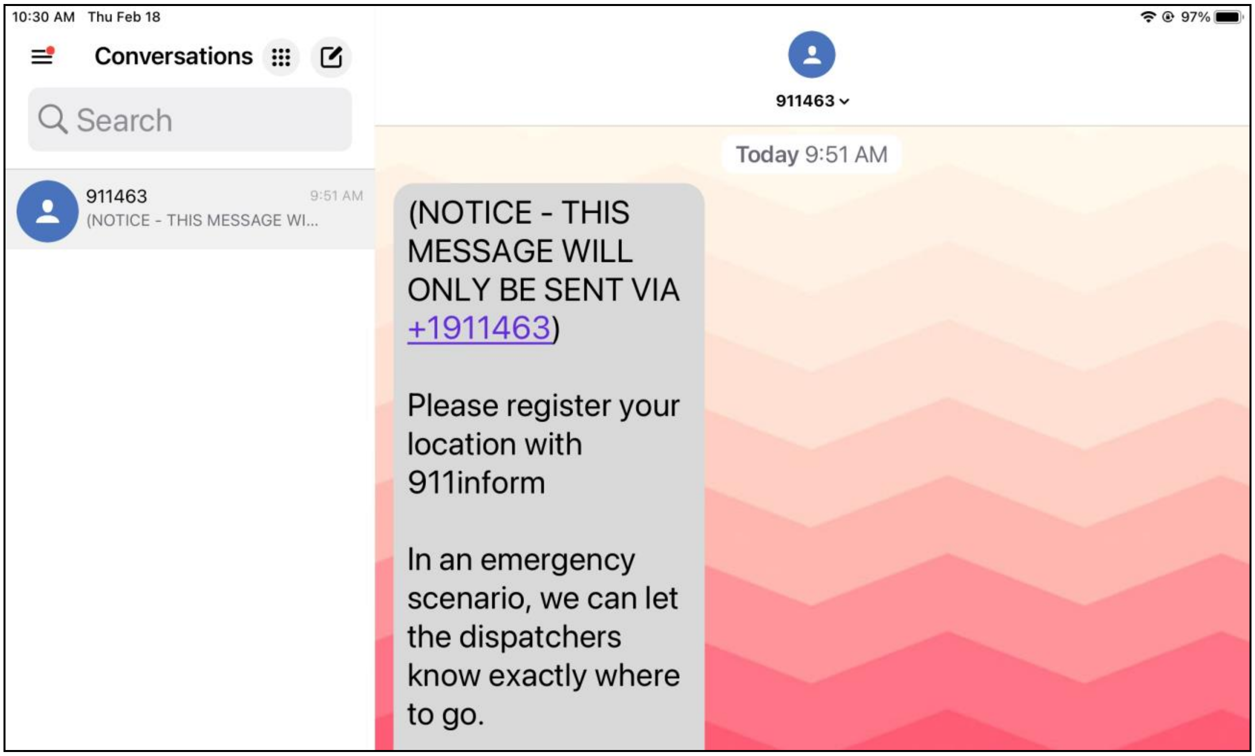
Please register your location with 911inform.
In an emergency scenario, we can let the dispatchers know exactly where to go.
If you have not changed rooms, or your extension has not changed, please disregard this email.

Click here to register!

9.4.2. Verify SMS Notification

Log the H.323 user into his/her SMS application or mobile phone. Verify that there is registration notification as shown below.

Repeat this section to verify SMS registration notification for the SIP user.



(NOTICE - THIS MESSAGE WILL ONLY BE SENT VIA +1911463)

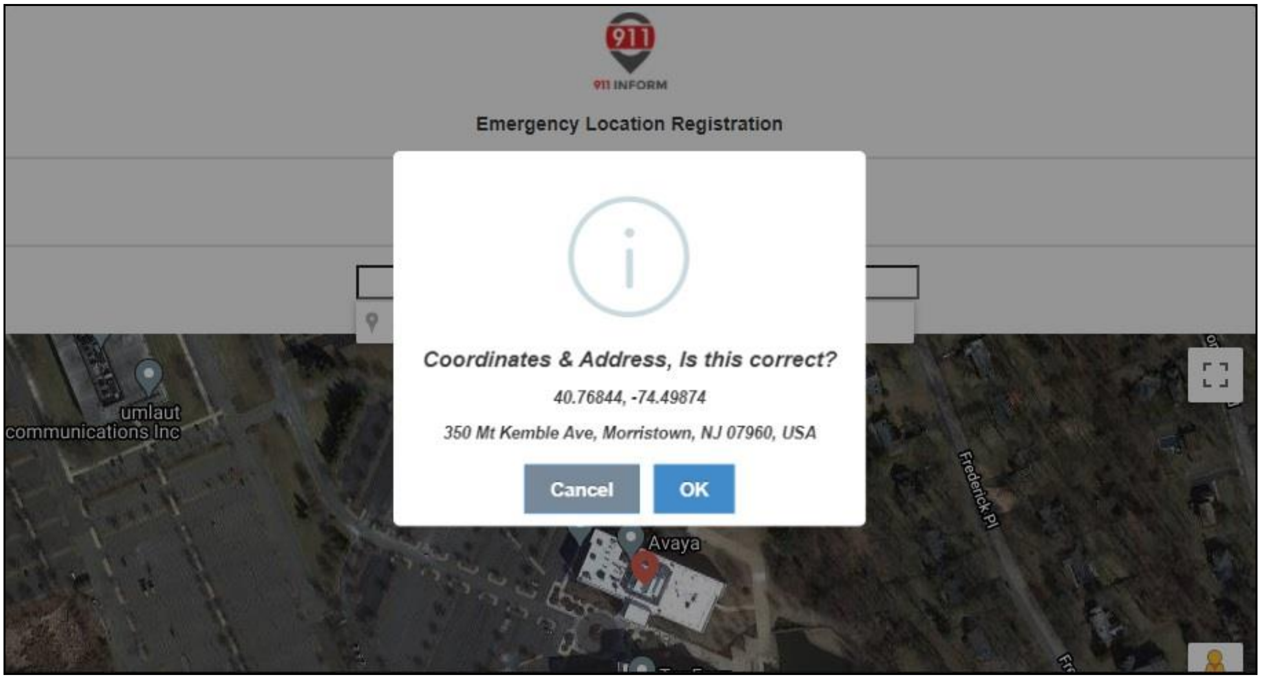
Please register your location with 911inform

In an emergency scenario, we can let the dispatchers know exactly where to go.

9.4.3. Verify Cloud Service

Click on the **Click here to register** link provided in the email notification from **Section 9.4.1** or the SMS notification from **Section 9.4.2** (not shown) to open a browser connection to the Cloud Service.

The **Emergency Location Registration** screen is displayed. Follow reference **[6]** to set and confirm the location address.



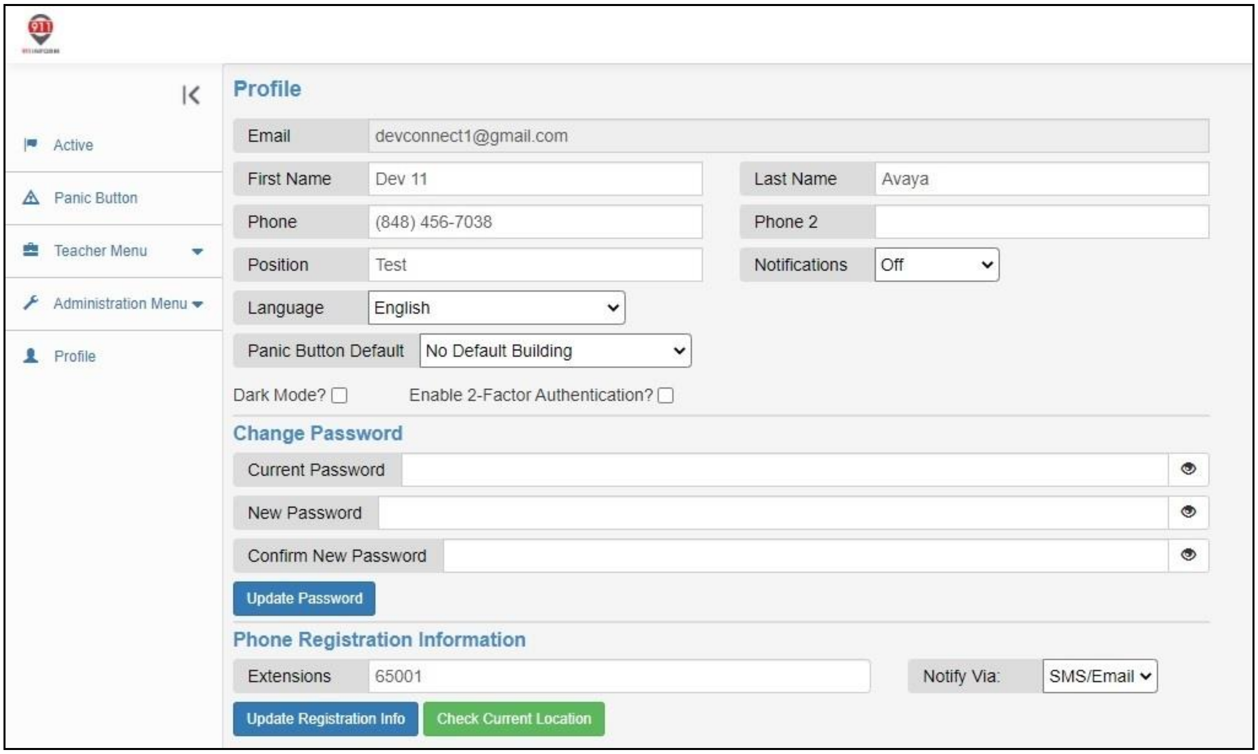
Emergency Location Registration

Coordinates & Address, Is this correct?

40.76844, -74.49874

350 Mt Kemble Ave, Morristown, NJ 07960, USA

Follow the procedures in **Section 8.4** to open another Internet browser window and log in with the H.323 user credentials. Select **Profile** from the left pane to display the **Profile** screen. Click **Check Current Location** toward bottom of screen.



Profile

Email	devconnect1@gmail.com		
First Name	Dev 11	Last Name	Avaya
Phone	(848) 456-7038	Phone 2	
Position	Test	Notifications	Off
Language	English		
Panic Button Default	No Default Building		

Dark Mode? □ Enable 2-Factor Authentication? □

Change Password

Current Password

New Password

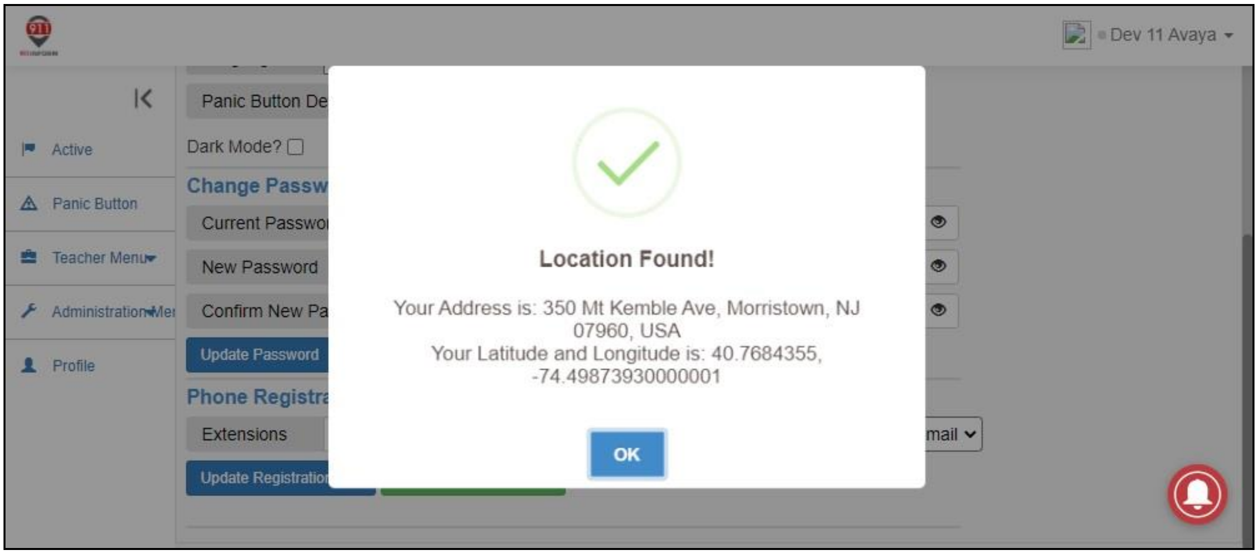
Confirm New Password

Phone Registration Information

Extensions	65001	Notify Via:	SMS/Email

Verify that a pop-up box is displayed with the same address set by the user.

Repeat this section to verify proper setting and verification of location address for the SIP user.



Location Found!

Your Address is: 350 Mt Kemble Ave, Morristown, NJ 07960, USA
Your Latitude and Longitude is: 40.7684355, -74.49873930000001

10. Conclusion

These Application Notes describe the configuration steps required for 911inform Location Discovery Solution to successfully interoperate with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Aura® Session Manager 8.1.3.   All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. 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. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at http://support.avaya.com.

4. *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, available at http://devconnectprogram.com.

5. *911inform LDS CM Integration*, available upon request to 911inform Support.

6. *911inform User Manual Administrator*, available upon request to 911inform Support.

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.