



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Intrado / 911 Enable Emergency Gateway with Avaya Aura® Session Manager, Avaya one-X® Deskphones and Avaya one-X® Communicator – Issue 1.0**

### **Abstract**

These Application Notes describe the procedures for configuring the Intrado / 911 Enable Emergency Gateway with Avaya Aura® Session Manager, Avaya one-X® Deskphones and Avaya one-X® Communicator.

The 911 Enable Emergency Gateway offers E911 call routing automatic and IP phone discovery. Avaya Aura® Session Manager connects to the Emergency Gateway via a SIP trunk and the Emergency Gateway connects to the public Internet to access the Emergency Routing Service. The compliance testing focused on placing 911 calls from Avaya one-X® Deskphones and Avaya one-X® Communicator connected to different network equipment to verify that their location and callback number could be properly determined.

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

# 1. Introduction

These Application Notes describe the procedures for configuring the Intrado / 911 Enable (911 Enable) Emergency Gateway (EGW) with Avaya Aura® Session Manager.

The 911 Enable Emergency Gateway offers E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. Avaya Aura® Session Manager connects to EGW via a SIP trunk. EGW connects to Intrado / 911 Enabled Emergency Routing Services (ERS) before the calls are routed to PSAP. The compliance testing focused on placing 911 calls from Avaya one-X® Deskphones and Avaya one-X® Communicator connected to different network equipment to verify that their location and callback number could be properly determined.

## 2. General Test Approach and Test Results

This section describes the compliance testing used to verify the interoperability of the EGW with Session Manager. This section covers the general test approach and the test results.

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 following features and functionality of the EGW were tested.

- Layer 2 discovery from supported SNMP enabled layer 2 switches.
- Layer 3 discovery of Avaya one-X® Deskphones that support the PUSH API.
- Layer 3 discovery of Avaya one-X® Communicator when used with 911 Enable E911 Softphone Locator (ESL) Software.
- PUSH API and ESL, both push the IP addresses and MAC addresses of Avaya IP phones to the EGW, therefore it is used for both layer 2 and layer 3 discovery
- Emergency calls from all endpoint types were routed to the ERS via the EGW.
- Proper location information provided for all “known” locations.
- Calls from “unknown” locations were routed to the 911 Enable Emergency Call Response Center (ECRC).
- Callback numbers were assigned using the EGW Extension-Bind feature.
- Calls placed using the provided callback number were routed to the proper extension.
- Failover to the secondary EGW, if the primary EGW was not available.
- If neither EGW was available, Session Manager routed emergency calls to the ECRC via the PSTN.
- If the ERS was not available, the EGW routed emergency calls to the ECRC via Session Manager.

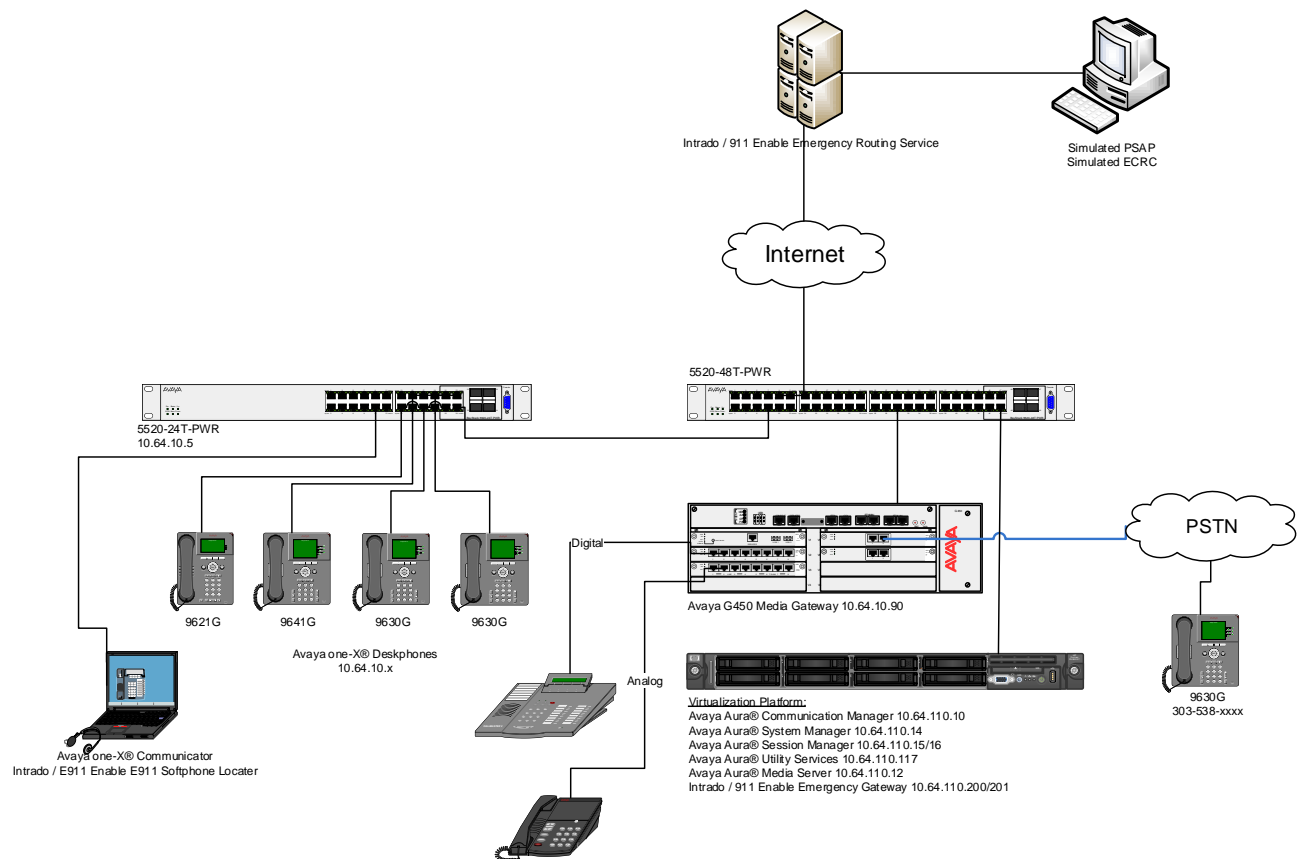
### 2.2. Test Results

The features described in **Section 2.1** were tested. All test cases passed successfully

## 2.3. Support

For technical support on the EGW, contact 911 Enable at [www.911enable.com](http://www.911enable.com).

## 3. Reference Configuration



### 3.1. Auto-Discovery of Endpoints

The EGW attempts to auto discover the presence and location of Avaya one-X® Desk Phones by correlating data obtained through two mechanisms.

1. The first mechanism is known as layer 2 discovery. To support layer 2 discovery, each layer 2 switch where the above telephone types are connected must support certain SNMP V1, V2 MIB objects required by the EGW. In the test configuration, Avaya 5520-24T-PWR was used. The data obtained from layer 2 discovery includes the MAC address of the device connected to each port of the switch.
2. The second mechanism required for auto-discovery is known as layer 3 discovery. To support layer 3 discovery, each listed telephone type uses an application downloaded to it during initialization to report information to the EGW. Thus, the Avaya one-X® Desk Phones telephone types used must support the PUSH API. The information collected includes the MAC address, IP address and extension of the phone. Correlating the

information from layer 2 and 3, the EGW learns what extensions are physically connected to which layer 2 switch.

The location of Avaya one-X® Communicator is gathered in a similar manner. Layer 2 discovery is dependent upon which layer 2 switch the Windows PC running Avaya one-X® Communicator is connected. Layer 3 discovery is done by installing the 911 Enable ESL software on the same PC, to report the necessary information for these endpoints.

All digital and analog endpoints also must be manually provisioned.

### 3.2. Callback Numbers

A callback number (CBN) is assigned to each extension for use by the 911 operator to reach the caller if the emergency call is dropped. The callback number for each extension would be its Direct Inward Dial (DID) number if it has one assigned. However, all internal extensions may not have a DID assigned. In this case, where an extension does not have a DID assigned, the EGW will temporarily map a DID number to that extension for the duration of the emergency call. This is known as the EGW Extension-Bind feature. The pool of DIDs used by the EGW is assigned to the EGW from the DIDs owned by the enterprise. In the case of the compliance test, none of the extensions were assigned an individual DID number, instead all extensions were assigned a temporary DID from the EGW during an emergency call. In addition, a single DID number was allocated to the EGW for this purpose.

### 3.3. Emergency Call Flows

Emergency calls are routed differently depending on whether all components are operational and what information is available about the caller.

1. **Typical “Sunny Day” Scenario:** If all components and user information are available then the call flow is as follows: User Extension → Session Manager → EGW → ERS → PSAP. If a callback call is needed and a temporary DID number is used from the EGW Extension-Bind pool, then the callback call flow is PSAP → PSTN → Session Manager → EGW → Session Manager → User Extension. If the user extension has its own DID number, then the callback call would not need to be routed through the EGW but would flow from PSAP → PSTN → Session Manager → User Extension.
2. **Missing User Information:** If all components are operational, but the emergency call does not have the proper location or callback information, then the call is routed to the ECRC where a trained 911 operator collects the correct information before forwarding the call to the PSAP. This call can reach the ECRC in two different ways based on the provisioning of the EGW. The EGW can be provisioned to reject the call if all necessary information is not present, so that Session Manager reroutes the call out the PSTN. This was done for the compliance test. The call flows from User Extension → Session Manager → EGW (rejects the call), then the call is rerouted as Session Manager → PSTN → ECRC → PSAP. Alternatively, the EGW can be provisioned to accept the call and send it to the ERS. The ERS will determine that all information is not present and send the call to the ECRC. The call flow would be User Extension → Session Manager → EGW → ERS → ECRC → PSAP. Either the ECRC or the PSAP can initiate a callback if necessary. If the callback is made from the PSAP, the callback call flow would be the same as described in scenario 1 above. If

the ECRC places the callback, the call flow is the same as described in scenario 1 with the exception that the ECRC replaces the PSAP in the call flow.

3. **ERS Unavailable:** If the EGW is operational but the ERS is unavailable, then when the EGW receives an emergency call, it will originate a call to the ECRC (using the 10 digit ECRC number) through Session Manager. The call flows from User Extension → Session Manager → EGW, then EGW → Session Manager → PSTN → ECRC → PSAP. The callback call flows would be the same as the callback call flows described in scenario 2 above.
4. **EGW Failover:** If the primary EGW fails, Session Manager will reroute the call to the secondary EGW. The call flow would be the same as scenario 1 above.
5. **Both EGWs Fail:** If both EGWs fail, Session Manager will reroute the call to the ECRC. The call flow is User Extension → Session Manager → EGW (no response), then the call is rerouted as Session Manager → PSTN → ECRC → PSAP. The callback call flows would be the same as the callback call flows described in scenario 2 above.

## 4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Aura® Communication Manager	7.0 Service Pack 1
Avaya G450 Media Gateway	39.17.0
Avaya Aura® Session Manager	7.0.0
Avaya Aura® System Manager	7.0
Avaya Aura® Utility Services	7.0
Avaya Aura® Media Server	7.7.0.226
Avaya one-X® Deskphones	SIP 7.0.0 H.323 6.6.0 H.323 3.2.5
Avaya one-X® Communicator	6.2 Feature Pack 10
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Intrado / 911 Enable Emergency Gateway	5.0.1
Intrado / 911 Enable Emergency Routing Service	3.8
Intrado / 911 Enable E911 Softphone Locator Software	2.4

## 5. Configure Avaya Aura® Session Manager

This section describes the Session Manager configuration to support connectivity to the EGWs and related functionality. It assumes all other components of **Figure 1** have already been configured. For more detailed information on any other Session Manager configuration shown in **Figure 1**, see [2]. Also note that, it is assumed that relevant configuration for Communication Manager is already in place.

The configuration of Session Manager was performed via Avaya Aura® System Manager. Enter the URL of System Manager such as <https://<system-manager-ip-address>/network-login/> of the System Manager. Log in using appropriate credentials.

**AVAYA**  
Aura® System Manager 7.0

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

## 5.1. Add a SIP Entity

Navigate to **Routing → SIP Entities**. Click **New** to add a new SIP entity for 911 Enable EGW.

- Type in a descriptive name in **Name**, egw-1.
- Type in IP address of 911 Enable EGW in **FQDN or IP Address**.
- Set **Type** to **SIP Trunk**.
- Set **Location** to a configured Location.

Click **Commit** to save changes.

The screenshot shows the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a 'Last Logged on at Nov' status. Below the navigation bar, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sub-menu on the left lists various routing-related options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area displays the 'SIP Entity Details' form for a new entity named 'egw-1'. The form is divided into sections: 'General' (containing fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Credential name, Securable, and Call Detail Recording), 'Loop Detection' (containing fields for Loop Detection Mode, Loop Count Threshold, and Loop Detection Interval), and 'SIP Link Monitoring' (containing a field for SIP Link Monitoring). The 'Commit' and 'Cancel' buttons are located at the top right of the form.

**AVAYA**  
Aura® System Manager 7.0

Last Logged on at Nov

Home Routing

Home / Elements / Routing / SIP Entities

**SIP Entity Details** Commit Cancel

**General**

\* Name: egw-1

\* FQDN or IP Address: 10.64.110.200

Type: SIP Trunk

Notes:

Adaptation:

Location: DevConnect-Lab

Time Zone: America/Denver

\* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: egress

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

Add another SIP Entity, Navigate to **Routing → SIP Entities**.

- Type in a descriptive name in **Name**, egw-2.
- Type in IP address of 911 Enable EGW in **FQDN or IP Address**.
- Set **Type** to **SIP Trunk**.
- Set **Location** to a configured Location.

Click **Commit** to save changes.



**AVAYA**  
Aura® System Manager 7.0

Last Logged on at Nov

Home Routing x

Home / Elements / Routing / SIP Entities

## SIP Entity Details

Commit Cancel

### General

\* Name: egw-2

\* FQDN or IP Address: 10.64.110.201

Type: SIP Trunk

Notes:

Adaptation:

Location: DevConnect-Lab

Time Zone: America/Denver

\* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: egress

### Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

### SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

## 5.2. Add an Entity Link

Once the SIP Entities are added, edit EGW1-911-Enable SIP Entity. At the bottom of the page click **Add** under **Entity Links**.

- Set **SIP Entity 1** to Session Manager's SIP Entity
- Set **Protocol** to **TCP**
- Set **Port** to **5060**
- Set **SIP Entity 2** to the egw-1 SIP Entity added in previous step
- Set **Port** to **5060**

Click **Commit** to save changes.

Add
Remove

1 Item
Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* asm_egw-1_5060_TCP	asm	TCP	* 5060	egw-1	* 5060	trusted

Select : All, None

**Note:** Repeat this step for egw-2 SIP Entity.

### 5.3. Add a Routing Policy

Routing Policies will need to be added for both SIP Entities for EGW. Navigate to **Routing** → **Routing Policies**. Click **New** to add a new Routing Policy for 911 Enable EGW.

- Type in the **Name** for Routing Policy.
- Select **SIP Entity as a destination**.
  - Select SIP Entity, egw-1.
- Under **Time of Day**, set **Ranking** to **1**.

Click **Commit** to save changes.

AVAYA  
Aura® System Manager 7.0

Last Logged on at November 18, 2015 4:33 PM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

\* Name: egw1

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
egw-1	10.64.110.200	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/> 1	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select : All, None

**Note:** Add another Routing Policy for EGW2-911-Enable. For **Time of Day**, set **Ranking** to **2**.

## 5.4. Add a Dial Pattern

Navigate to **Routing → Dial Patterns**. Click **New** to add a new Dial Pattern for 911 Enable EGW. On **Dial Patterns** page, click on **New**

- Set **Pattern** to **911**
- Set **Min** and **Max** to 3
- Check box for **Emergency Call**
- Type in **Emergency Priority**
- Type in **Emergency Type**
- Add **Originating Locations and Routing Policies** (Screen capture not shown)
  - Select location configured
  - Select Routing Policies configured for 911 Enable EGWs and Communication Manager

**Note:** It is assumed that Routing Policy for Communication Manager is pre-configured with **Ranking of 3**.

Click **Commit** to save changes.

AVAYA  
Aura® System Manager 7.0

Last Logged on at December 24, 2015 11:23 AM  
Go... Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel

Help ?

**General**

\* Pattern: 911

\* Min: 3

\* Max: 3

Emergency Call: ☒

\* Emergency Priority: 1

\* Emergency Type: Fire

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnect-Lab		egw1	1	<input type="checkbox"/>	egwr-1	
<input type="checkbox"/>	DevConnect-Lab		egw2	2	<input type="checkbox"/>	egwr-2	
<input type="checkbox"/>	DevConnect-Lab		acm	3	<input type="checkbox"/>	acm	

Select : All, None

## 6. Configure the Avaya Endpoints

This section describes the configuration required of Avaya endpoints to support the EGW functionality. Avaya H.323 and SIP telephones require additions to the 46xxsettings.txt file to support layer 3 discovery. The Avaya one-X® Communicator requires installation of the ESL software on the same PC running the Avaya one-X® Communicator. No special configuration is required for analog or digital telephones.

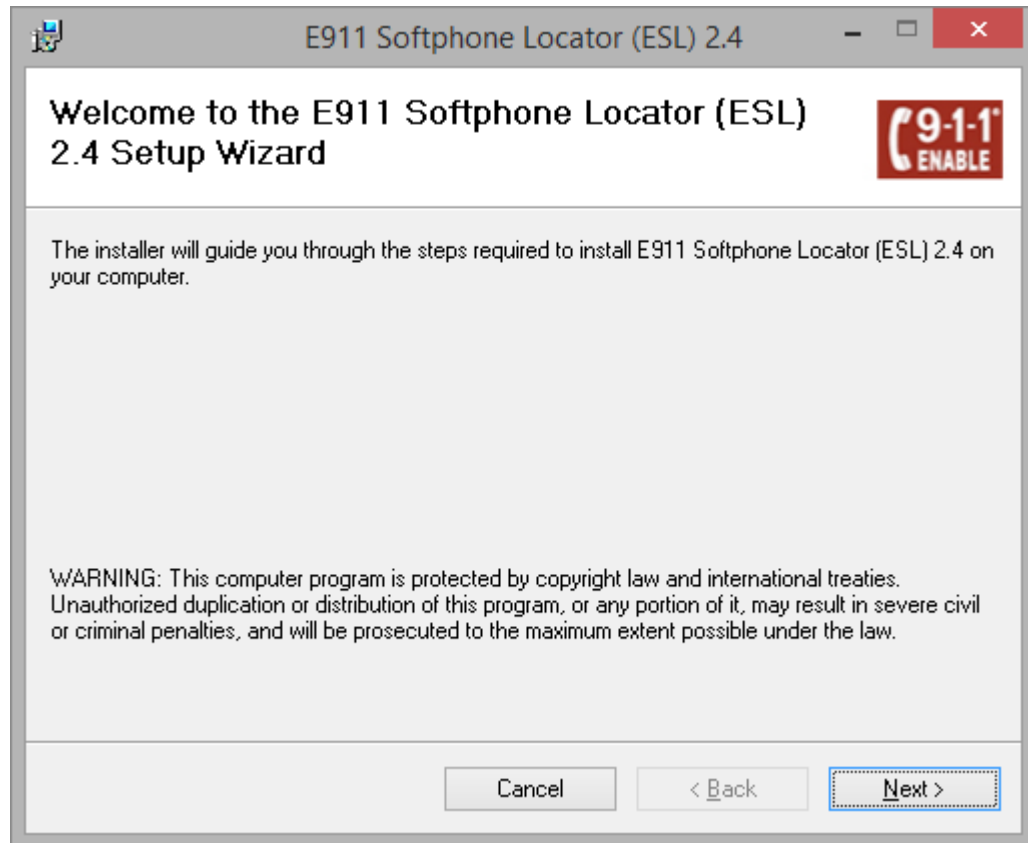
### 6.1. Avaya H.323 and SIP Telephone Configuration File

In order to support layer 3 discovery, the following lines need to be added to the 46xxsettings.txt configuration file for Avaya H.323 and SIP telephones. The two highlighted parameters in the **SUBSCRIBELIST** and **WMLHOME** URLs must be modified for a specific installation. The first parameter (**10.64.110.200**) represents the IP address of the private side of the primary EGW. The second parameter (**2**) is the **IP-PBX ID** number created in **Section 6, Step 6**.

```
## 911 Enable Settings
SET TPSLIST /
SET SUBSCRIBELIST http://10.64.110.200/2/r
SET PUSHPORT 80
SET PUSHCAP 2
SET WMLHOME http://10.64.110.200/wml/2/service.html
```

## 6.2. Avaya one-X® Communicator– ESL software installation

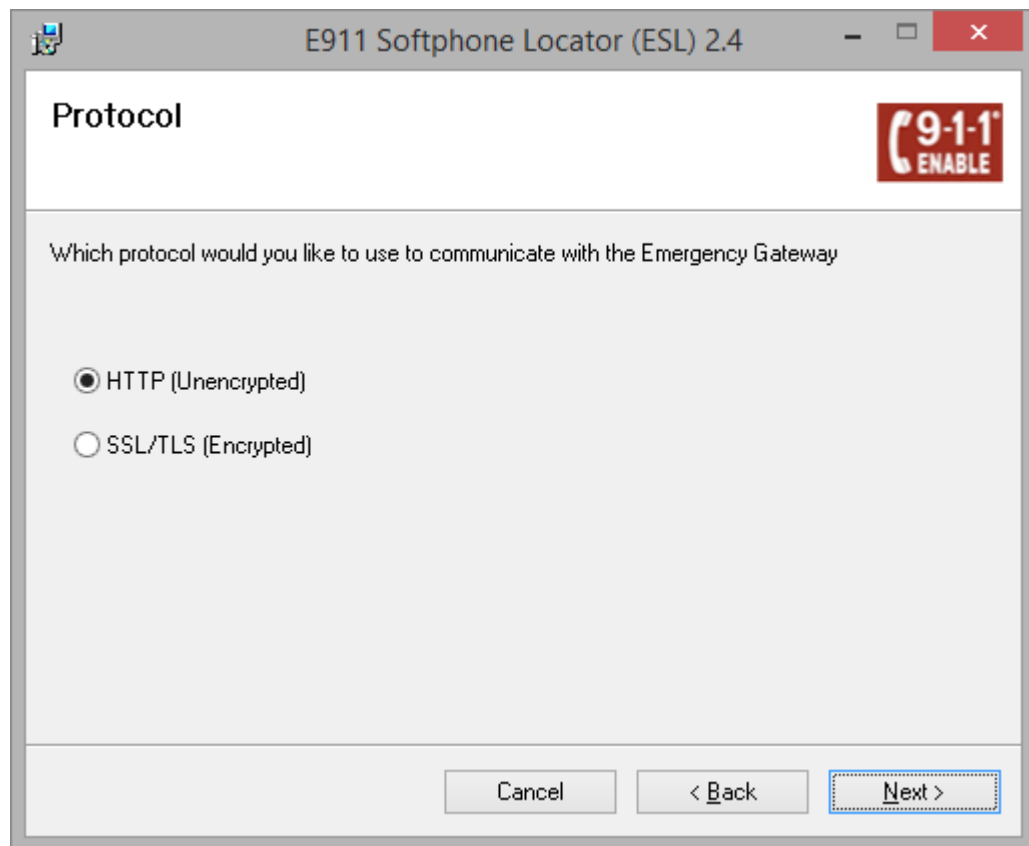
1. On the PC running the Avaya one-X® Communicator, launch the ESL setup application. A welcome screen will appear. Click **Next** to proceed.



2.

### ESL Installation – Select Protocol

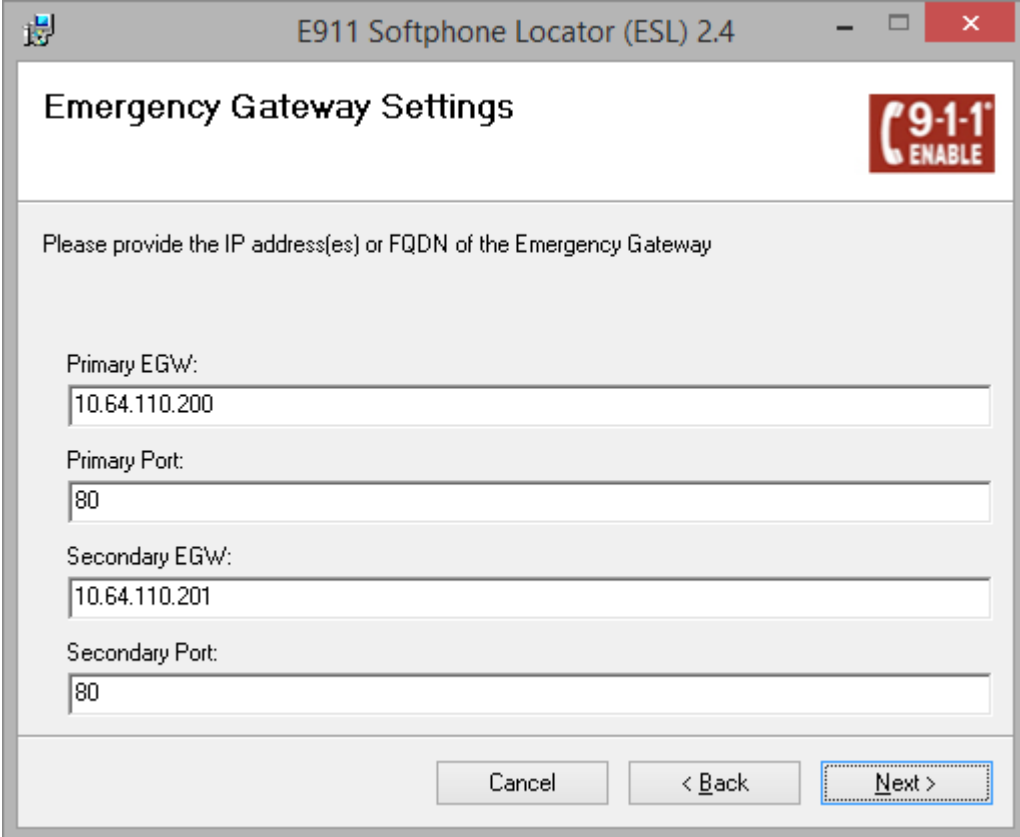
Select the desired protocol. HTTP was used for the compliance test. Click **Next**.



3.

### ESL Installation – EGW Settings

Enter the IP addresses for both EGWs. Use the default port **80** for HTTP. Click **Next**.



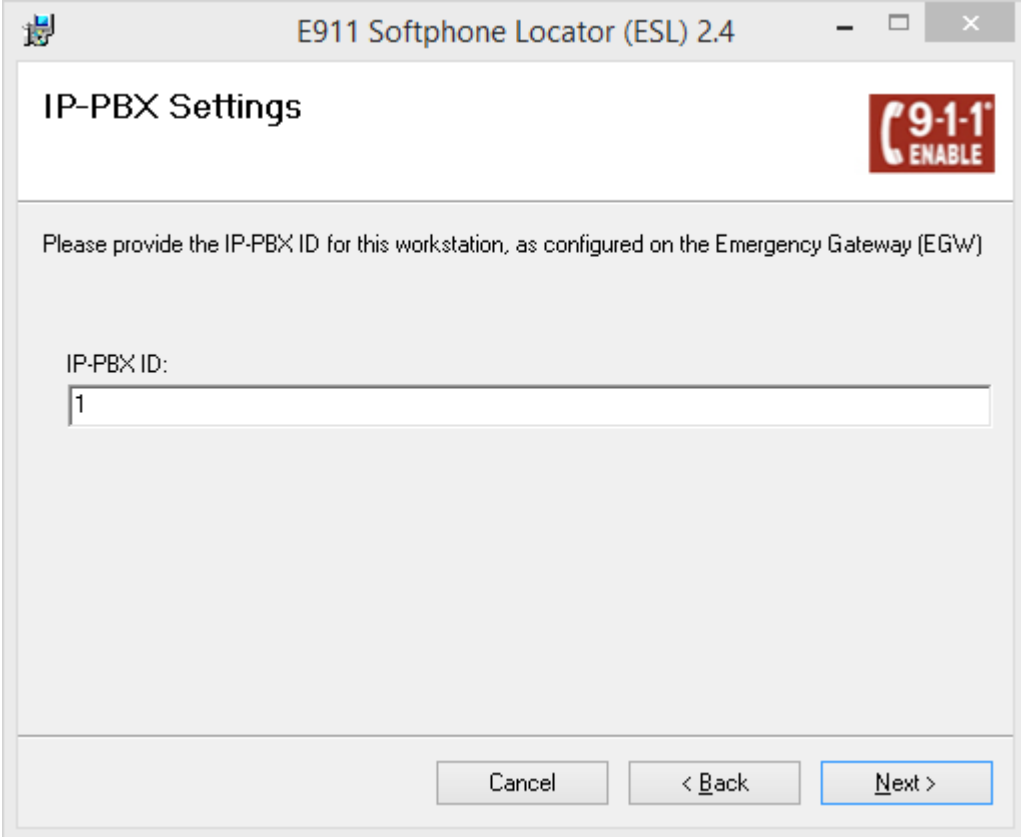
The screenshot shows a window titled "E911 Softphone Locator (ESL) 2.4". Inside the window, the title "Emergency Gateway Settings" is displayed at the top left, and a red "9-1-1 ENABLE" button is at the top right. Below the title, a message reads: "Please provide the IP address(es) or FQDN of the Emergency Gateway". There are four input fields: "Primary EGW:" with the value "10.64.110.200", "Primary Port:" with the value "80", "Secondary EGW:" with the value "10.64.110.201", and "Secondary Port:" with the value "80". At the bottom, there are three buttons: "Cancel", "< Back", and "Next >". The "Next >" button is highlighted with a blue dashed border.



4.

#### ESL Installation – IP-PBX Settings

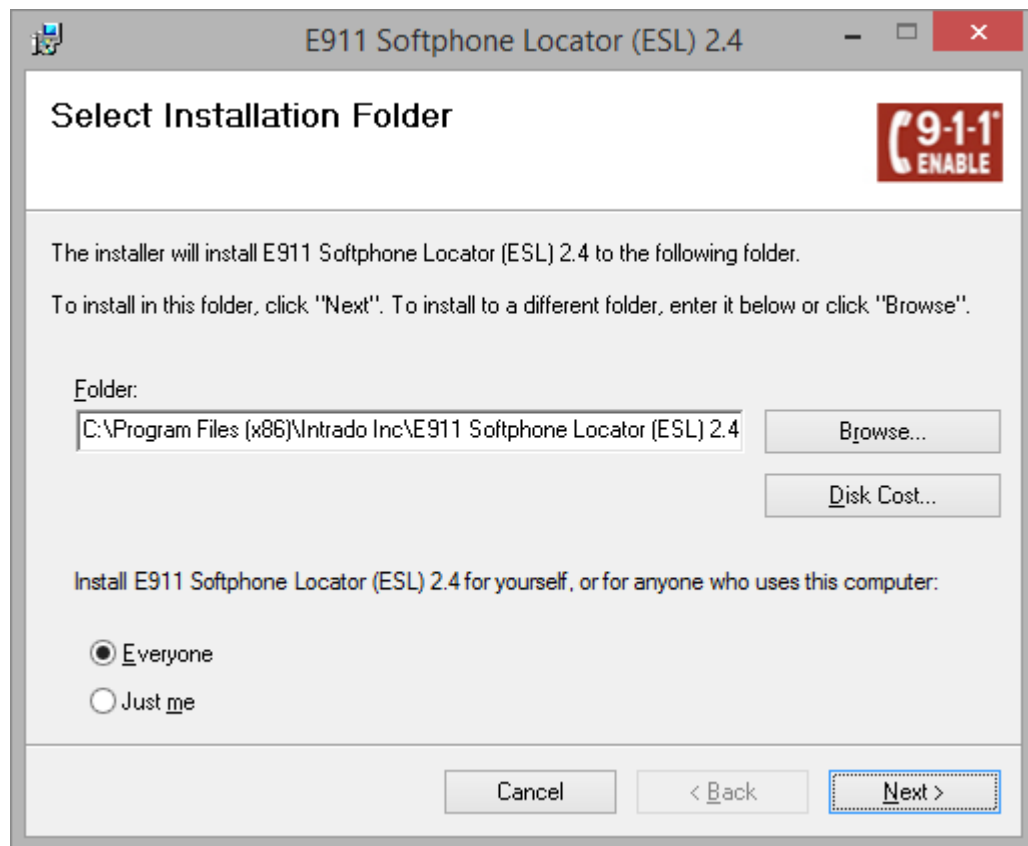
Enter an **IP-PBX ID**. Click **Next**.



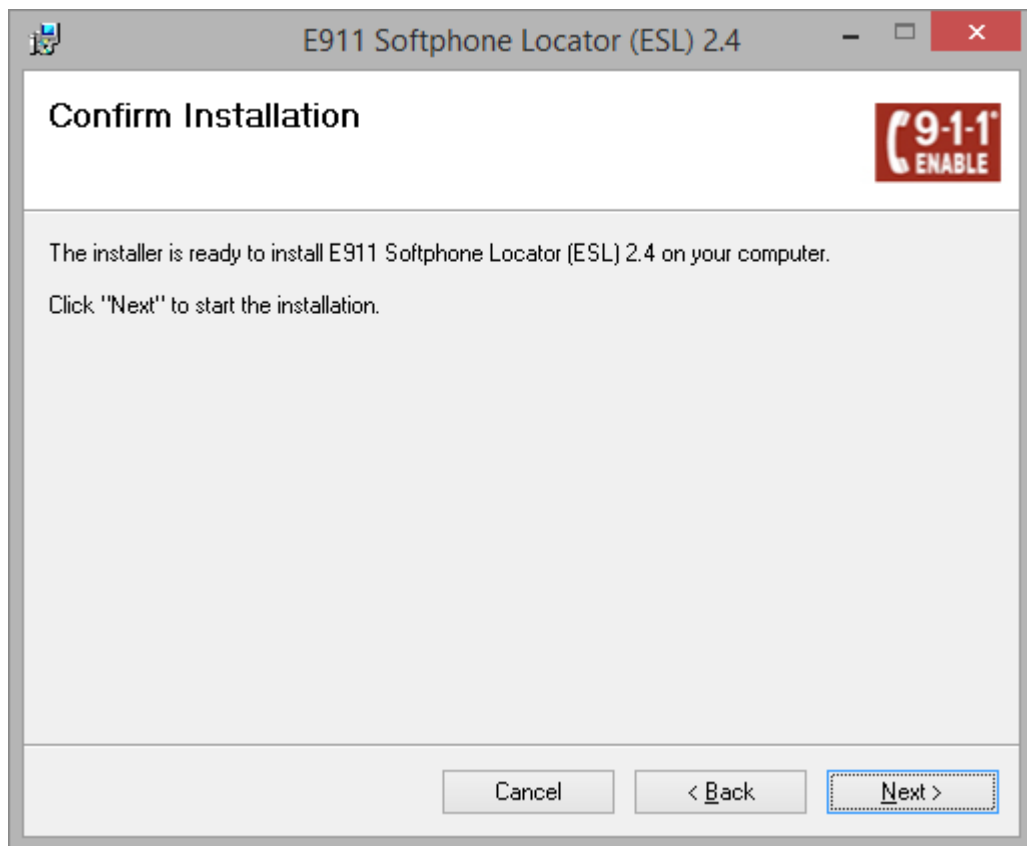
The screenshot shows a window titled "E911 Softphone Locator (ESL) 2.4". Inside the window, the title "IP-PBX Settings" is displayed at the top left, and a red "9-1-1 ENABLE" logo is at the top right. Below the title, a message reads: "Please provide the IP-PBX ID for this workstation, as configured on the Emergency Gateway (EGW)". Underneath this message, the label "IP-PBX ID:" is followed by a text input field containing the number "1". At the bottom of the window, there are three buttons: "Cancel", "< Back", and "Next >". The "Next >" button is highlighted with a blue border.

5. **ESL Installation – Installation Folder**

Enter the installation folder and who should have access to the software. Click **Next**.



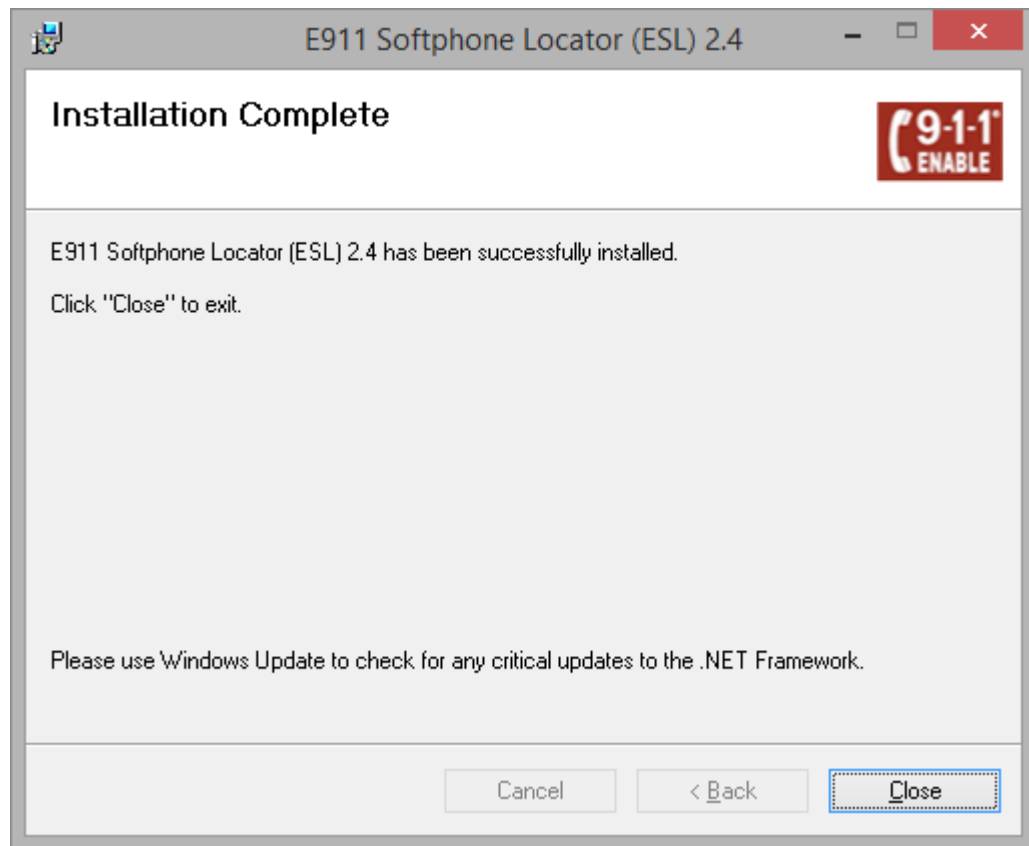
6. **ESL Installation – Confirm**  
Confirm the installation by clicking **Next**.



7.

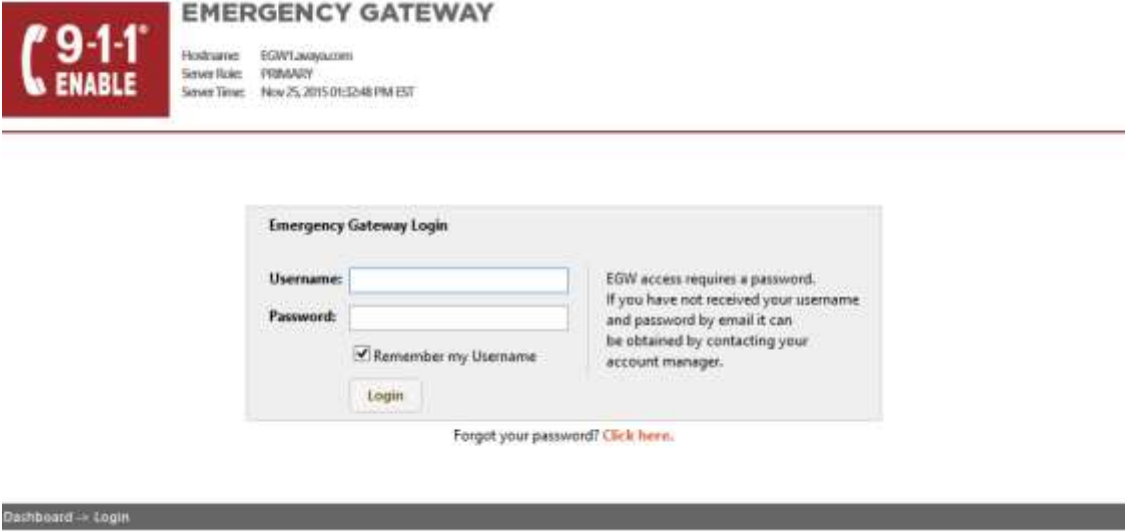
### **ESL Installation – Complete**


The following screen appears when installation is complete. Click **Close** to exit the set-up application.

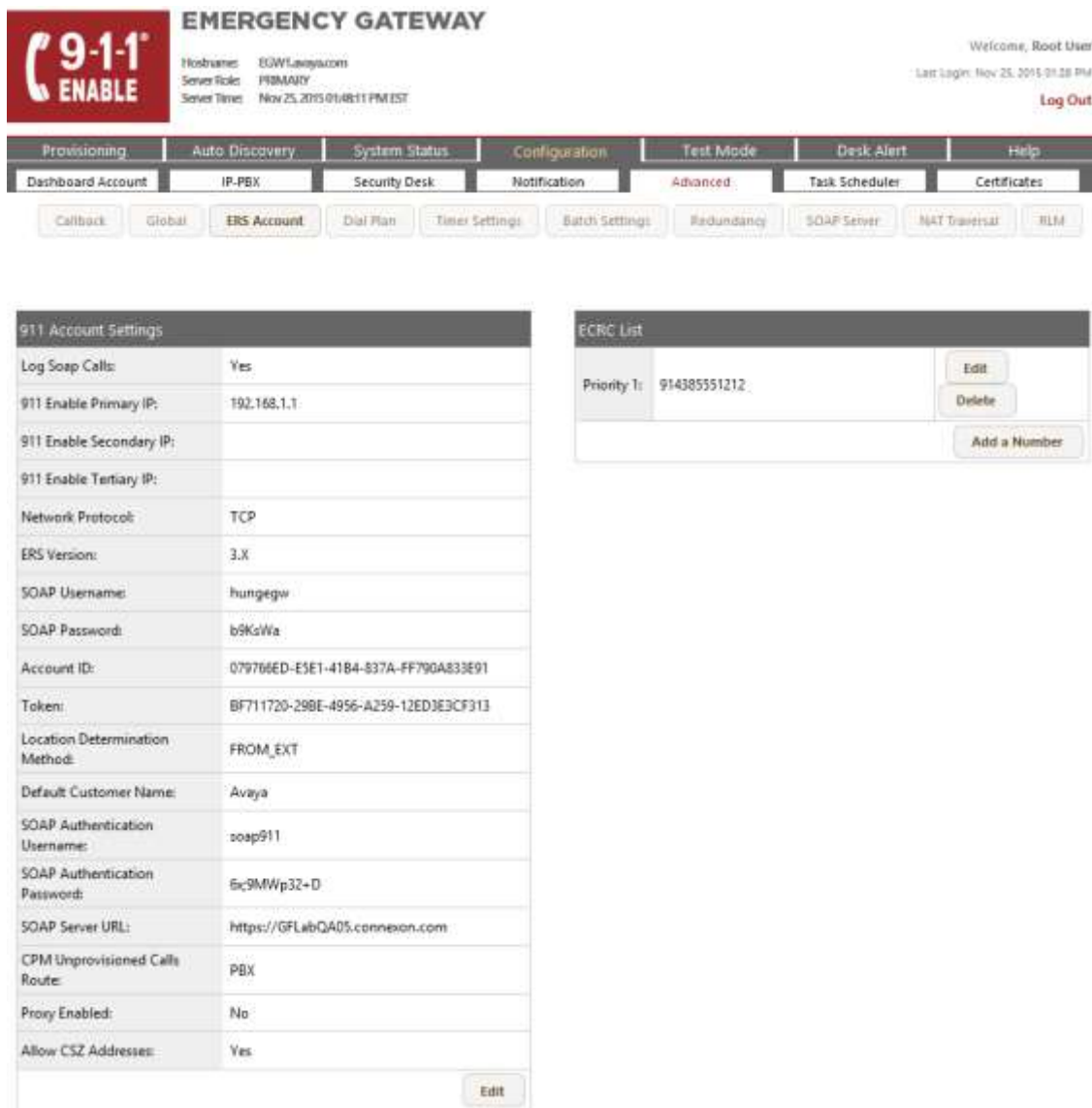


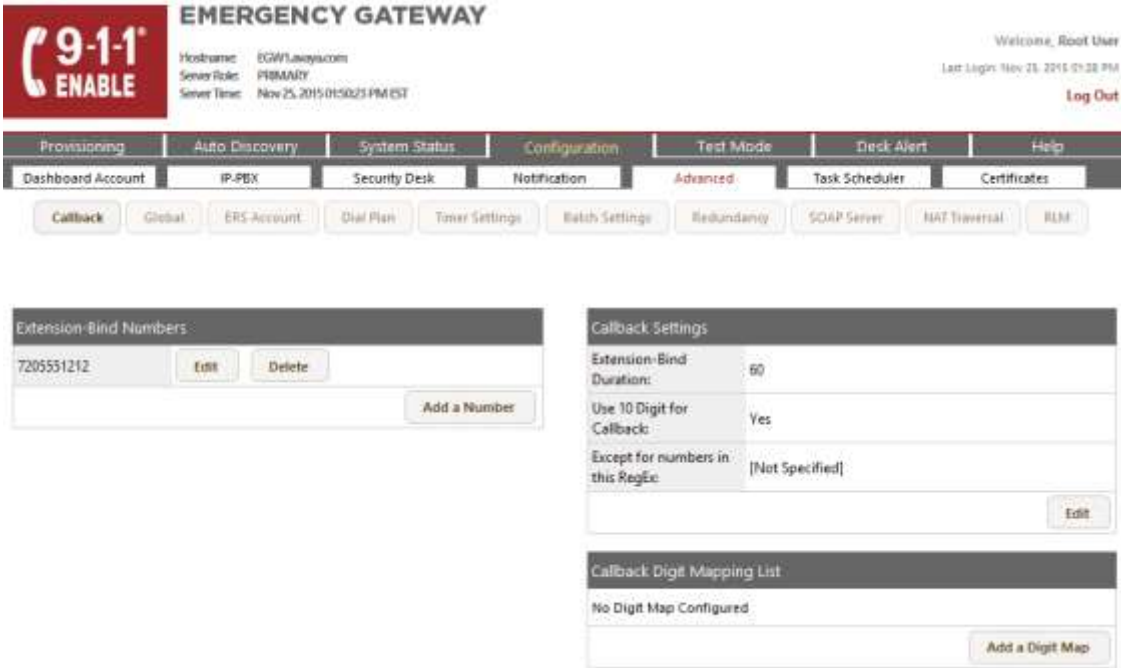

## 7. Configure Intrado / 911 Enable Emergency Gateway (EGW)

The configuration of the EGW is performed by 911 Enable for the customer when the customer subscribes to 911 Enable's Emergency Routing Service. The information in this section is included simply as a reference.

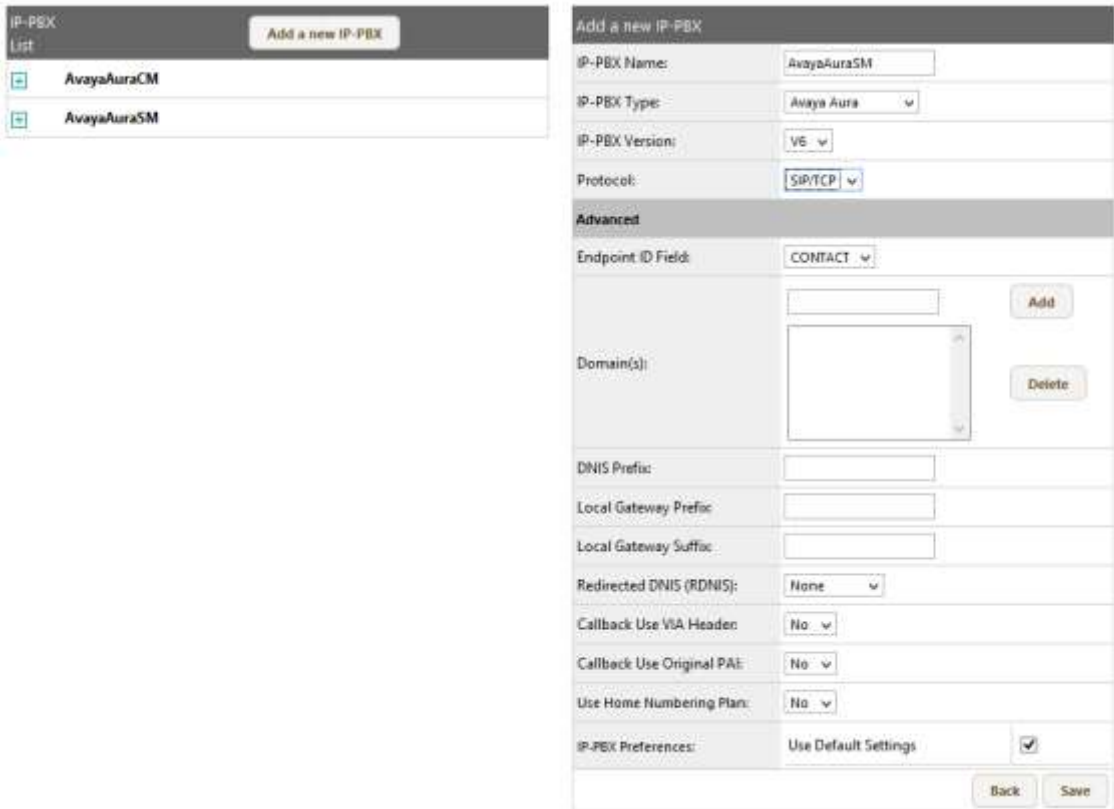
Step	Description
1.	<p><b>Login</b></p> <p>The EGW is configured via a web browser. To access the web interface, enter <a href="http://&lt;ip-addr&gt;">http://&lt;ip-addr&gt;</a> in the address field of the web browser, where &lt;ip-addr&gt; is the IP address of the primary EGW. Log in with the appropriate credentials. Click <b>Login</b>.</p> 


Step	Description																																																																																																																																																										
2.	<p><b>Main Page</b></p> <p>The main page of the EGW will appear.</p> <div><div></div><div><p><b>EMERGENCY GATEWAY</b></p><p>Hostname: EGW1aegw1a01m Server Role: PRIMARY Server Time: Nov 25, 2015 01:33:55 PM EST</p></div><div><p>Welcome, Root!</p><p>Last Login: Nov 25, 2015 01:31</p><p>Log</p></div><div><table><tr><td>Provisioning</td><td>Auto Discovery</td><td>System Status</td><td>Configuration</td><td>Test Mode</td><td>Desk Alert</td><td>Help</td></tr><tr><td>Status</td><td>Logs</td><td>Reports</td><td>CDRs</td><td>Alarms</td><td>Maintenance</td><td></td></tr></table></div><div><table><tr><th colspan="2">General Information</th><th colspan="12">Last 12 Months Endpoints Peak Reported:</th></tr><tr><td>Server Role:</td><td>Primary</td><td>January</td><td>February</td><td>March</td><td>April</td><td>May</td><td>June</td><td>July</td><td>August</td><td>September</td><td>October</td><td>November</td><td>Decen</td></tr><tr><td>PBX Count:</td><td>2</td><td>Total</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>10</td><td>0</td></tr><tr><td>ERLs Count:</td><td>6</td><td>Date</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>0000-00-00</td><td>2015-11-14</td><td>0000-0</td></tr><tr><td>Maximum Endpoints Allowed:</td><td>100</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Endpoints Count:</td><td>9</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Provisioned Endpoints Count:</td><td>9</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Billable Endpoints:</td><td>9</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Active Alarms Count:</td><td>16</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Switches Count:</td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></div></div>	Provisioning	Auto Discovery	System Status	Configuration	Test Mode	Desk Alert	Help	Status	Logs	Reports	CDRs	Alarms	Maintenance		General Information		Last 12 Months Endpoints Peak Reported:												Server Role:	Primary	January	February	March	April	May	June	July	August	September	October	November	Decen	PBX Count:	2	Total	0	0	0	0	0	0	0	0	0	10	0	ERLs Count:	6	Date	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	2015-11-14	0000-0	Maximum Endpoints Allowed:	100													Endpoints Count:	9													Provisioned Endpoints Count:	9													Billable Endpoints:	9													Active Alarms Count:	16													Switches Count:	1												
Provisioning	Auto Discovery	System Status	Configuration	Test Mode	Desk Alert	Help																																																																																																																																																					
Status	Logs	Reports	CDRs	Alarms	Maintenance																																																																																																																																																						
General Information		Last 12 Months Endpoints Peak Reported:																																																																																																																																																									
Server Role:	Primary	January	February	March	April	May	June	July	August	September	October	November	Decen																																																																																																																																														
PBX Count:	2	Total	0	0	0	0	0	0	0	0	0	10	0																																																																																																																																														
ERLs Count:	6	Date	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	0000-00-00	2015-11-14	0000-0																																																																																																																																														
Maximum Endpoints Allowed:	100																																																																																																																																																										
Endpoints Count:	9																																																																																																																																																										
Provisioned Endpoints Count:	9																																																																																																																																																										
Billable Endpoints:	9																																																																																																																																																										
Active Alarms Count:	16																																																																																																																																																										
Switches Count:	1																																																																																																																																																										

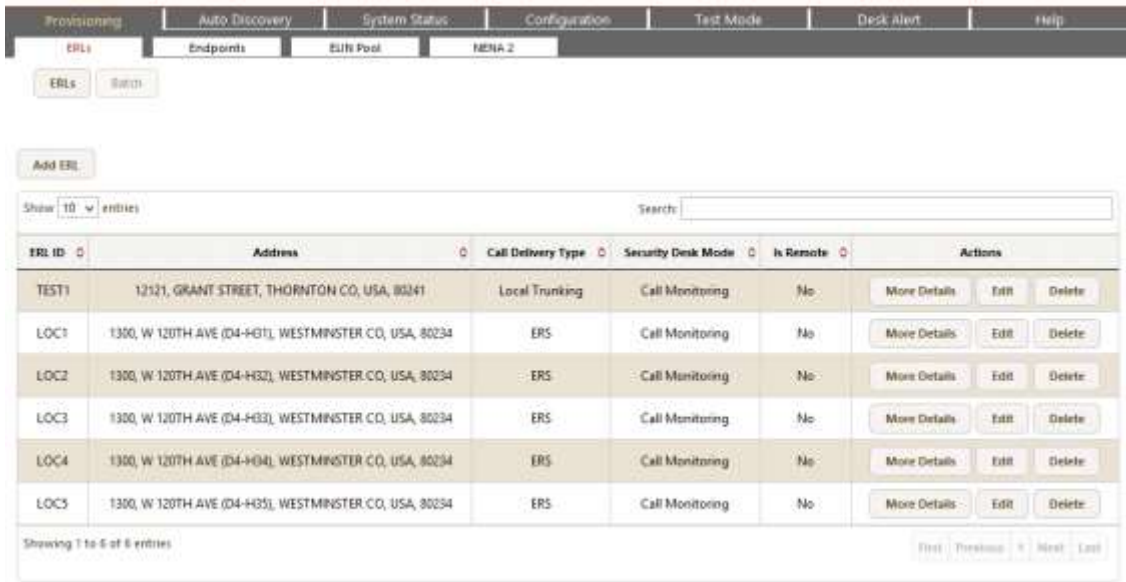
Step	Description																																										
3.	<p><b>ERS Account</b></p> <p>The ERS account defines the parameters used to connect to the Emergency Routing Service. Navigate to the <b>Configuration → Advanced → ERS Account</b> tab to configure these settings. The example below shows the settings used for the compliance test. The necessary values for each field shown for the <b>911 Account Settings</b> and the <b>ECRC List</b> are provided by 911 Enable for connection to the ERS. The ECRC list shows the phone number of the ECRC. This number is dialed through Session Manager so it contains the preceding 9 (ARS feature access code) followed by the 11-digit number. For security reasons, 911 Enable Primary IP and ECRC List number has been changed.</p>  <p>The screenshot displays the EMERGENCY GATEWAY web interface. At the top, there is a header with the 9-1-1 ENABLE logo, system information (Hostnames: EGW1.lanaya.com, Server Role: PRIMARY, Server Time: Nov 25, 2015 01:48:11 PM EST), and a user greeting (Welcome, Root User) with a last login time (Nov 25, 2015 01:28 PM) and a Log Out button. Below the header is a navigation menu with tabs: Provisioning, Auto Discovery, System Status, Configuration (selected), Test Mode, Desk Alert, and Help. Under the Configuration tab, there are sub-tabs: Dashboard Account, IP-PBX, Security Desk, Notification, Advanced (selected), Task Scheduler, and Certificates. A row of buttons includes Callback, Global, ERS Account (selected), Dial Plan, Timer Settings, Batch Settings, Redundancy, SOAP Server, NAT Traversal, and RLM. The main content area is divided into two panels. The left panel, titled '911 Account Settings', contains a table of configuration parameters. The right panel, titled 'ECRC List', shows a table with one entry and buttons for Edit, Delete, and Add a Number.</p> <table border="1"> <thead> <tr> <th colspan="2">911 Account Settings</th> </tr> </thead> <tbody> <tr> <td>Log Soap Calls:</td> <td>Yes</td> </tr> <tr> <td>911 Enable Primary IP:</td> <td>192.168.1.1</td> </tr> <tr> <td>911 Enable Secondary IP:</td> <td></td> </tr> <tr> <td>911 Enable Tertiary IP:</td> <td></td> </tr> <tr> <td>Network Protocol:</td> <td>TCP</td> </tr> <tr> <td>ERS Version:</td> <td>3.X</td> </tr> <tr> <td>SOAP Username:</td> <td>hungegw</td> </tr> <tr> <td>SOAP Password:</td> <td>b9KdWa</td> </tr> <tr> <td>Account ID:</td> <td>079766ED-E5E1-41B4-837A-FF790A833E91</td> </tr> <tr> <td>Token:</td> <td>BF711720-298E-4956-A259-12ED3E3CF313</td> </tr> <tr> <td>Location Determination Method:</td> <td>FROM_EXT</td> </tr> <tr> <td>Default Customer Name:</td> <td>Avaya</td> </tr> <tr> <td>SOAP Authentication Username:</td> <td>soap911</td> </tr> <tr> <td>SOAP Authentication Password:</td> <td>6c9MWp3Z+D</td> </tr> <tr> <td>SOAP Server URL:</td> <td>https://GFLabQA05.connexion.com</td> </tr> <tr> <td>CPM Unprovisioned Calls Route:</td> <td>PBX</td> </tr> <tr> <td>Proxy Enabled:</td> <td>No</td> </tr> <tr> <td>Allow CSZ Addresses:</td> <td>Yes</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">ECRC List</th> </tr> </thead> <tbody> <tr> <td>Priority 1:</td> <td>914385551212</td> </tr> </tbody> </table>	911 Account Settings		Log Soap Calls:	Yes	911 Enable Primary IP:	192.168.1.1	911 Enable Secondary IP:		911 Enable Tertiary IP:		Network Protocol:	TCP	ERS Version:	3.X	SOAP Username:	hungegw	SOAP Password:	b9KdWa	Account ID:	079766ED-E5E1-41B4-837A-FF790A833E91	Token:	BF711720-298E-4956-A259-12ED3E3CF313	Location Determination Method:	FROM_EXT	Default Customer Name:	Avaya	SOAP Authentication Username:	soap911	SOAP Authentication Password:	6c9MWp3Z+D	SOAP Server URL:	https://GFLabQA05.connexion.com	CPM Unprovisioned Calls Route:	PBX	Proxy Enabled:	No	Allow CSZ Addresses:	Yes	ECRC List		Priority 1:	914385551212
911 Account Settings																																											
Log Soap Calls:	Yes																																										
911 Enable Primary IP:	192.168.1.1																																										
911 Enable Secondary IP:																																											
911 Enable Tertiary IP:																																											
Network Protocol:	TCP																																										
ERS Version:	3.X																																										
SOAP Username:	hungegw																																										
SOAP Password:	b9KdWa																																										
Account ID:	079766ED-E5E1-41B4-837A-FF790A833E91																																										
Token:	BF711720-298E-4956-A259-12ED3E3CF313																																										
Location Determination Method:	FROM_EXT																																										
Default Customer Name:	Avaya																																										
SOAP Authentication Username:	soap911																																										
SOAP Authentication Password:	6c9MWp3Z+D																																										
SOAP Server URL:	https://GFLabQA05.connexion.com																																										
CPM Unprovisioned Calls Route:	PBX																																										
Proxy Enabled:	No																																										
Allow CSZ Addresses:	Yes																																										
ECRC List																																											
Priority 1:	914385551212																																										

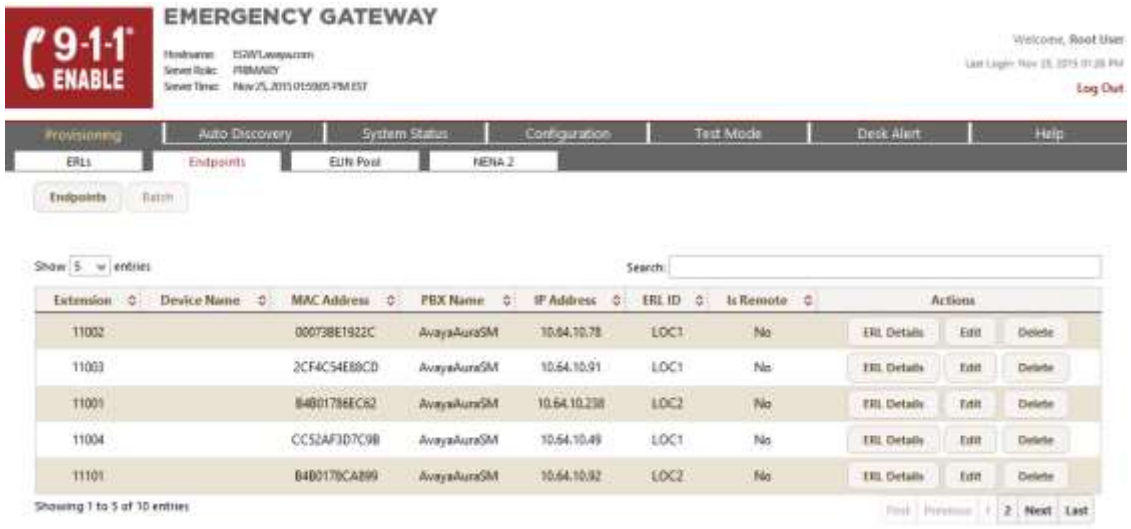
Step	Description
4.	<p><b>Extension-Bind Numbers</b></p> <p>The Extension-Bind numbers are the pool of DID numbers owned by the enterprise that the EGW can use as callback numbers for active 911 calls. Navigate to the <b>Configuration → Advanced → Callback</b> tab to configure these Extension-Bind numbers. For the compliance test, a single number was used in the Extension-Bind Numbers list. To add a number to the list, click the <b>Add a number</b> button. Enter the number in the subsequent window (not shown). Each number is represented by 10-digits. For security reasons, the full PSTN number is not shown.</p>  <p>The screenshot shows the 'EMERGENCY GATEWAY' web interface. At the top, there's a header with a '9-1-1 ENABLE' logo, system information (Hostname: EGW1lawys.com, Server Role: PRIMARY, Server Time: Nov 25, 2015 01:50:23 PM EST), and a user greeting (Welcome, Root User, Last Login: Nov 25, 2015 01:28 PM). Below the header is a navigation bar with tabs: Provisioning, Auto Discovery, System Status, Configuration, Test Mode, Desk Alert, and Help. Under the Configuration tab, there are sub-tabs: Dashboard Account, IP-PBX, Security Desk, Notification, Advanced (selected), Task Scheduler, and Certificates. Below these are buttons for various settings: Callback, Global, ERS Account, Dial Plan, Timer Settings, Batch Settings, Redundancy, SOAP Server, NAT Traversal, and RLM. The main content area is divided into two panels. The left panel, titled 'Extension-Bind Numbers', shows a list with one entry '7205551212' and buttons for 'Edit' and 'Delete'. There is an 'Add a Number' button at the bottom. The right panel, titled 'Callback Settings', shows fields for 'Extension-Bind Duration' (60), 'Use 10 Digit for Callbacks' (Yes), and 'Except for numbers in this RegEx' ([Not Specified]). There is an 'Edit' button at the bottom. Below this is a 'Callback Digit Mapping List' section showing 'No Digit Map Configured' and an 'Add a Digit Map' button.</p>
5.	<p><b>IP-PBX</b></p> <p><b>Steps 5 – 7</b> define the parameters needed to connect to Session Manager via a SIP trunk on the private side of the EGW. Navigate to <b>Configuration → IP-PBX</b> to configure these settings. First, an IP-PBX is defined by clicking the <b>Add a new IP-PBX</b> button. The example below shows the IP-PBX created for the compliance test. Click the IP-PBX name to view the details.</p>  <p>The screenshot shows the 'IP-PBX' configuration page in the EGW web interface. It has the same navigation bar as the previous screenshot, with the 'IP-PBX' sub-tab selected under the 'Configuration' tab. Below the navigation bar are buttons for 'IP-PBX' and 'IP-PBX Groups'. The main content area is titled 'IP-PBX List' and features an 'Add a new IP-PBX' button. Below the button is a table listing two IP-PBX entries: 'AvayaAuraCM' and 'AvayaAuraSM', each with a small icon to its left.</p>

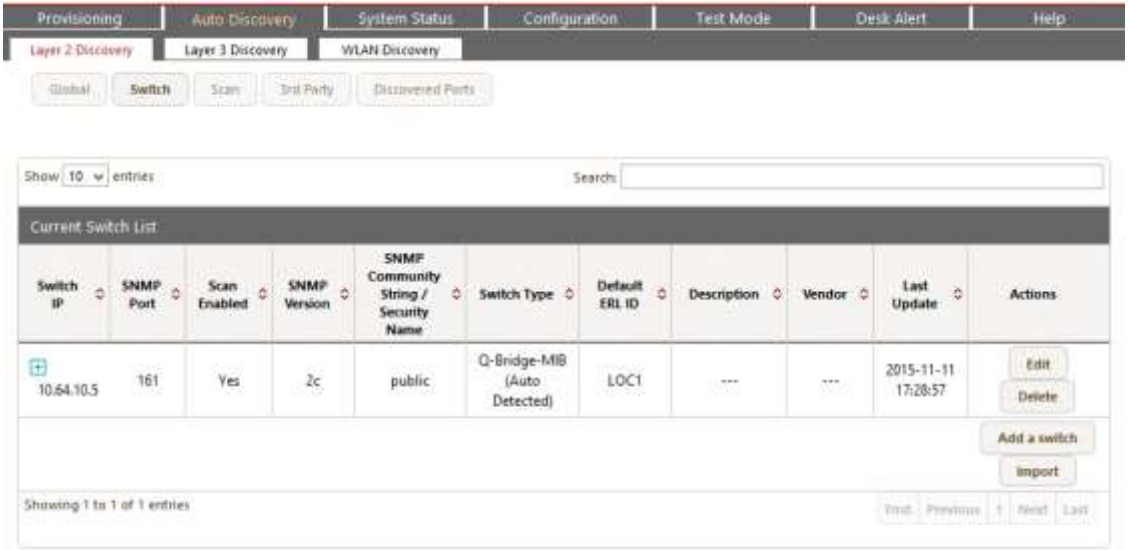



Step	Description
6.	<p><b>IP-PBX – Continued</b></p> <p>The IP-PBX was created with the following parameters. Use default values for all other fields.</p> <ul style="list-style-type: none"> <li>Set the <b>IP-PBX Name</b> to a descriptive name.</li> <li>Set the <b>IP-PBX Type</b> to <i>Avaya</i>.</li> <li>Set the <b>IP-PBX Version</b> to <i>V6</i>.</li> <li>Set the <b>Protocol</b> to <i>SIP/TCP</i>.</li> </ul> <p>The EGW automatically assigned the IP-PBX ID number shown below. This value is needed for the configuration of the Avaya H.323 and SIP Telephone 46xxsettings file (<b>Section 6, Step 1</b>) and the ESL installation (<b>Section 7, Step 5</b>).</p> <div data-bbox="318 625 1425 1428">  <p>The left screenshot shows the 'IP-PBX List' with two entries: 'AvayaAuraCM' and 'AvayaAuraSM'. The right screenshot shows the 'Add a new IP-PBX' configuration form. The form includes fields for 'IP-PBX Name' (AvayaAuraSM), 'IP-PBX Type' (Avaya Aura), 'IP-PBX Version' (V6), and 'Protocol' (SIP/TCP). Below these are 'Advanced' settings including 'Endpoint ID Field' (CONTACT), 'Domain(s)', 'DNIS Prefix', 'Local Gateway Prefix', 'Local Gateway Suffix', 'Redirected DNIS (RDNIS)', 'Callback Use VIA Header', 'Callback Use Original PAE', 'Use Home Numbering Plan', and 'IP-PBX Preferences' (Use Default Settings). Buttons for 'Add', 'Delete', 'Back', and 'Save' are also visible.</p> </div>

Step	Description
7.	<p><b>IP-PBX – Continued</b></p> <p>The IP-PBX created in the previous step can be comprised of multiple servers. To view the list of servers, click the + icon next to the IP-PBX name. The example below shows the server list for the IP-PBX named <i>AvayaAuraSM</i> created for the compliance test. The list contains a single server named <i>SMServer</i>. Click the server name to see the details.</p> <p>A server can be added by clicking the <b>Add PBX Server</b> button. Enter a descriptive name for the <b>Server Name</b>. Set the <b>Signaling IP Address/FQDN</b> to the IP address of the Avaya Server terminating the SIP trunk at the far-end. Use default values for all other fields.</p> <div data-bbox="318 594 1425 898">  <p>The screenshot displays two parts of the user interface. On the left, the 'IP-PBX List' shows three entries: 'AvayaAuraCM', 'AvayaAuraSM', and 'SMServer'. The 'AvayaAuraSM' entry is selected, and a '+ Add PBX Server' button is visible. On the right, the 'IP-PBX Server' details for 'SMServer' are shown. The fields are: IP-PBX Server ID: 3, IP-PBX Name: AvayaAuraSM, Server Name: SMServer, Signaling IP Address/FQDN: 10.64.110.13, Callback Port: 5060, Connection Timeout: 30, and Monitoring Enabled: Yes.</p> </div>

Step	Description
8.	<p><b>Emergency Response Locations (ERLs)</b></p> <p>The ERL is a location identifier that is associated with a physical address. This association is contained in a batch file uploaded to the EGW. To perform this upload, navigate to the <b>Provisioning → ERLs</b> tab. Enter the file name in the <b>Batch File</b> field and click the <b>Upload</b> button. At the bottom of the screen, <b>Status</b> and <b>Actions</b> columns will appear associated with the batch file. The following actions are necessary to complete the upload but are not all shown in the screen below. Next, click <b>Validate</b> under <b>Actions</b>. Once the file is validated, click <b>Batch Process</b> which will appear under <b>Actions</b>. Once this completes, the <b>Status</b> will change to <b>Finished</b>. An example of an ERL batch file is shown in <b>Step 9</b>.</p>  <p>The screenshot displays the 'ERLs' tab in a web application. At the top, there are navigation tabs: Provisioning, Auto Discovery, System Status, Configuration, Test Mode, Desk Alert, and Help. Under 'Provisioning', there are sub-tabs: ERLs, Endpoints, ESR Pool, and NENA 2. Below these, there are buttons for 'ERLs' and 'Batch'. A table titled 'Add ERL' is shown with a search bar and a dropdown for 'Show 10 entries'. The table has columns: ERL ID, Address, Call Delivery Type, Security Desk Mode, Is Remote, and Actions. The table contains six rows of data, including TEST1 and LOC1 through LOC5. Each row has three buttons in the Actions column: More Details, Edit, and Delete. At the bottom of the table, it says 'Showing 1 to 6 of 6 entries' and there are navigation buttons: First, Previous, Next, Last.</p>

Step	Description
9.	<p><b>Provisioned Endpoints</b></p> <p>All endpoints that can not be auto-discovered, should be manually provisioned so that each extension that is not auto-discovered is associated with an ERL. This association is contained in a batch file uploaded to the EGW. To perform this upload, navigate to the <b>Provisioning → Endpoints</b> tab. Enter the file name in the <b>Batch File</b> field and click the <b>Upload</b> button. At the bottom of the screen, <b>Status</b> and <b>Actions</b> columns will appear associated with the batch file. The following actions are necessary to complete the upload but are not all shown in the screen below. Next, click <b>Validate</b> under <b>Actions</b>. Once the file is validated, click <b>Batch Process</b> which will appear under <b>Actions</b>. Once this completes, the <b>Status</b> will change to <b>Finished</b>.</p> 

Step	Description
10.	<p><b>Layer 2 Discovery</b></p> <p>Each enterprise layer 2 switch that has Avaya H.323 or SIP telephones connected to it must be configured on the EGW so that it can be queried as part of layer 2 discovery. Navigate to the <b>Auto Discovery → Layer 2 Discovery → Switch</b> tab to display the list of layer 2 switches. The example below shows the list used for the compliance test. Click the <b>Add a switch</b> button to enter the switch parameters. Enter the management IP address of the switch in the <b>Switch IP</b> field and enter the appropriate string in the <b>SNMP Community String</b> field. Enter the ERL where the switch resides in the <b>Default ERL ID</b> field. Default values may be used for all other fields.</p>  <p>The screenshot displays the 'Layer 2 Discovery' interface. At the top, there are tabs for 'Provisioning', 'Auto Discovery', 'System Status', 'Configuration', 'Test Mode', 'Desk Alert', and 'Help'. Under 'Auto Discovery', there are sub-tabs for 'Layer 2 Discovery', 'Layer 3 Discovery', and 'WLAN Discovery'. The 'Layer 2 Discovery' tab is active, showing a 'Switch' sub-tab. Below the tabs, there are buttons for 'Global', 'Switch', 'Scan', '3rd Party', and 'Discovered Ports'. A search bar is present with the text 'Show 10 entries' and a search input field. The main area is titled 'Current Switch List' and contains a table with the following columns: Switch IP, SNMP Port, Scan Enabled, SNMP Version, SNMP Community String / Security Name, Switch Type, Default ERL ID, Description, Vendor, Last Update, and Actions. The table contains one entry with the following values: Switch IP: 10.64.10.5, SNMP Port: 161, Scan Enabled: Yes, SNMP Version: 2c, SNMP Community String / Security Name: public, Switch Type: Q-Bridge-MIB (Auto Detected), Default ERL ID: LOC1, Description: ---, Vendor: ---, Last Update: 2015-11-11 17:28:57. The Actions column has 'Edit' and 'Delete' buttons. Below the table, there are buttons for 'Add a switch' and 'Import'. At the bottom, it says 'Showing 1 to 1 of 1 entries' and has pagination controls: 'First', 'Previous', '1', 'Next', 'Last'.</p>

Step	Description
11.	<p><b>Security Desk</b></p> <p>Emergency calls may be routed to a Security Desk extension as well as being sent to the Emergency Routing Service. Navigate to the <b>Configuration → Security Desk → Groups</b> tab to create the Security Desk List. To create a security desk, click <b>Add a Security Desk Group</b>. The example below shows the Security Desk created for the compliance test. Click the <b>Edit</b> button to view the details.</p> 

## 8. Verification Steps

The following steps may be used to verify the configuration:

- On Avaya Aura® System Manager, navigate to **Home → Session Manager → System Status → SIP Entity Monitoring**.
  - Value in the **Conn. Status** column, should be **Up**. This verifies that the SIP connectivity between Avaya Aura® Session Manager and 911 Enable EGW is established successfully.

5 Items   Refresh										Filter: Enable	
	SIP Entity Name	1 ▲	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status		
<input type="radio"/>	<a href="#">acm</a>		10.64.110.10	5061	TLS	FALSE	UP	200 OK	UP		
<input type="radio"/>	<a href="#">asm-remote</a>		10.64.10.62	5060	TCP	FALSE	UP	200 OK	UP		
<input type="radio"/>	<a href="#">egw-1</a>		10.64.110.200	5060	TCP	FALSE	UP	200 OK	UP		
<input type="radio"/>	<a href="#">egw-2</a>		10.64.110.201	5060	TCP	FALSE	UP	200 OK	UP		

- On the EGW, verify the endpoints. Navigate to the **Provisioning** → **Endpoints** tab, verify that all endpoints are displayed.

Provisioning	Auto Discovery	System Status	Configuration	Test Mode	Desk Alert	Help
ERLs	Endpoints	ELIN Pool	NENA 2			
Endpoints	Batch					

Show 5 entries
Search:

Extension	Device Name	MAC Address	PBX Name	IP Address	ERL ID	Is Remote	Actions		
11101		B4B0178CA899	AvayaAuraSM	10.64.10.92	LOC2	No	ERL Details	Edit	Delete
11002		00073BE1922C	AvayaAuraSM	10.64.10.78	LOC1	No	ERL Details	Edit	Delete
11004		CC52AF3D7C9B	AvayaAuraSM	10.64.10.49	LOC1	No	ERL Details	Edit	Delete
11001		B4B01786EC62	AvayaAuraSM	10.64.10.238	LOC2	No	ERL Details	Edit	Delete
11003		2CF4C54E88CD	AvayaAuraSM	10.64.10.91	LOC1	No	ERL Details	Edit	Delete

Showing 1 to 5 of 10 entries
First Previous 1 2 Next Last



- Verify that 911 calls can be placed from different endpoints types from different locations. Verify from the EGW Call Detail Records (CDR), that the correct location and callback number is being passed to 911 Enable. Navigate to the **System Status → CDRs** tab to display this information. The example below shows two emergency 911 calls as represented by the value **ERS** in the **Call Destination** field. The example also shows three callback calls which show the local extension being called back in the **Call Destination** field. Each of the 911 calls shows the correct location and callback information for that endpoint.

Provisioning	Auto Discovery	System Status	Configuration	Test Mode	Desk Alert	Help
Status	Logs	Reports	CDRs	Alarms	Maintenance	

Search CDRs

Search from:  to:  Search:  

Download Call Detail Records

Select by Month:

Call Detail Records <input type="checkbox"/> Show expired callbacks								
Start Time	Duration (s)	Endpoint Caller ID	ERL ID	Callback Number	Call Destination	Wave File	Call Status	URL Data
Nov 13, 2015 05:25 PM	4	11004	LOC1	7209772872	ERS	<a href="#">Download</a>	ANSWER	
Nov 13, 2015 05:24 PM	4	11004	LOC1	7209772872	ERS	<a href="#">Download</a>	CANCEL	
Nov 13, 2015 05:24 PM	4	11004	LOC1	11004	Security Desk	<a href="#">Download</a>	CANCEL	
Nov 13, 2015 05:22 PM	11	"IP Station 4" <11004>	LOC1	7209772872	ERS	<a href="#">View Peer</a>	ANSWER	
Nov 13, 2015 05:22 PM	11	"IP Station 4" <11004>	LOC1	11004	Security Desk	<a href="#">View Peer</a>	CANCEL	
Nov 13, 2015 05:21 PM	9	"IP Station 4" <11004>	LOC1	7209772872	ERS	<a href="#">View Peer</a>	CANCEL	
Nov 13, 2015 05:21 PM	9	"IP Station 4" <11004>	LOC1	11004	Security Desk	<a href="#">View Peer</a>	CANCEL	
Nov 13, 2015 05:08 PM	18	"to_PSTN" <5147452143>	No Location	"to_PSTN" <5147452143>	11002@10.64.110.10:1720	<a href="#">View Peer</a>	ANSWER	
Nov 13, 2015 05:08 PM	15	"IP Station 2" <11002>	LOC1	7209772872	ERS	<a href="#">View Peer</a>	ANSWER	
Nov 13, 2015 05:08 PM	14	"IP Station 2" <11002>	LOC1	11002	Security Desk	<a href="#">View Peer</a>	ANSWER	
<div> Pages / Rows <input type="text" value="10"/> Previous   <a href="#">Next</a> Go to page: <input type="text" value="First Page"/> <input type="button" value="Go"/> </div>								

## 9. Conclusion

Intrado / 911 Enable Emergency Gateway passed compliance testing. These Application Notes describe the procedures required to configure the connectivity between Avaya Aura® Communication Manager and the 911 Enable equipment and service as shown in **Figure 1**, along with Avaya one-X® Deskphones and Avaya one-X® Communicator.

## 10. Additional References

This section references the documentation relevant to these Application Notes. Avaya product documentation is available at <http://support.avaya.com>. Product documentation for the EGW can be obtained from 911 Enable.

- [1] Administering Avaya Aura® Communication Manager, Release 7.0, Document 03-300509, Issue 1, August 2015*
- [2] Administering Avaya Aura® Session Manager, Release 7.0, Issue 1, August 2015*
- [3] 911Enable Emergency Gateway System Guide 5.0 Nov 1<sup>st</sup>, 2015*
- [4] ESL Configuration Guide Rev. A, Rev. G, Nov 20, 2015*

---

**©2016 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ® are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).