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.

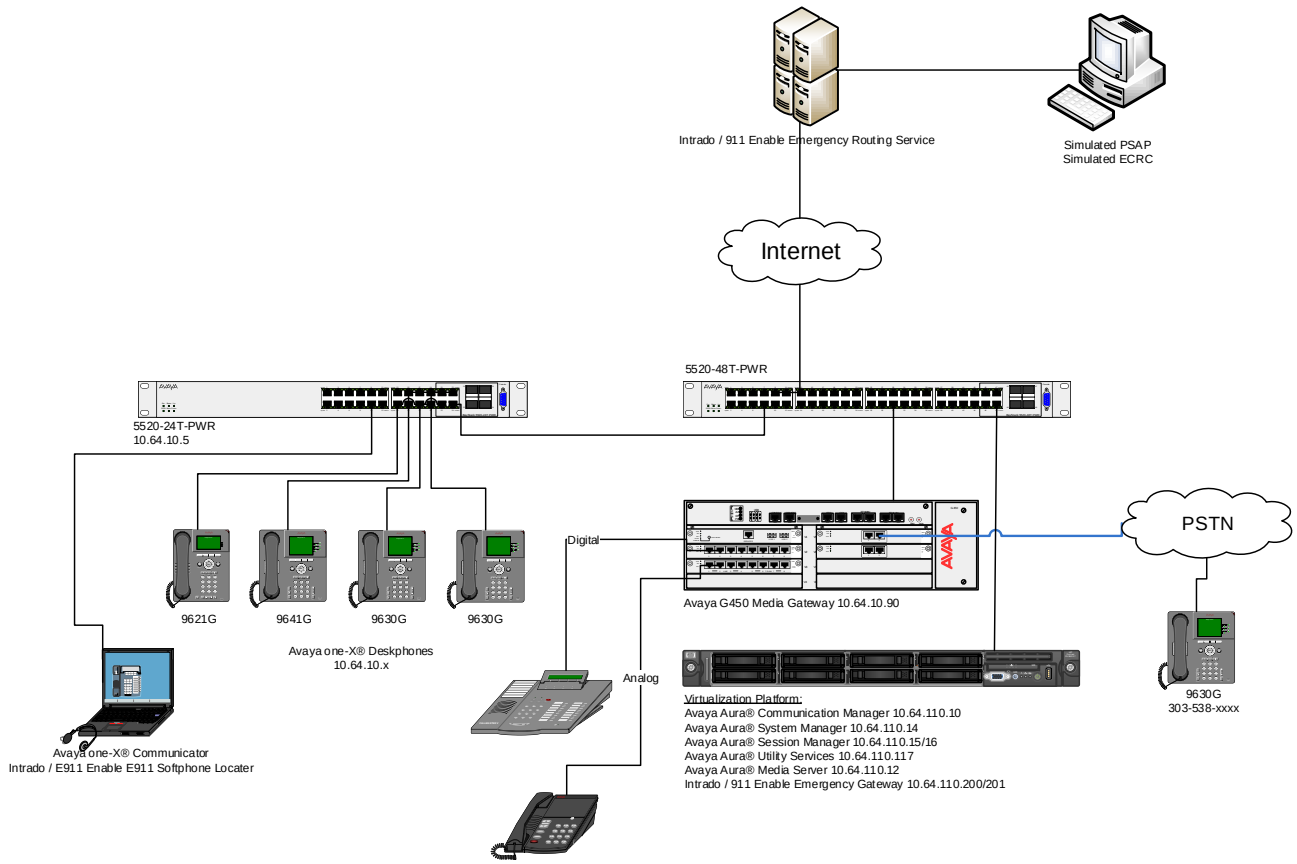
2.2. Test Results

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.

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 telephones 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

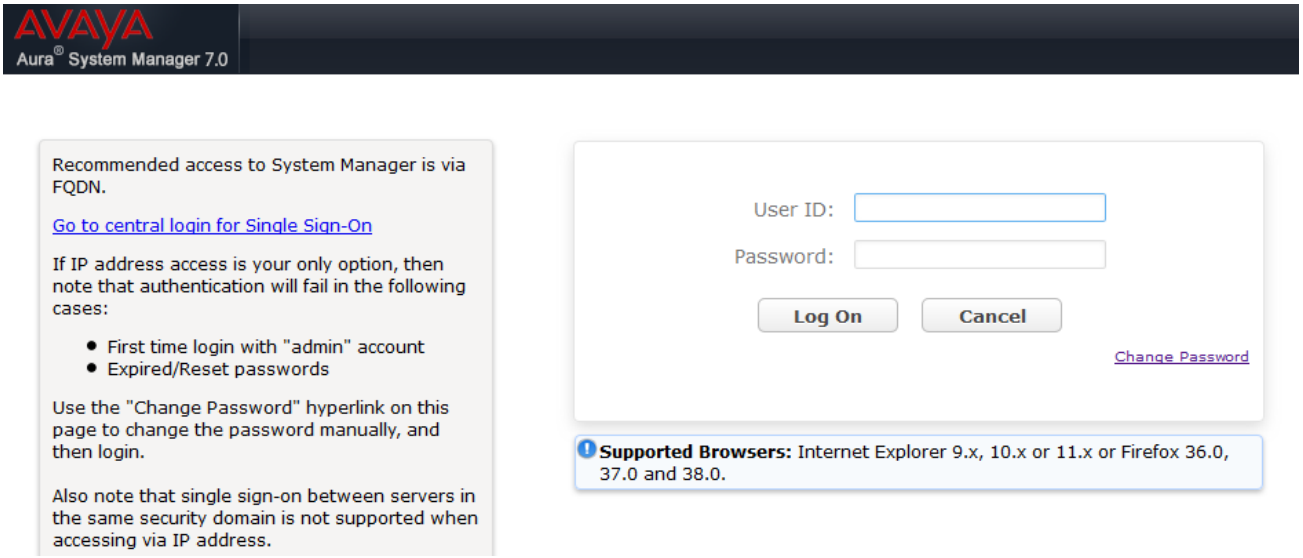
The following equipment and software/firmware were used for the sample configuration provided:

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.

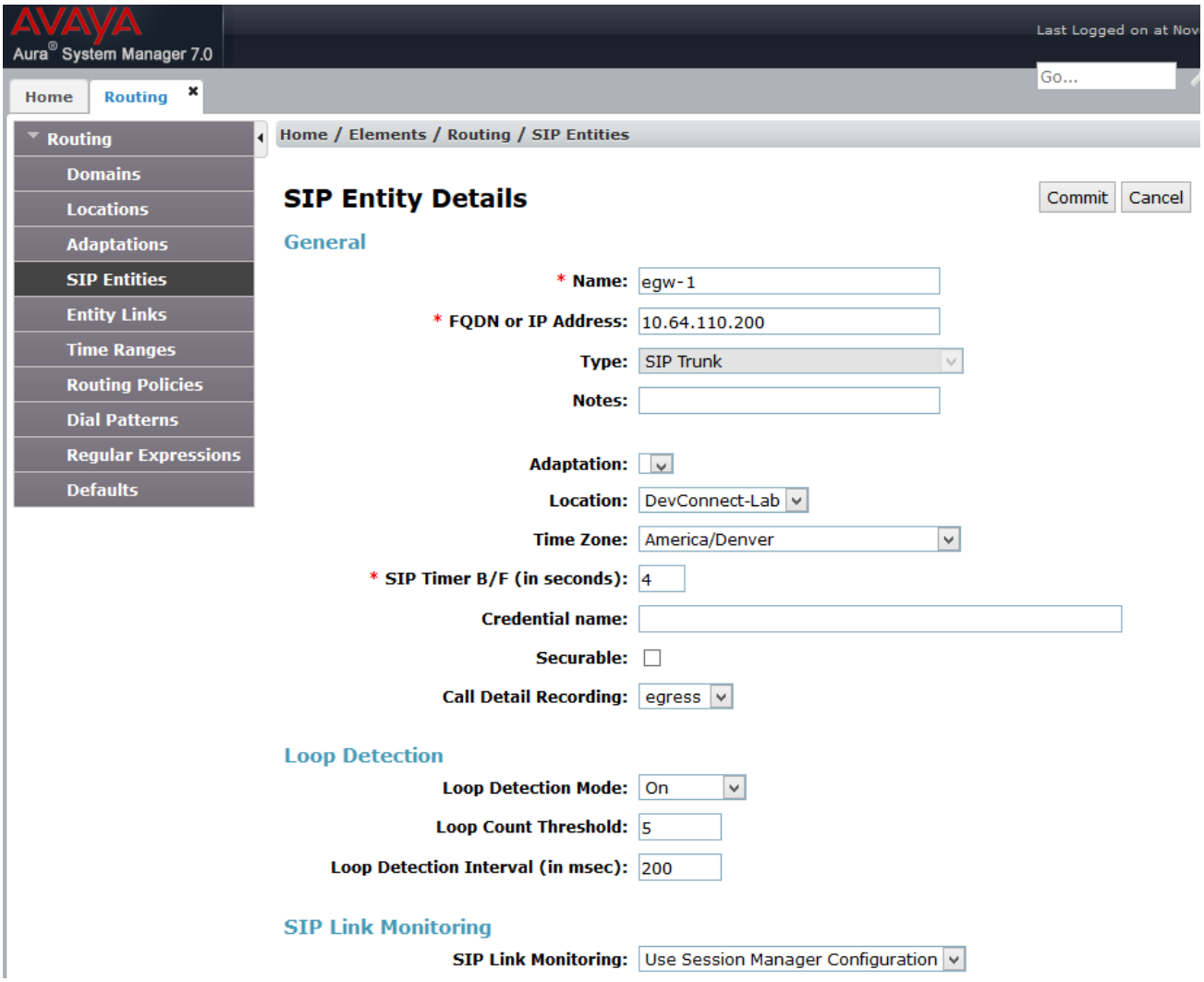


5.1. Add a SIP Entity

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.

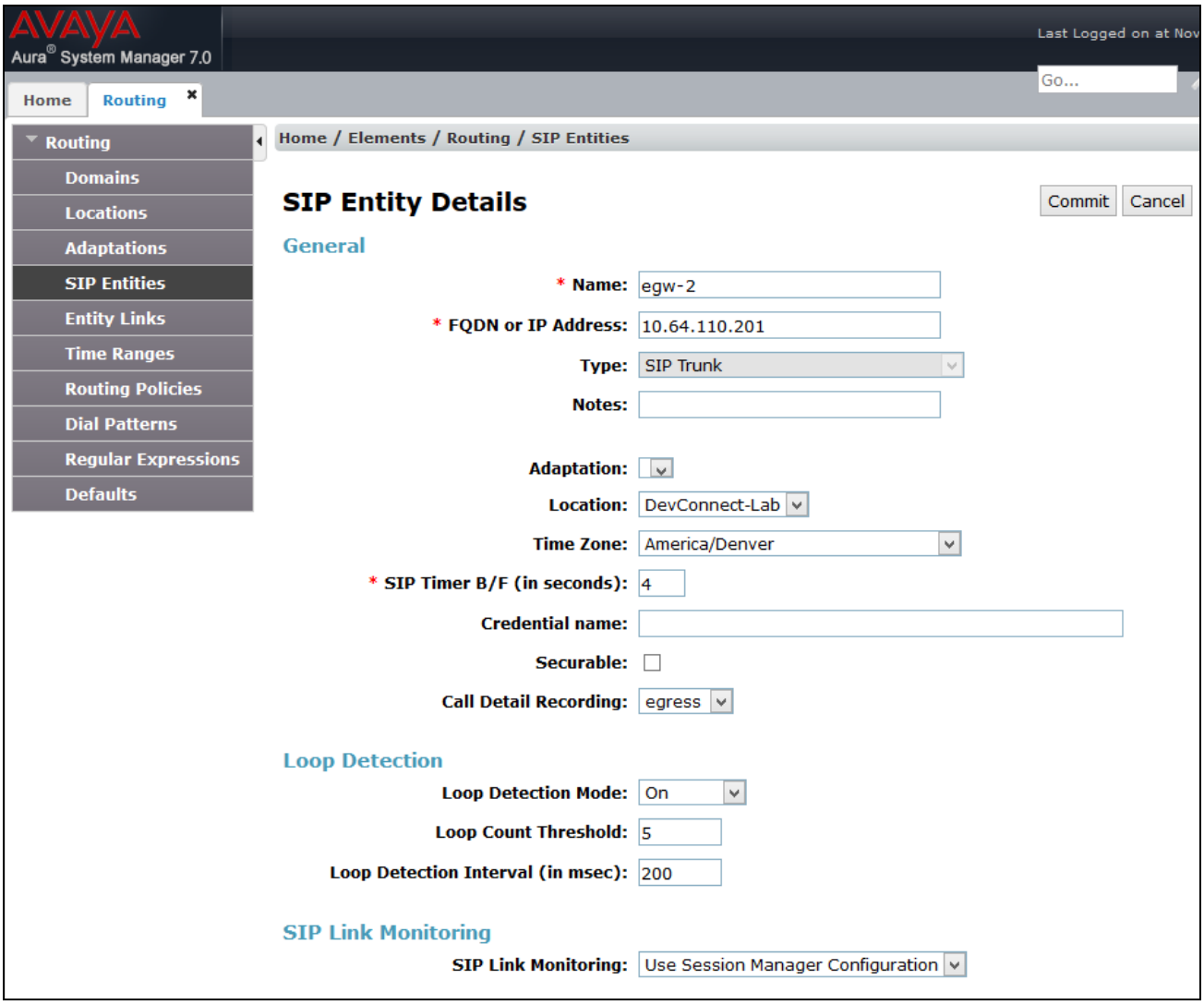
Click **Commit** to save changes.



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.

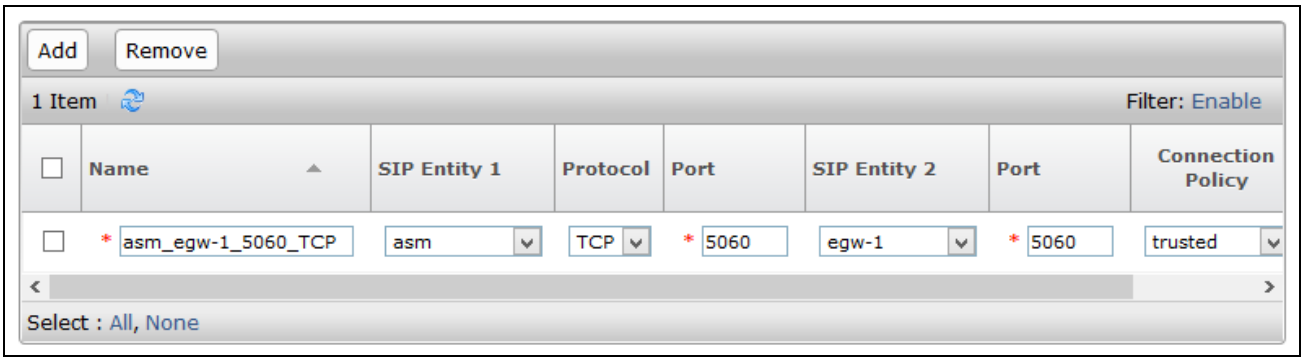


5.2. Add an Entity Link

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.



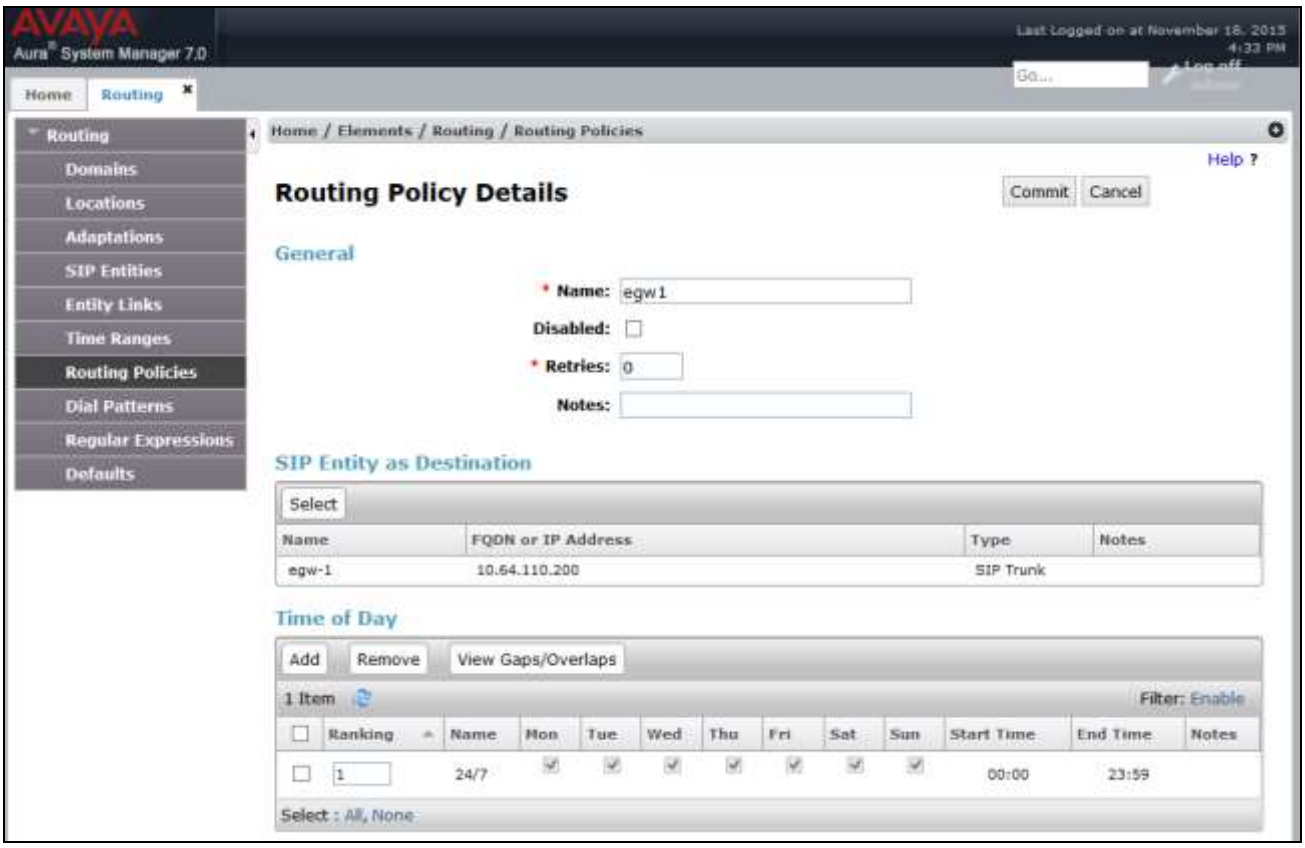
Note: Repeat this step for egw-2 SIP Entity.

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.



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

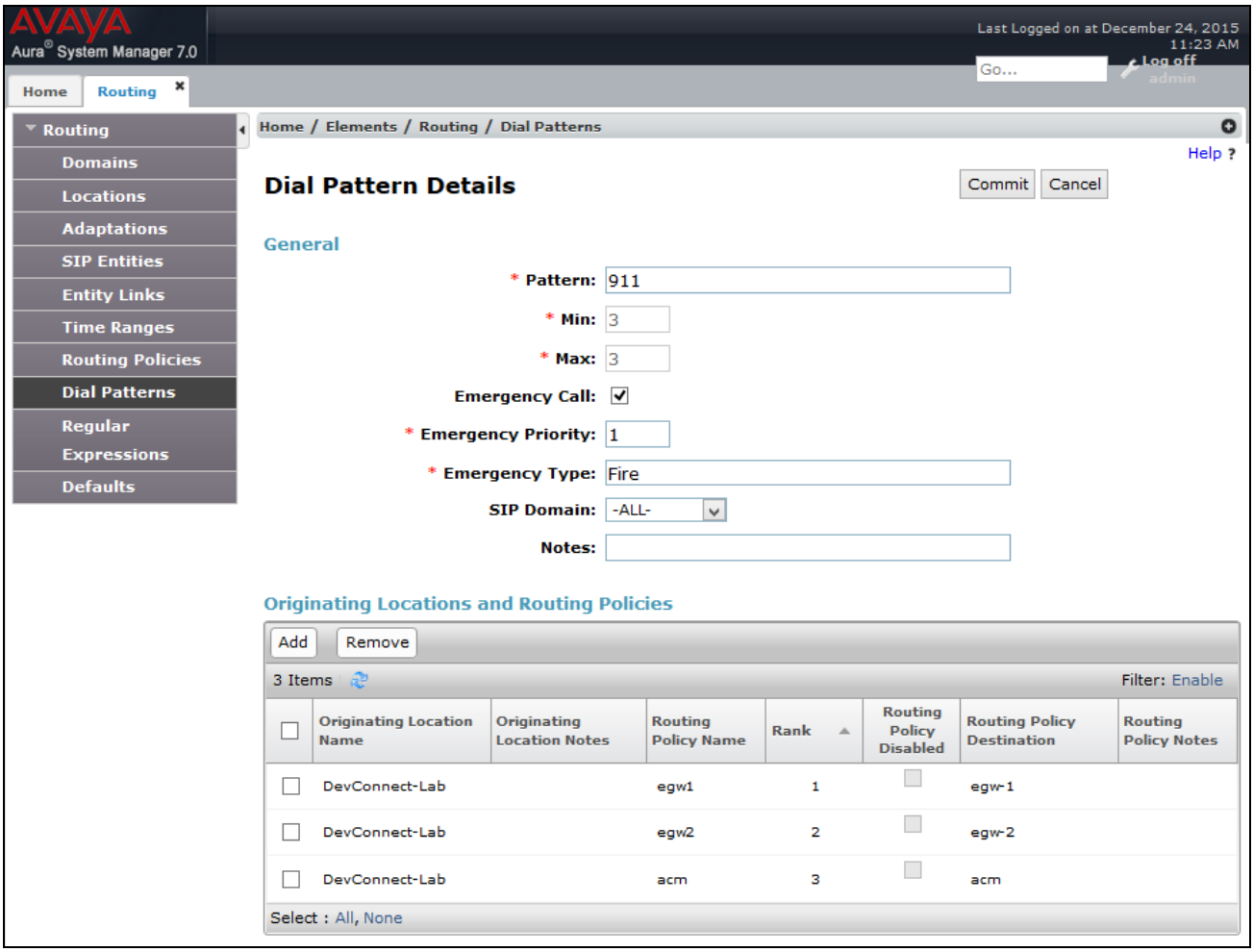
5.4. Add a Dial Pattern

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.



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.

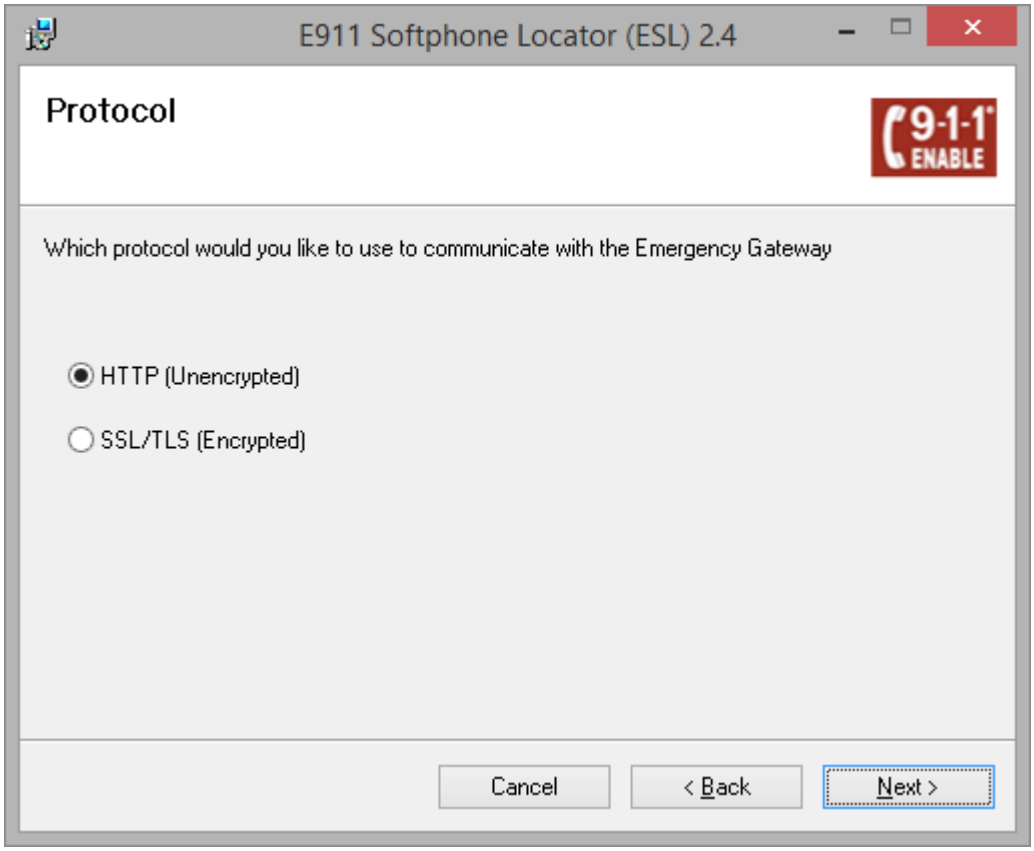
6.1. Avaya H.323 and SIP Telephone Configuration File

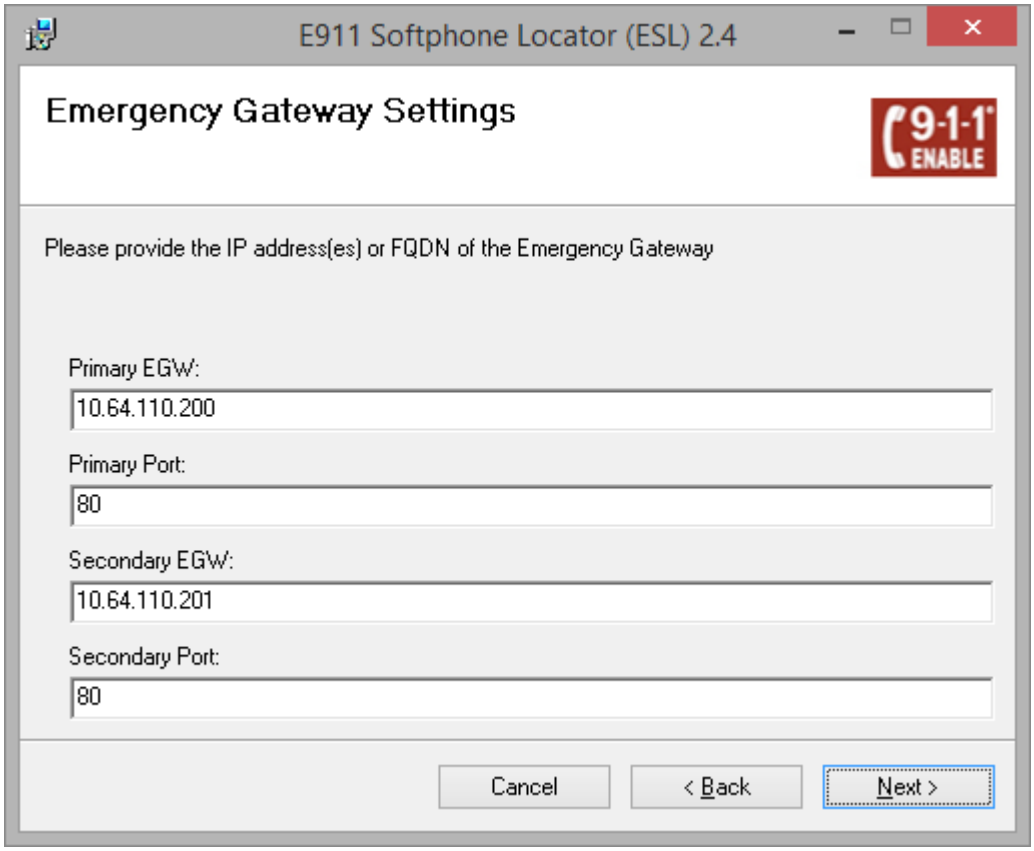
In order to support layer 3 discovery, the following lines need to be added to the 46xxsettings.txt configuration file for Avaya H.323 and SIP telephones. The two highlighted parameters in the **SUBSCRIBELIST** and **WMLHOME** URLs must be modified for a specific installation. The first parameter (***10.64.110.200***) 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**.

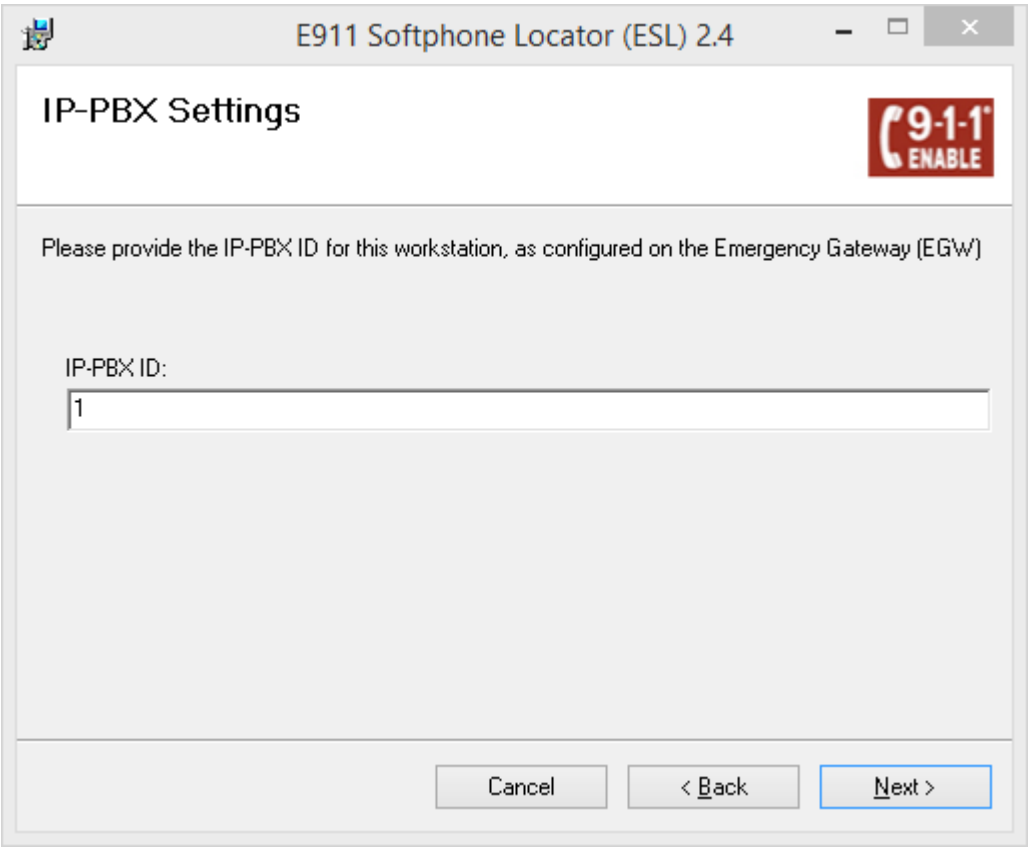
```
## 911 Enable Settings
SET TPSLIST /
SET SUBSCRIBELIST http://10.64.110.200/2/r
SET PUSHPORT 80
SET PUSHCAP 2
SET WMLHOME http://10.64.110.200/wml/2/service.html
```

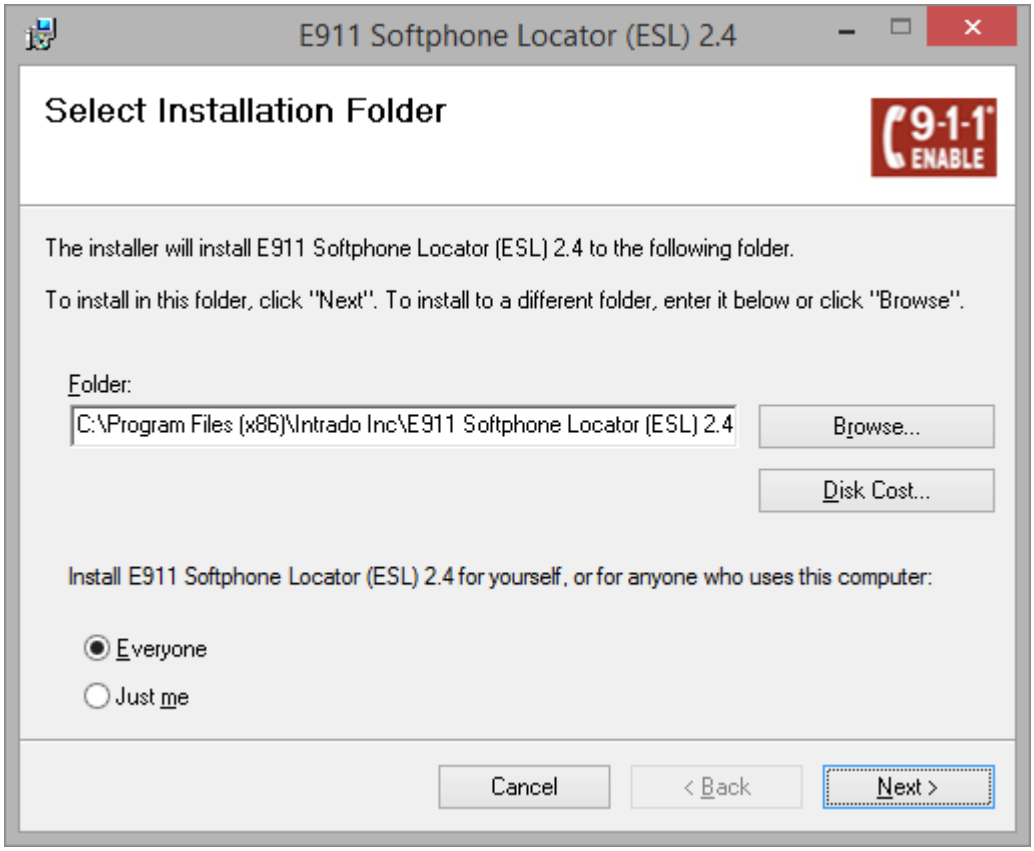
6.2. Avaya one-X® Communicator– ESL software installation

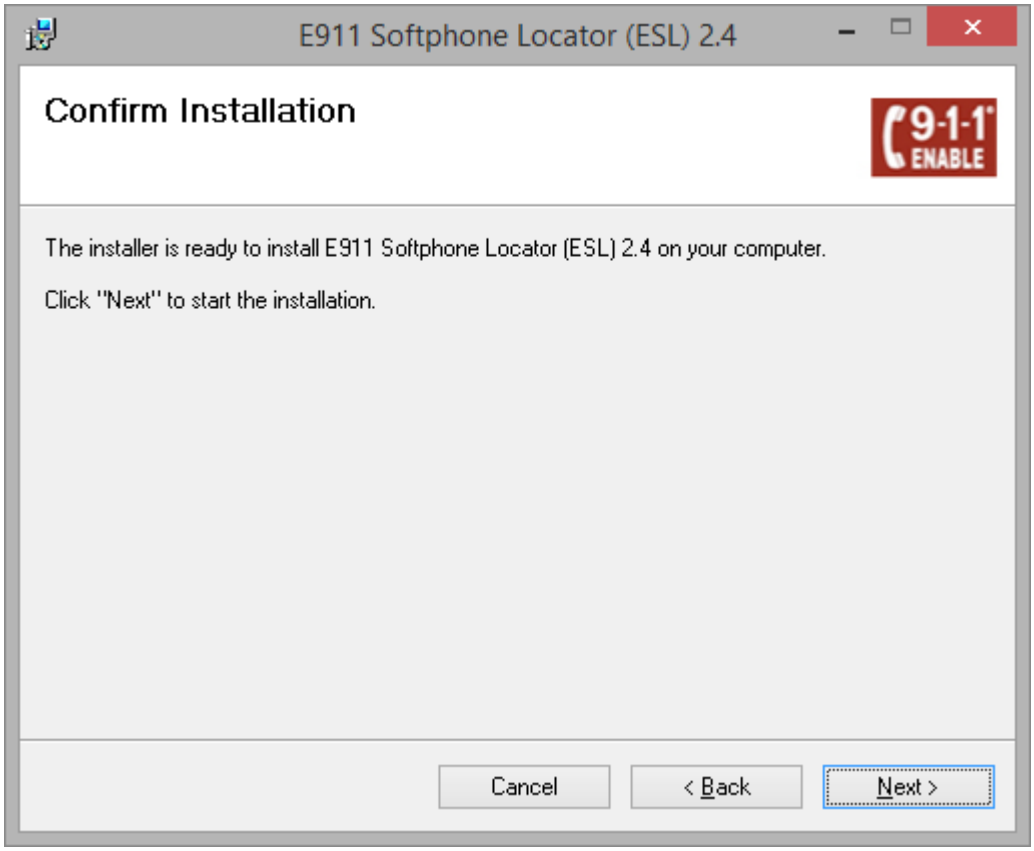
1.	On the PC running the Avaya one-X® Communicator, launch the ESL setup application. A welcome screen will appear. Click **Next** to proceed. 

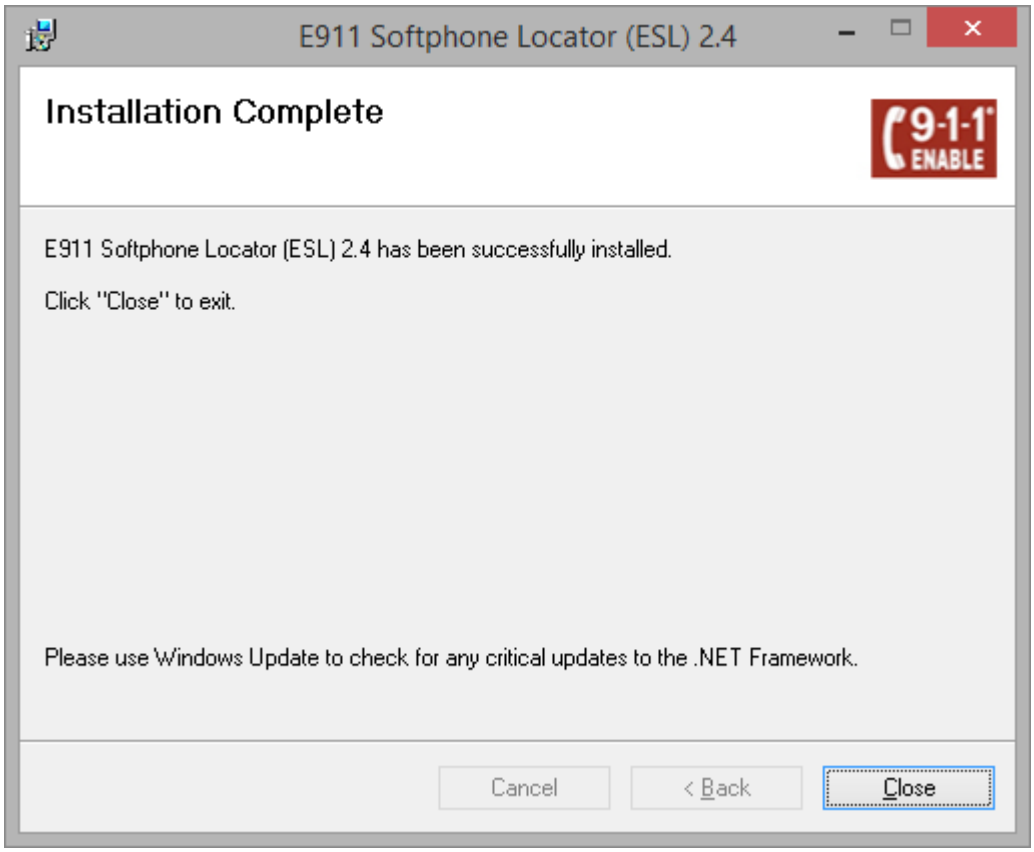
2.	**ESL Installation – Select Protocol** Select the desired protocol. HTTP was used for the compliance test. Click **Next**. 

3.	**ESL Installation – EGW Settings** Enter the IP addresses for both EGWs. Use the default port ***80*** for HTTP. Click **Next**. 

4.	**ESL Installation – IP-PBX Settings** Enter an **IP-PBX ID**. Click **Next**. 

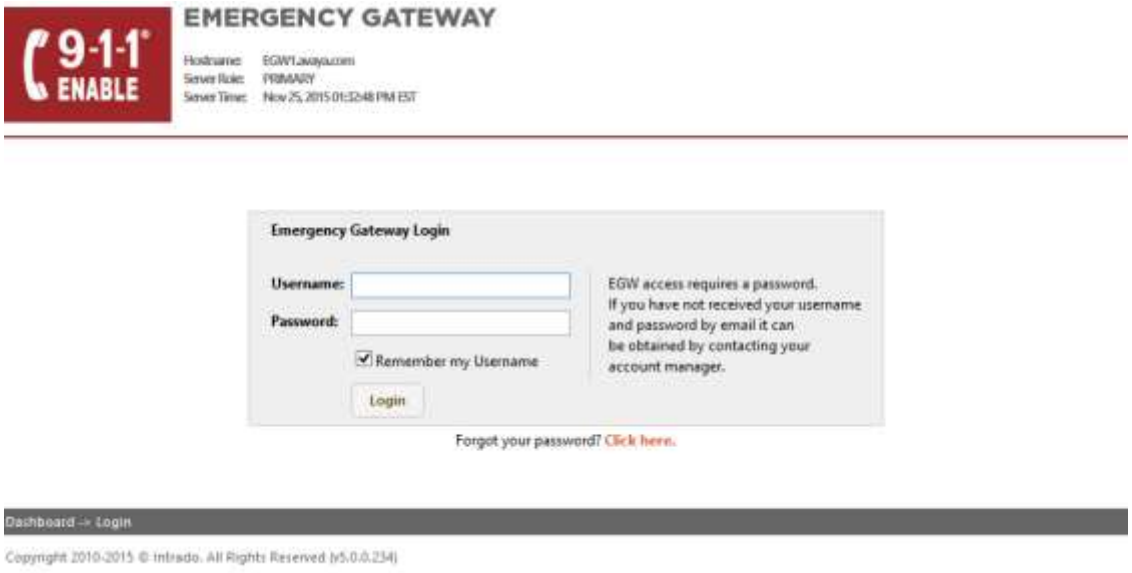
5.	**ESL Installation – Installation Folder** Enter the installation folder and who should have access to the software. Click **Next**. 

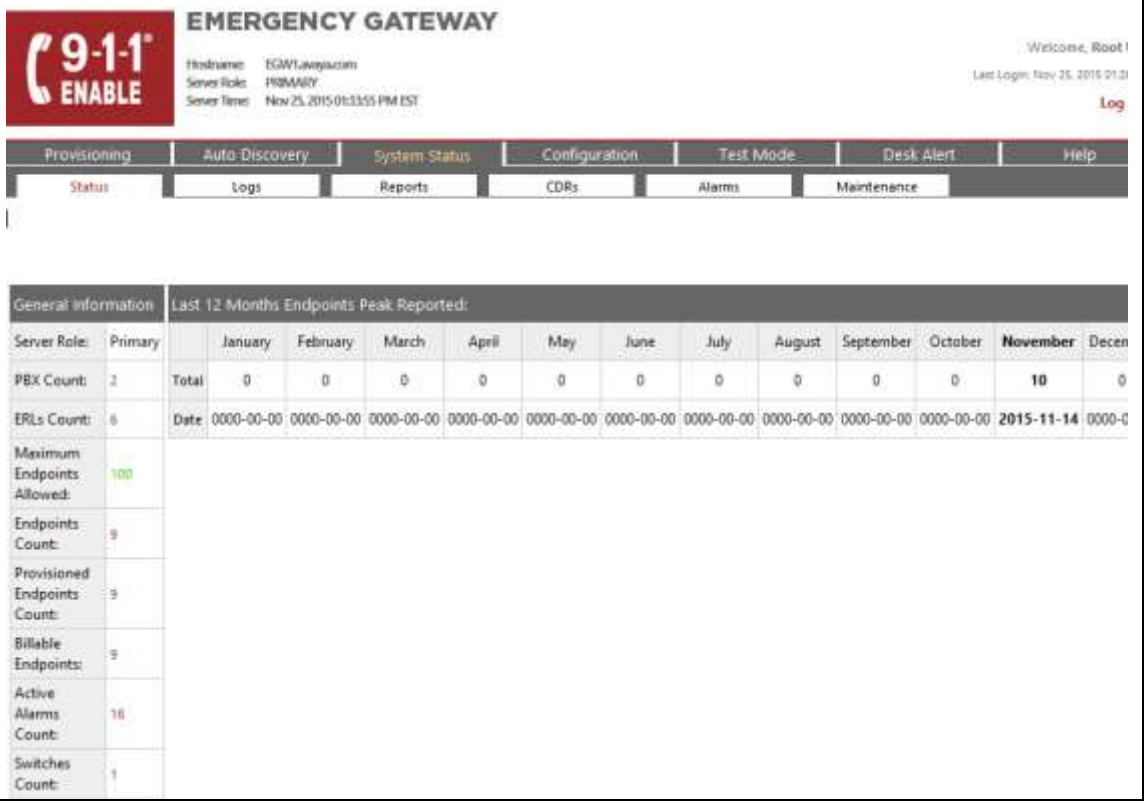
6.	**ESL Installation – Confirm** Confirm the installation by clicking **Next**. 

7.	**ESL Installation – Complete** The following screen appears when installation is complete. Click **Close** to exit the set-up application. 

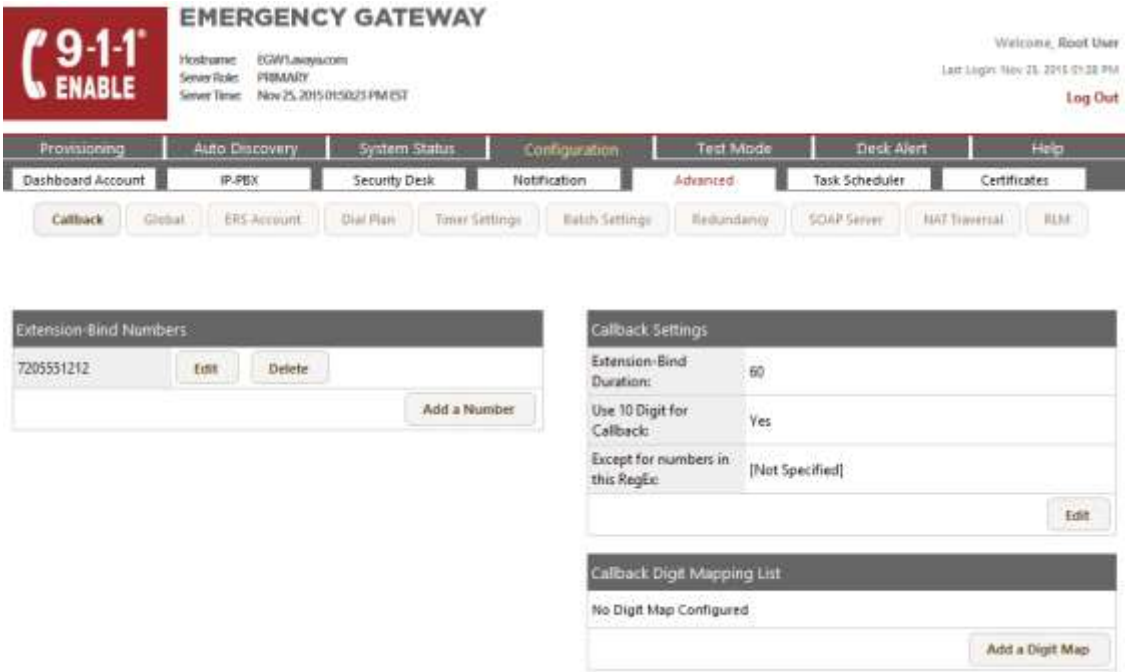
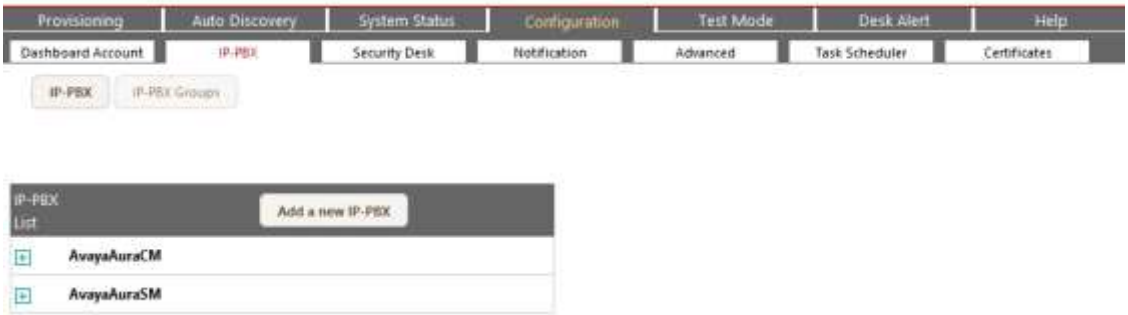
7. Configure Intrado / 911 Enable Emergency Gateway (EGW)

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.	**Login** The EGW is configured via a web browser. To access the web interface, enter http://<*ip-addr*> in the address field of the web browser, where <*ip-addr*> is the IP address of the primary EGW. Log in with the appropriate credentials. Click **Login**. 

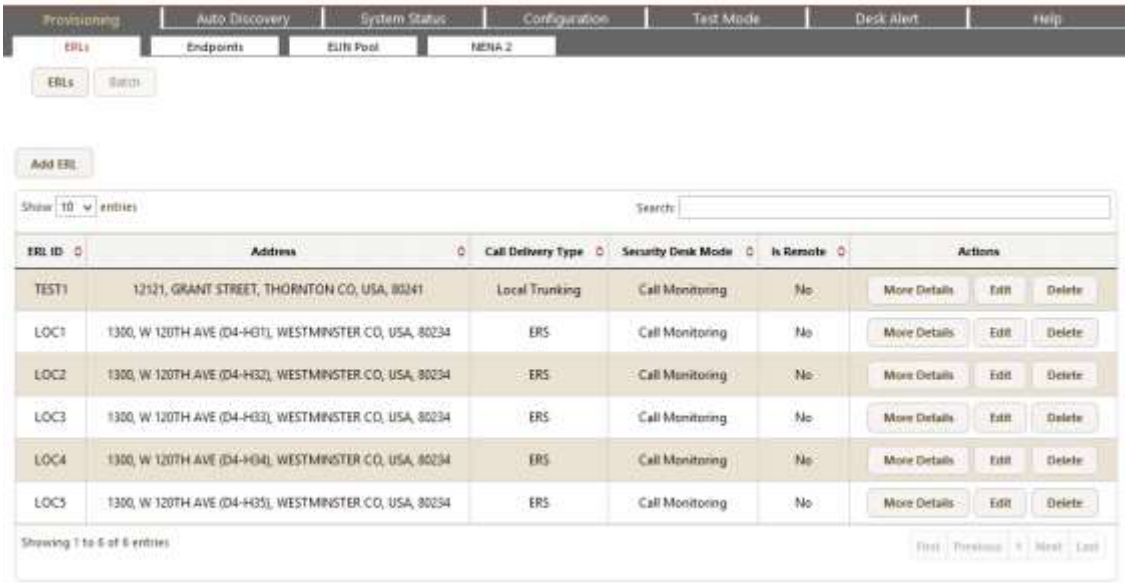
Step	Description
2.	**Main Page** The main page of the EGW will appear. 

Step	Description
3.	**ERS Account** The ERS account defines the parameters used to connect to the Emergency Routing Service. Navigate to the **Configuration → Advanced → ERS Account** 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 **911 Account Settings** and the **ECRC List** 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.  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: b9KsWa Account ID: 079766ED-E5E1-41B4-837A-FF790A833E91 Token: BF711720-29BE-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.connexon.com CPM Unprovisioned Calls Route: PBX Proxy Enabled: No Allow CSZ Addresses: Yes Edit ECRC List Priority 1: 914385551212 Edit Delete Add a Number

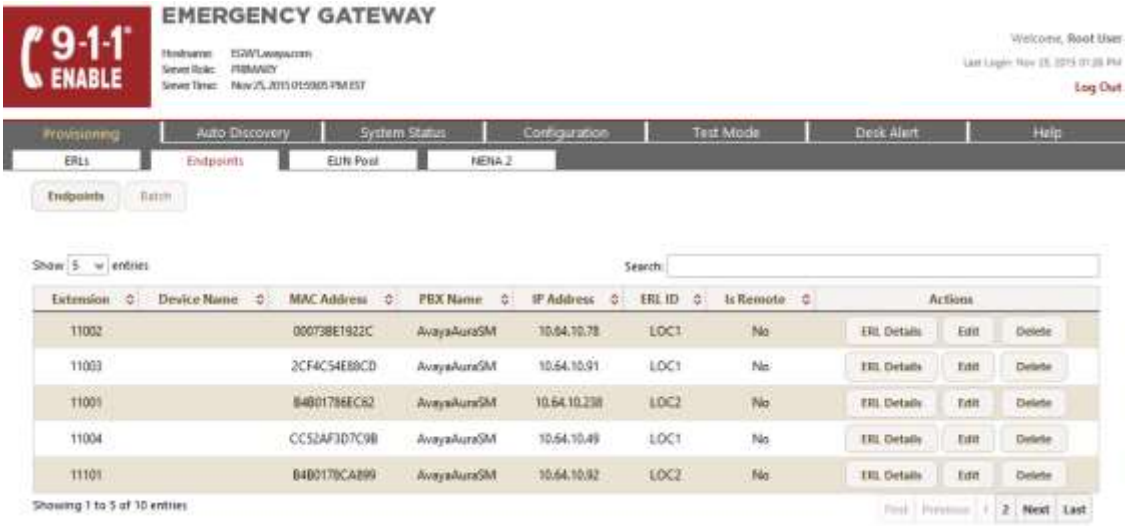
Step	Description
4.	**Extension-Bind Numbers** The Extension-Bind numbers are the pool of DID numbers owned by the enterprise that the EGW can use as callback numbers for active 911 calls. Navigate to the **Configuration → Advanced → Callback** tab to configure these Extension-Bind numbers. For the compliance test, a single number was used in the Extension-Bind Numbers list. To add a number to the list, click the **Add a number** 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. 
5.	**IP-PBX** **Steps 5 – 7** define the parameters needed to connect to Session Manager via a SIP trunk on the private side of the EGW. Navigate to **Configuration → IP-PBX** to configure these settings. First, an IP-PBX is defined by clicking the **Add a new IP-PBX** button. The example below shows the IP-PBX created for the compliance test. Click the IP-PBX name to view the details. 

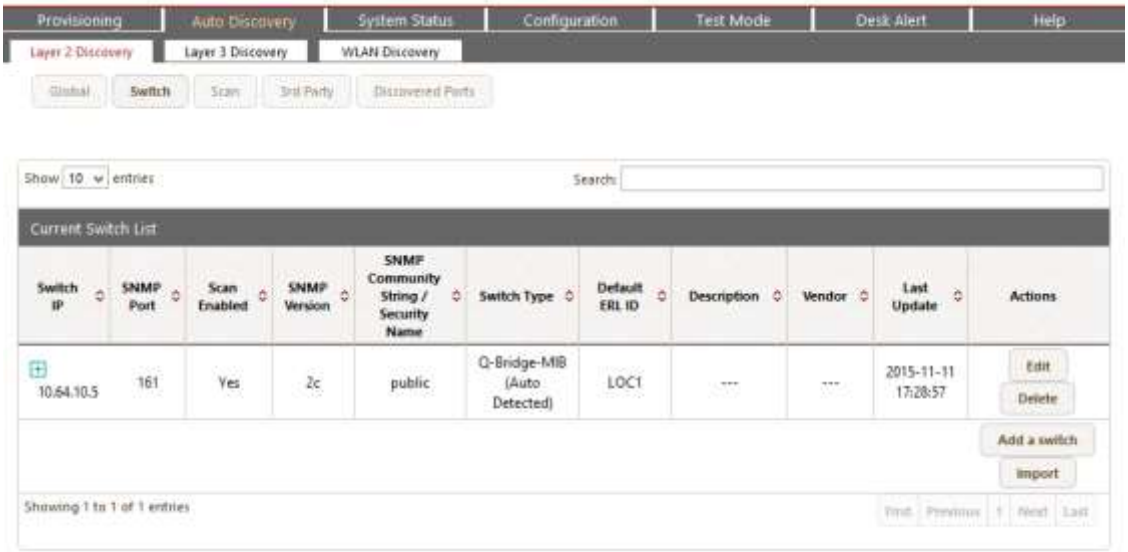
Step	Description
6.	**IP-PBX – Continued** The IP-PBX was created with the following parameters. Use default values for all other fields. ▪ Set the **IP-PBX Name** to a descriptive name. ▪ Set the **IP-PBX Type** to ***Avaya***. ▪ Set the **IP-PBX Version** to ***V6.*** ▪ Set the **Protocol** to ***SIP/TCP***. 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 (**Section 6**, **Step 1**) and the ESL installation (**Section 7**, **Step 5**).  

Step	Description
7.	**IP-PBX – Continued** 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 ***AvayaAuraSM*** created for the compliance test. The list contains a single server named ***SMServer***. Click the server name to see the details. A server can be added by clicking the **Add PBX Server** button. Enter a descriptive name for the **Server Name**. Set the **Signaling IP Address/FQDN** to the IP address of the Avaya Server terminating the SIP trunk at the far-end. Use default values for all other fields.  

Step	Description
8.	**Emergency Response Locations (ERLs)** 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 **Provisioning → ERLs** tab. Enter the file name in the **Batch File** field and click the **Upload** button. At the bottom of the screen, **Status** and **Actions 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 **Validate** under **Actions**. Once the file is validated, click **Batch Process** which will appear under **Actions**. Once this completes, the **Status** will change to **Finished**. An example of an ERL batch file is shown in **Step 9**.  Provisioning | Auto Discovery | System Status | Configuration | Test Mode | Desk Alert | Help ERLs | Endpoints | ELIN Pool | NENA 2 ERLs | Batch Add ERL Show 10 entries Search: Showing 1 to 6 of 6 entries First | Previous | 1 | Next | Last

ERL ID	Address	Call Delivery Type	Security Desk Mode	Is Remote	Actions
TEST1	12121, GRANT STREET, THORNTON CO, USA, 80241	Local Trunking	Call Monitoring	No	More Details Edit Delete
LOC1	1300, W 120TH AVE (D4-H01), WESTMINSTER CO, USA, 80234	ERS	Call Monitoring	No	More Details Edit Delete
LOC2	1300, W 120TH AVE (D4-H02), WESTMINSTER CO, USA, 80234	ERS	Call Monitoring	No	More Details Edit Delete
LOC3	1300, W 120TH AVE (D4-H03), WESTMINSTER CO, USA, 80234	ERS	Call Monitoring	No	More Details Edit Delete
LOC4	1300, W 120TH AVE (D4-H04), WESTMINSTER CO, USA, 80234	ERS	Call Monitoring	No	More Details Edit Delete
LOC5	1300, W 120TH AVE (D4-H05), WESTMINSTER CO, USA, 80234	ERS	Call Monitoring	No	More Details Edit Delete

Step	Description
9.	**Provisioned Endpoints** 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 **Provisioning → Endpoints** tab. Enter the file name in the **Batch File** field and click the **Upload** button. At the bottom of the screen, **Status** and **Actions 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 **Validate** under **Actions**. Once the file is validated, click **Batch Process** which will appear under **Actions**. Once this completes, the **Status** will change to **Finished**. 

Step	Description
10.	**Layer 2 Discovery** 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 **Auto Discovery → Layer 2 Discovery → Switch** tab to display the list of layer 2 switches. The example below shows the list used for the compliance test. Click the **Add a switch** button to enter the switch parameters. Enter the management IP address of the switch in the **Switch IP** field and enter the appropriate string in the **SNMP Community String** field. Enter the ERL where the switch resides in the **Default ERL ID** field. Default values may be used for all other fields. 

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

8. Verification Steps

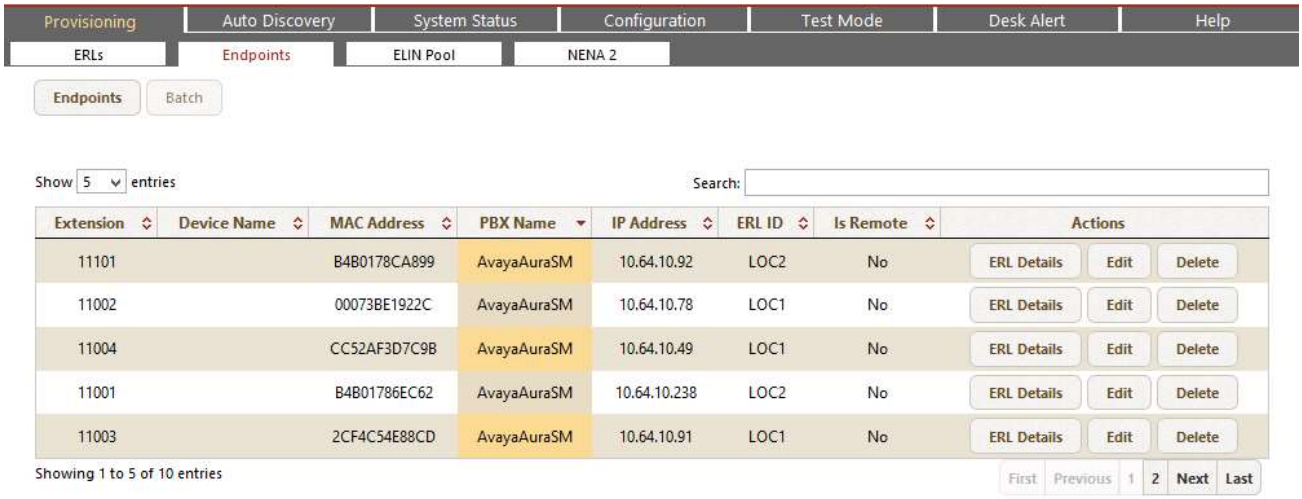
The following steps may be used to verify the configuration:

- 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.

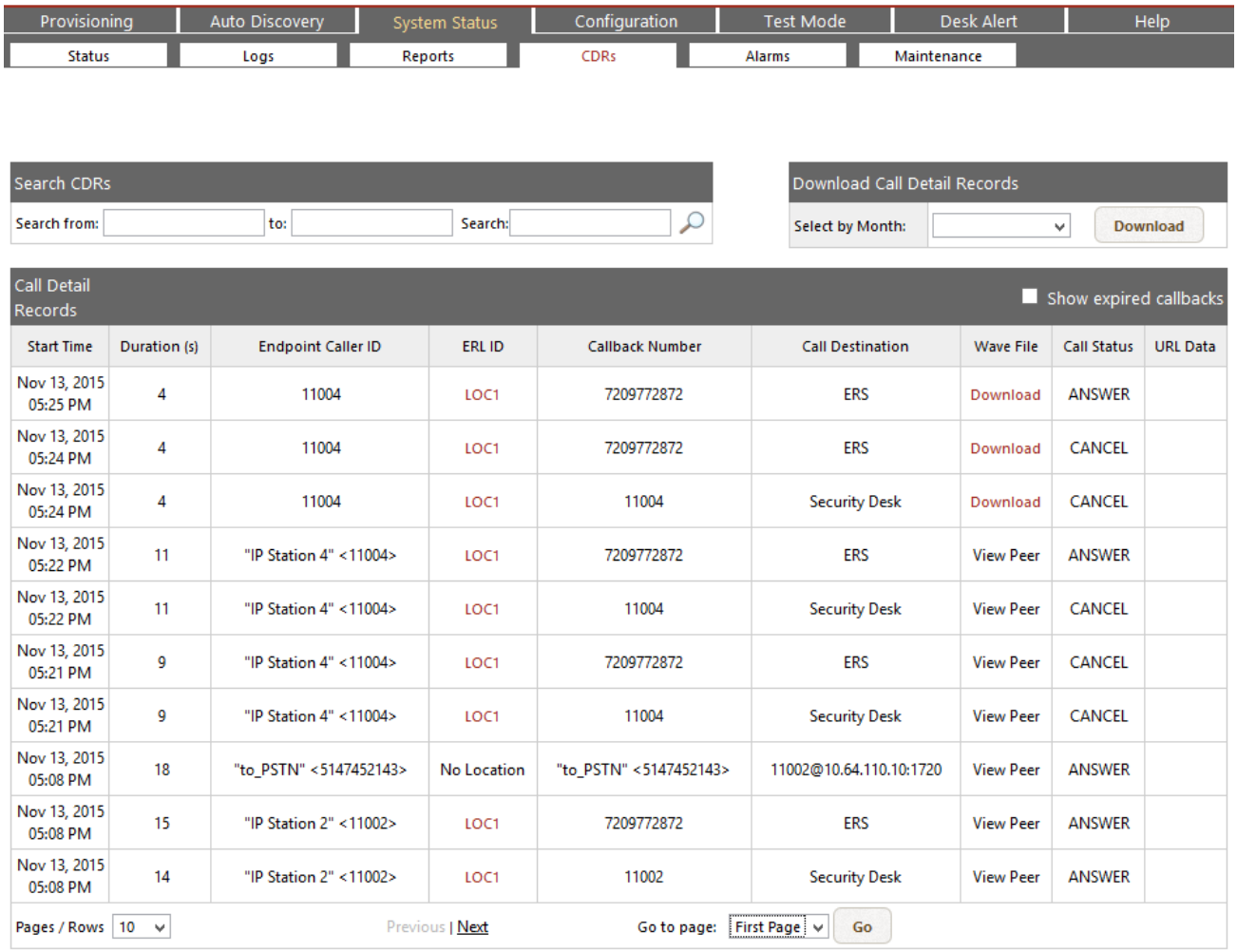
5 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	acm	10.64.110.10	5061	TLS	FALSE	UP	200 OK	UP
○	asm-remote	10.64.10.62	5060	TCP	FALSE	UP	200 OK	UP
○	egw-1	10.64.110.200	5060	TCP	FALSE	UP	200 OK	UP
○	egw-2	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.



- 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.



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	Download	ANSWER	
Nov 13, 2015 05:24 PM	4	11004	LOC1	7209772872	ERS	Download	CANCEL	
Nov 13, 2015 05:24 PM	4	11004	LOC1	11004	Security Desk	Download	CANCEL	
Nov 13, 2015 05:22 PM	11	"IP Station 4" <11004>	LOC1	7209772872	ERS	View Peer	ANSWER	
Nov 13, 2015 05:22 PM	11	"IP Station 4" <11004>	LOC1	11004	Security Desk	View Peer	CANCEL	
Nov 13, 2015 05:21 PM	9	"IP Station 4" <11004>	LOC1	7209772872	ERS	View Peer	CANCEL	
Nov 13, 2015 05:21 PM	9	"IP Station 4" <11004>	LOC1	11004	Security Desk	View Peer	CANCEL	
Nov 13, 2015 05:08 PM	18	"to_PSTN" <5147452143>	No Location	"to_PSTN" <5147452143>	11002@10.64.110.10:1720	View Peer	ANSWER	
Nov 13, 2015 05:08 PM	15	"IP Station 2" <11002>	LOC1	7209772872	ERS	View Peer	ANSWER	
Nov 13, 2015 05:08 PM	14	"IP Station 2" <11002>	LOC1	11002	Security Desk	View Peer	ANSWER	

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 1st, 2015

[4] ESL Configuration Guide Rev. A, Rev. G, Nov 20, 2015

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.