Avaya Solution & Interoperability Test Lab

Application Notes for Configuring 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Session Manager R6.2, Avaya one-X® Desk Phones and Avaya one-X® Communicator – Issue 1.2

Abstract

These Application Notes describe the procedures for configuring the 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Session Manager R6.2 and Avaya one-X® Desk Phones.

The 911 Enable Emergency Gateway offer 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® Desk Phones 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 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 the Emergency Gateway via a SIP trunk. The compliance testing focused on placing 911 calls from various endpoint types 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 and ERS 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 layer 2 switches.
- Layer 3 discovery of Avaya one-X® Desk Phones that support the PUSH API.
- Layer 3 discovery of Avaya one-X® Communicator when used with 911 Enable E911 Softphone Locator (ESL) Software.
- 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.

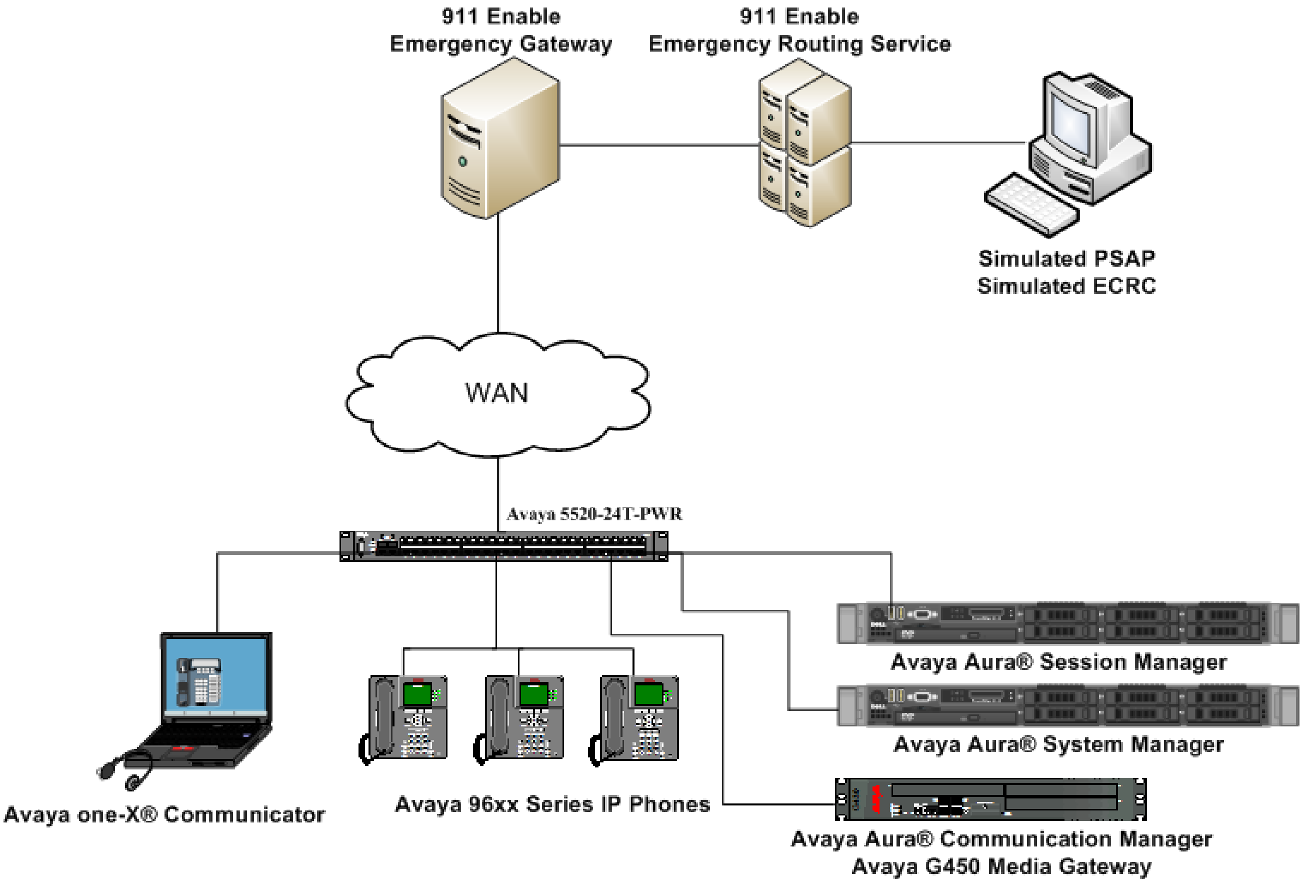
2.2. Test Results

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


911 Enable
Emergency Gateway
911 Enable
Emergency Routing Service
Simulated PSAP
Simulated ECRC
WAN
Avaya 5520-24T-PWR
Avaya Aura® Session Manager
Avaya Aura® System Manager
Avaya one-X® Communicator
Avaya 96xx Series IP Phones
Avaya Aura® Communication Manager
Avaya G450 Media Gateway

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 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 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 respond with a "503 Service Unavailable" response.

This will result in Session Manager, redirecting the call to an alternate destination. The call flows from User Extension → Session Manager → EGW. After EGW responds with a negative response the same call will flow 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. **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 are unreachable (do not respond to SIP INVITEs), Session Manager will timeout on its call requests to EGWs and 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

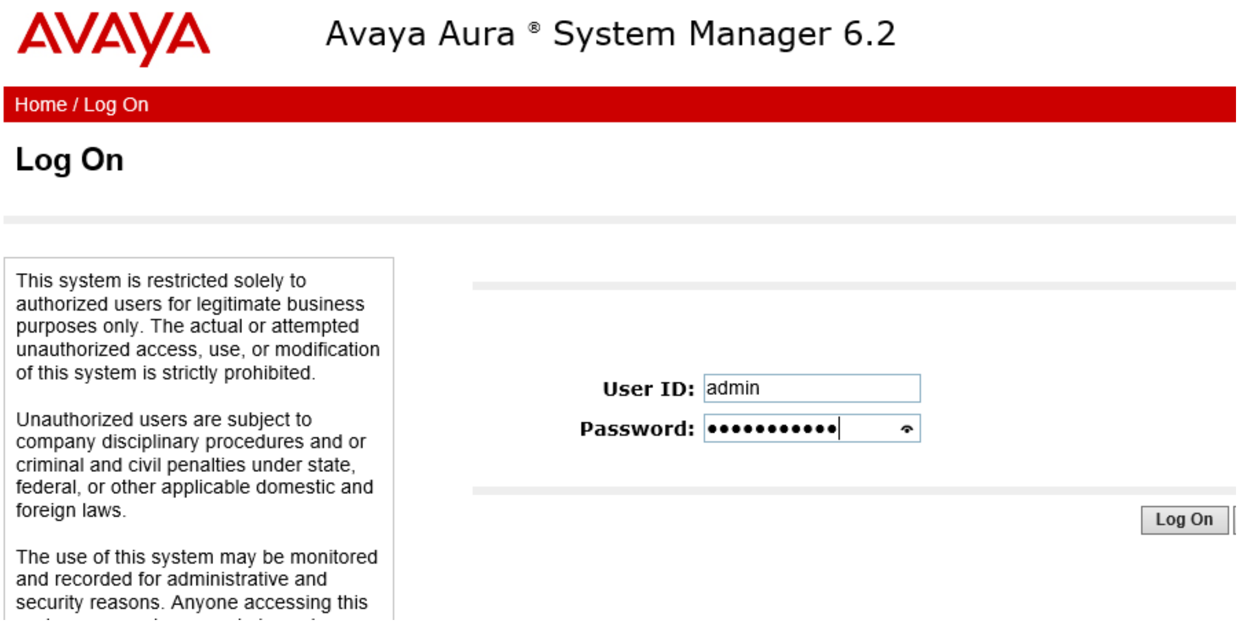
The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya Aura® Session Manager	6.2 SP3
Avaya G450 Media Gateway	31.20.1
Avaya Aura® Communication Manager	6.2 SP3
Avaya 9630 IP Phone Avaya 9608 IP Phone Avaya 9641 IP Phone	SIP 2.6.7 H.323 3.1.5
Avaya one-X® Communicator	6.1
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
911 Enable Emergency Gateway	4.1
911 Enable E911 Softphone Locator Software	1.5
911 Enable Emergency Routing Service	2.12

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].

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 6.2

Home / Log On

Log On

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

User ID: admin

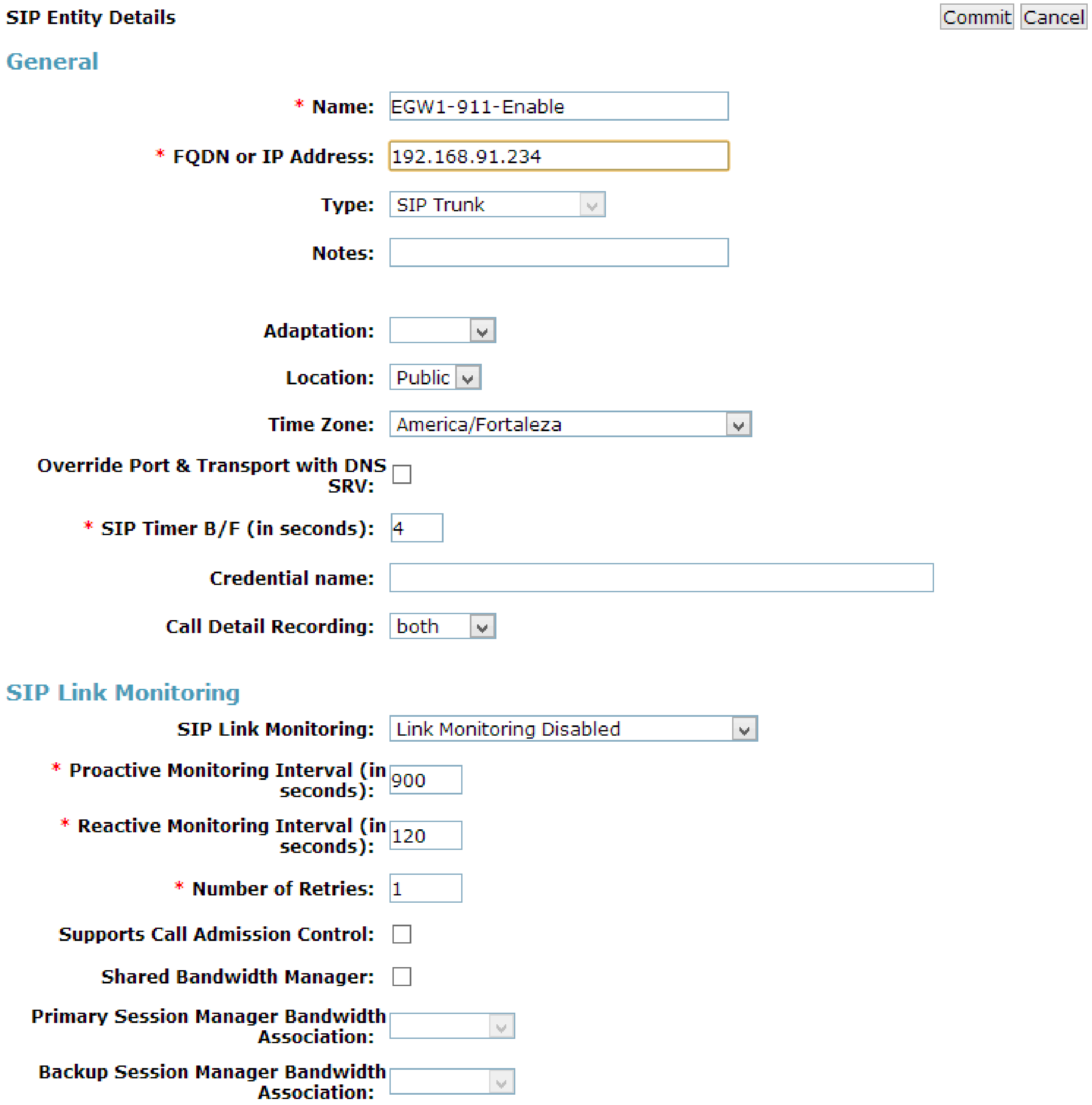
Password: •••••••••••

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**, EGW1-911-Enable**.**
- 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.



SIP Entity Details

General

* Name:	EGW1-911-Enable
* FQDN or IP Address:	192.168.91.234
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	Public
Time Zone:	America/Fortaleza
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	both

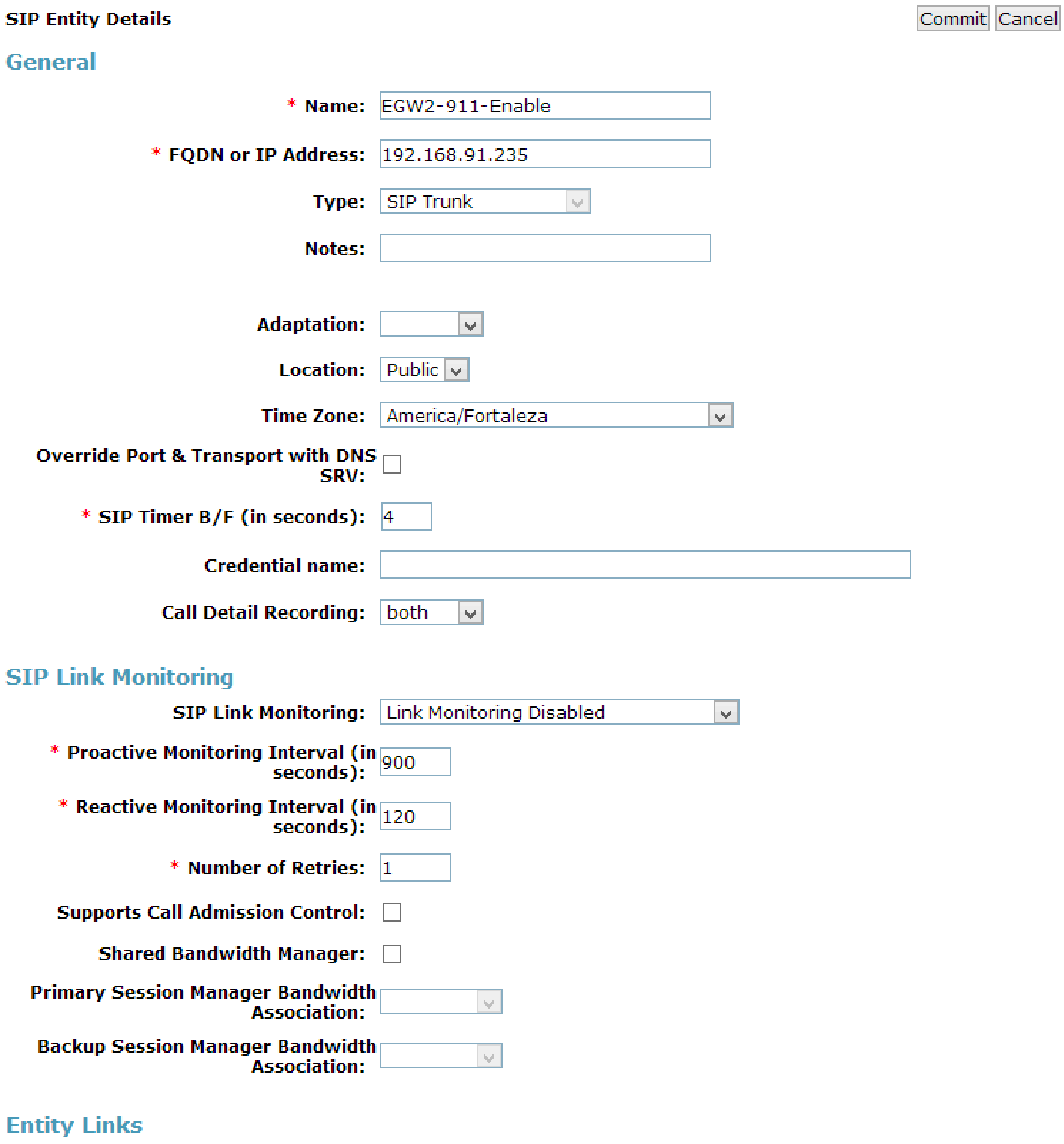
SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Disabled
* Proactive Monitoring Interval (in seconds):	900
* Reactive Monitoring Interval (in seconds):	120
* Number of Retries:	1
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□
Primary Session Manager Bandwidth Association:	
Backup Session Manager Bandwidth Association:	

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

- Type in a descriptive name in **Name**, EGW2-911-Enable**.**
- 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.



SIP Entity Details

General

* Name: EGW2-911-Enable

* FQDN or IP Address: 192.168.91.235

Type: SIP Trunk

Notes:

Adaptation:

Location: Public

Time Zone: America/Fortaleza

Override Port & Transport with DNS SRV: □

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

Credential name:

Call Detail Recording: both

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Supports Call Admission Control: □

Shared Bandwidth Manager: □

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

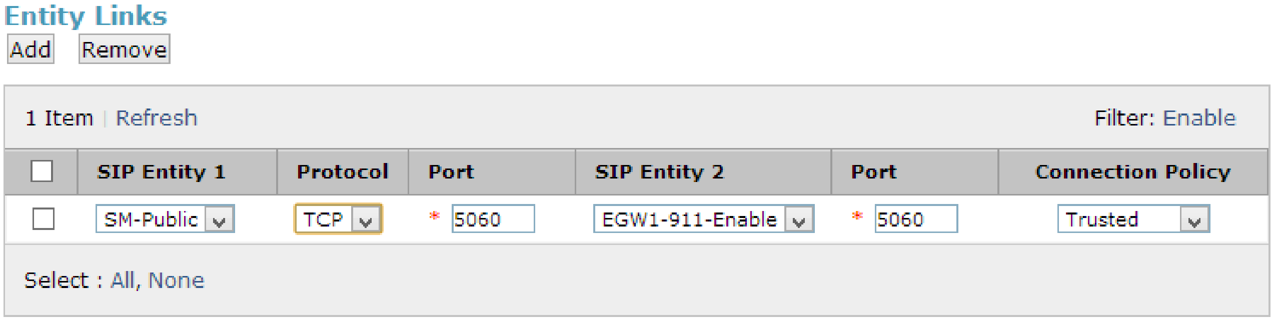
Entity Links

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 EGW1 SIP Entity added in previous step
- Set **Port** to **5060**

Click **Commit** to save changes.



Entity Links

Add Remove

1 Item | Refresh   Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	SM-Public	TCP	* 5060	EGW1-911-Enable	* 5060	Trusted

Select : All, None

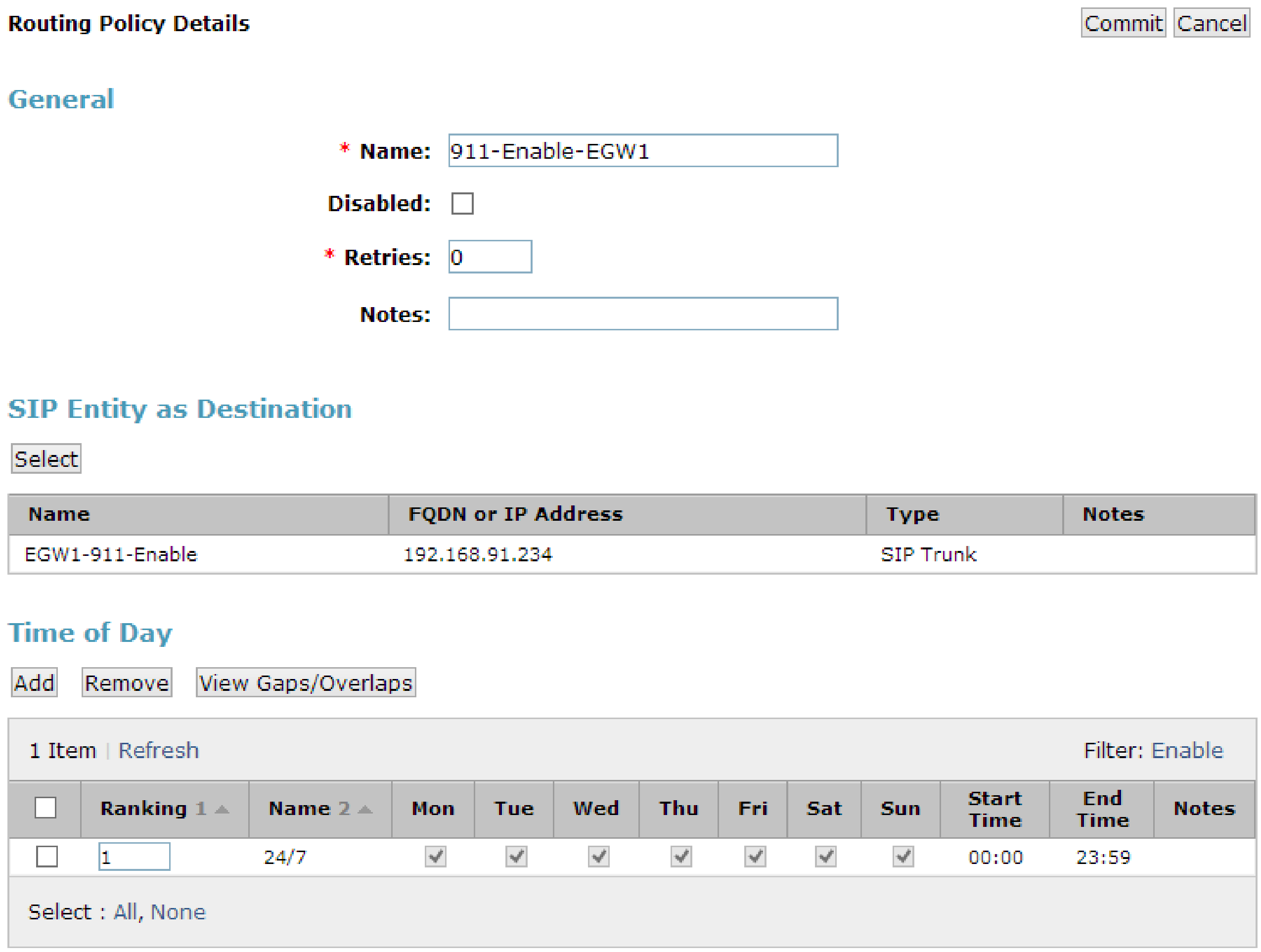
Note: Repeat this step for EGW2-911-Enable SIP Entity.

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, EGW1-911-Enable**.**
- Under **Time of Day**, set **Ranking** to **1.**

Click **Commit** to save changes.



Routing Policy Details

General

* **Name:**	911-Enable-EGW1
Disabled:	☐
* **Retries:**	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
EGW1-911-Enable	192.168.91.234	SIP Trunk	

Time of Day

1 Item | Refresh

☐	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	1	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

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

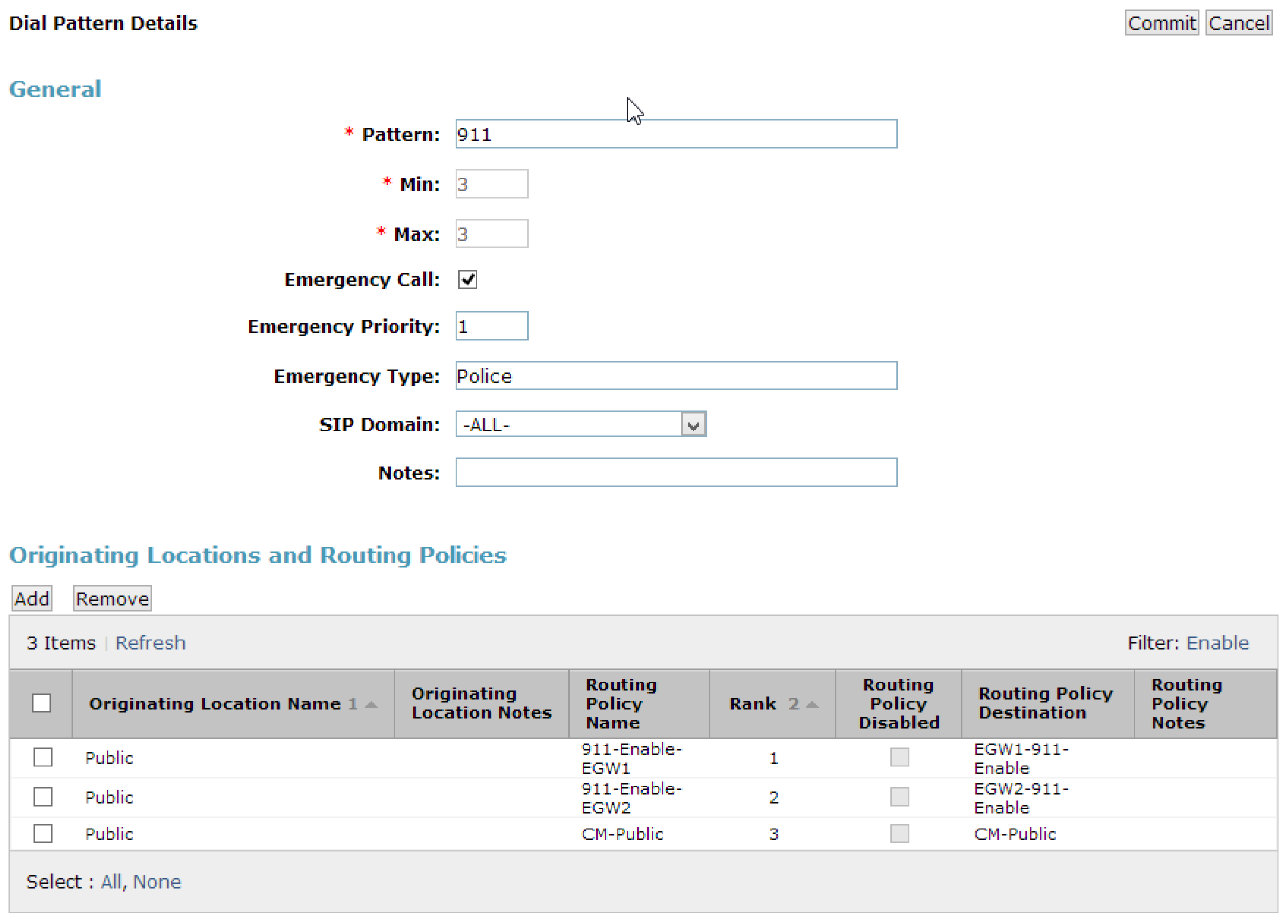
5.4. Add a Dial Pattern

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.



General

* Pattern:	911
* Min:	3
* Max:	3
Emergency Call:	☑
Emergency Priority:	1
Emergency Type:	Police
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

□	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Public		911-Enable-EGW1	1	□	EGW1-911-Enable	
□	Public		911-Enable-EGW2	2	□	EGW2-911-Enable	
□	Public		CM-Public	3	□	CM-Public	

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 of analog or digital telephones.

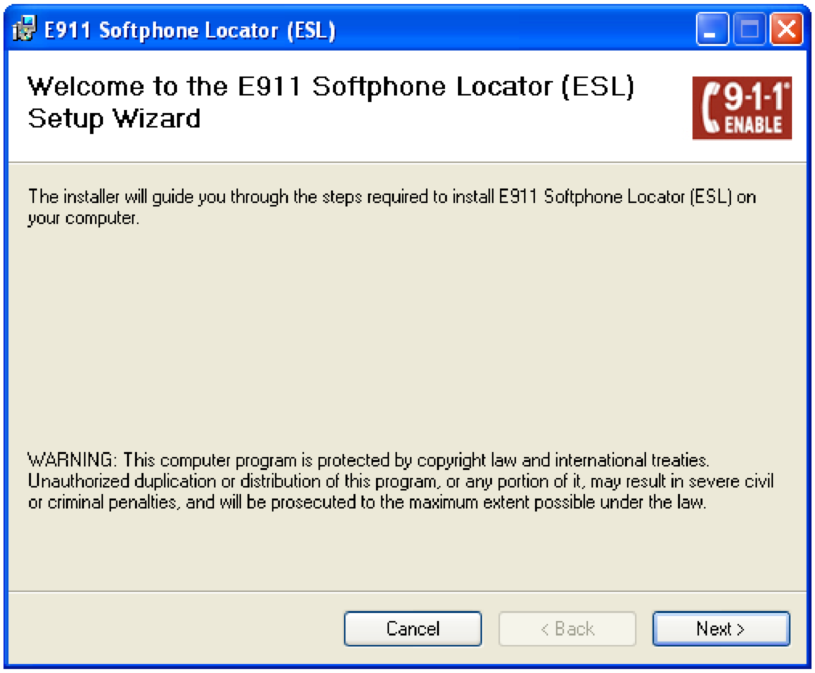
6.1. Avaya H.323 and SIP Telephone Configuration File

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 (***192.168.0.118***) represents the IP address of the private side of the primary EGW. The second parameter (***19***) is the **IP-PBX ID** number that is created when configuring EGW.

```
## 911 Enable Settings
SET TPSLIST /
SET SUBSCRIBELIST http://192.168.0.118/19/r
SET PUSHPORT 80
SET PUSHCAP 2
SET WMLHOME http://192.168.0.118/wml/19/service.html
```

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

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



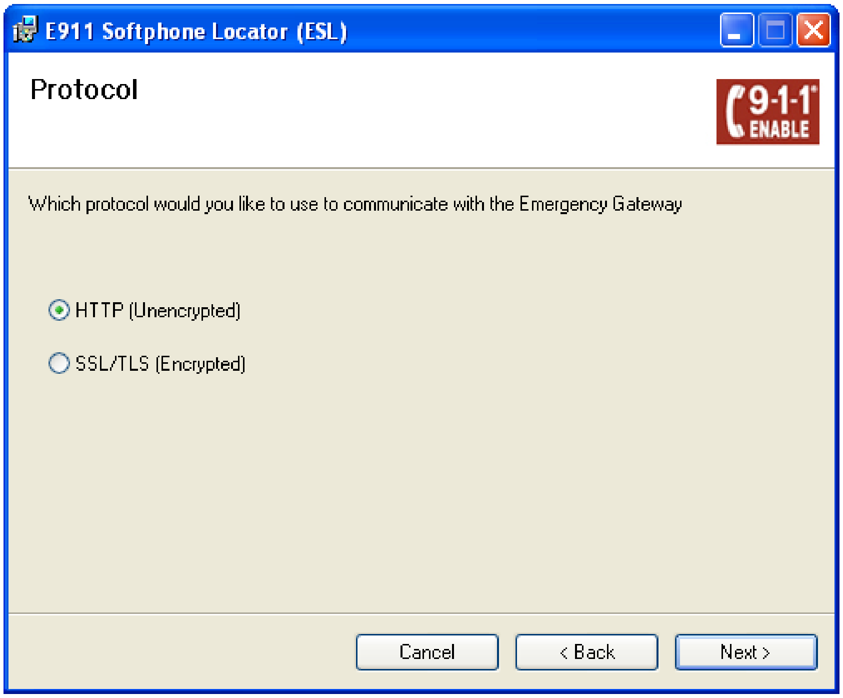
E911 Softphone Locator (ESL)

Welcome to the E911 Softphone Locator (ESL) Setup Wizard

The installer will guide you through the steps required to install E911 Softphone Locator (ESL) on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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



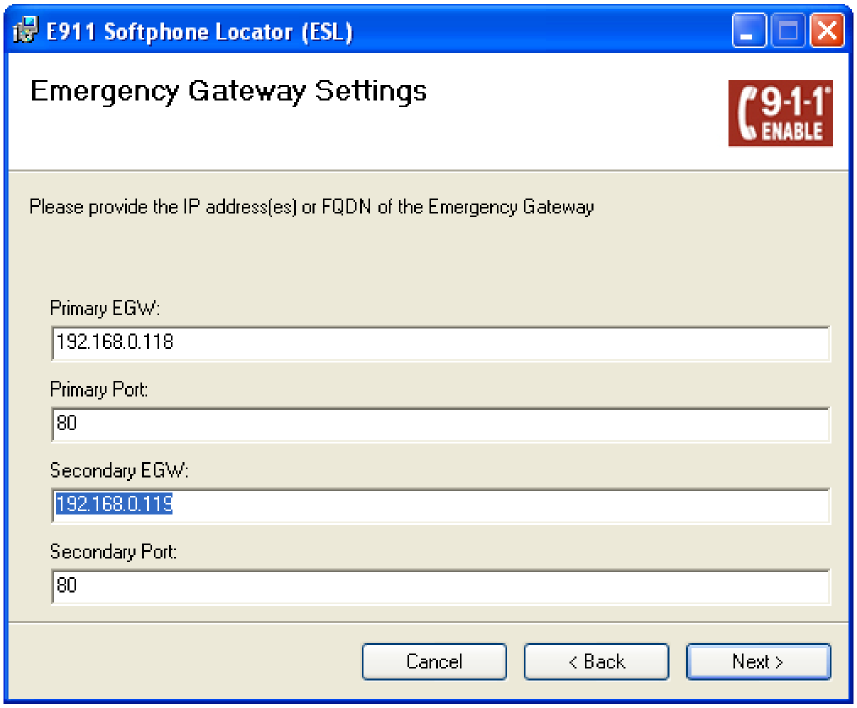
Protocol

Which protocol would you like to use to communicate with the Emergency Gateway

● HTTP (Unencrypted)

○ SSL/TLS (Encrypted)

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



Emergency Gateway Settings

Please provide the IP address(es) or FQDN of the Emergency Gateway

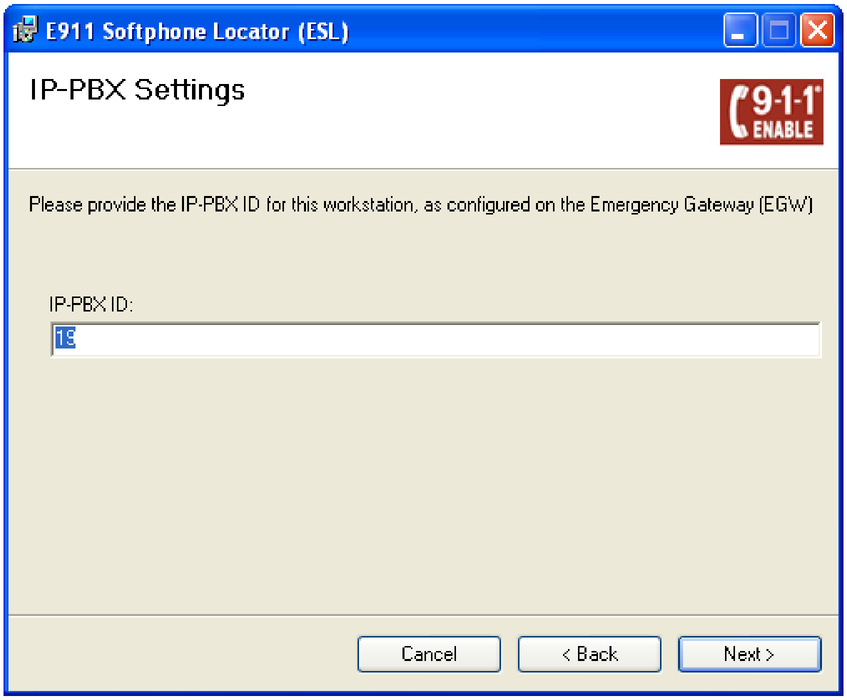
Primary EGW: 192.168.0.118

Primary Port: 80

Secondary EGW: 192.168.0.119

Secondary Port: 80

Enter an **IP-PBX ID** that is created while configuring EGW, Click **Next**.



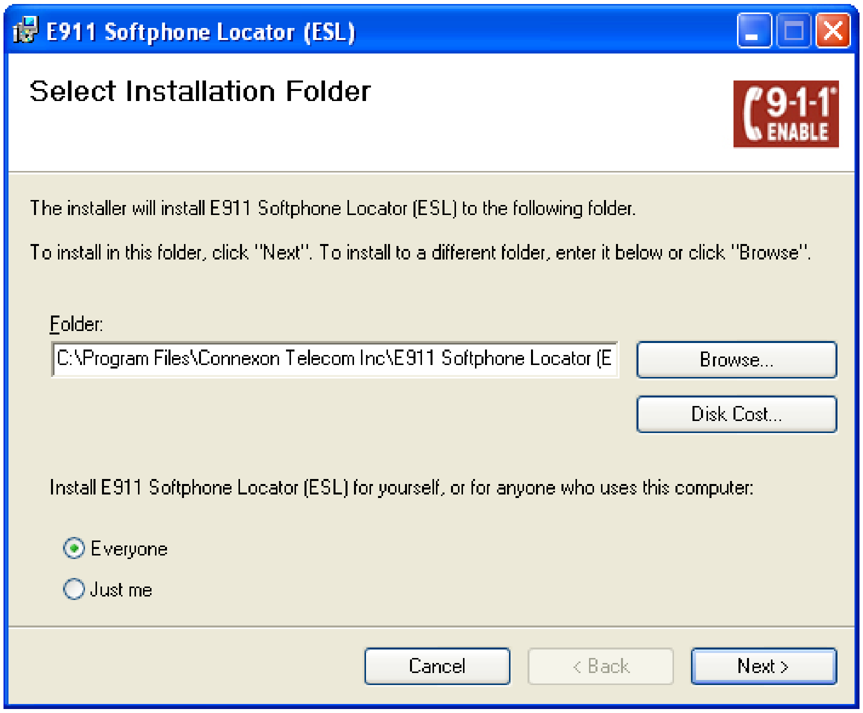
E911 Softphone Locator (ESL)

IP-PBX Settings

Please provide the IP-PBX ID for this workstation, as configured on the Emergency Gateway (EGW)

IP-PBX ID: 19

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



E911 Softphone Locator (ESL)

Select Installation Folder

The installer will install E911 Softphone Locator (ESL) to the following folder.

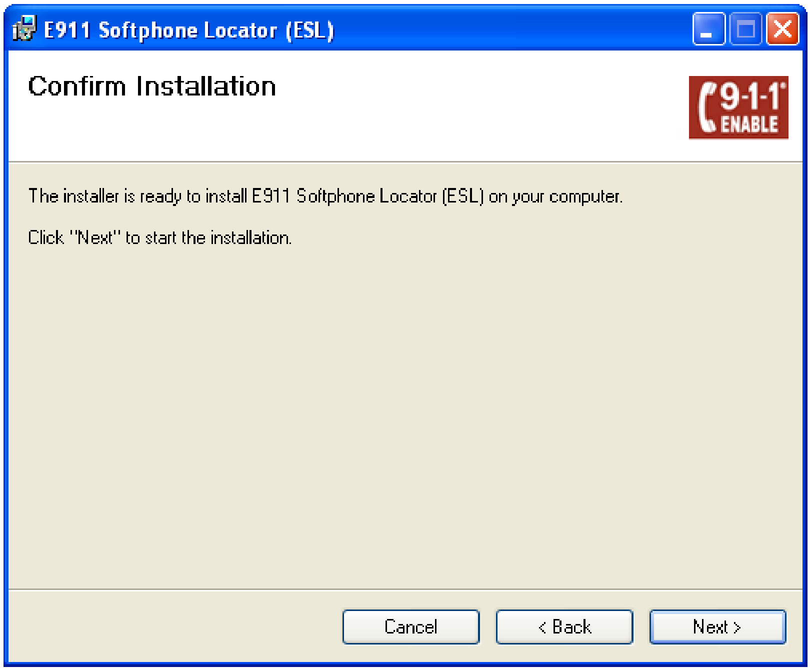
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Connexon Telecom Inc\E911 Softphone Locator (E

Install E911 Softphone Locator (ESL) for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Confirm the installation by clicking **Next**.

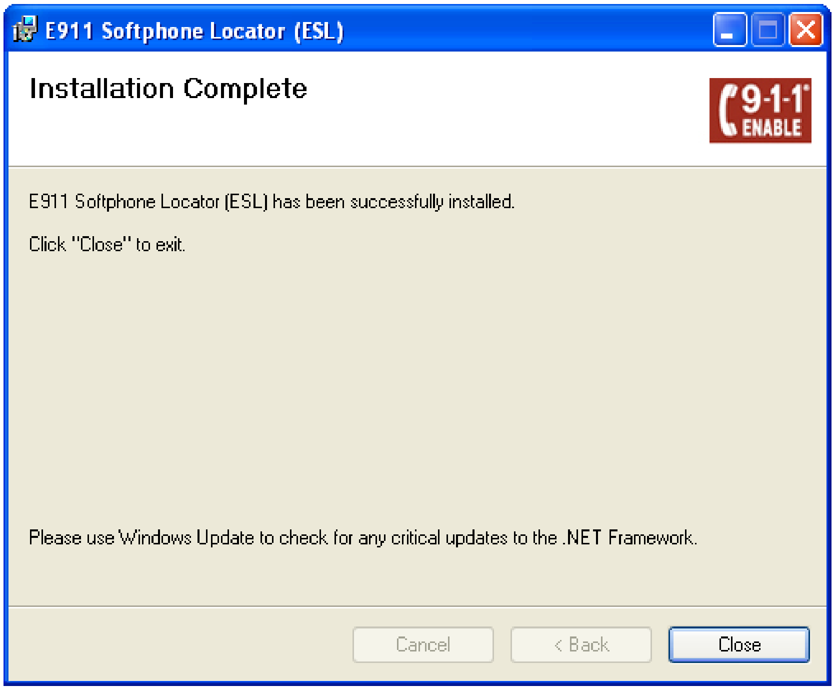


Confirm Installation

The installer is ready to install E911 Softphone Locator (ESL) on your computer.

Click "Next" to start the installation.

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



Installation Complete

E911 Softphone Locator (ESL) has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

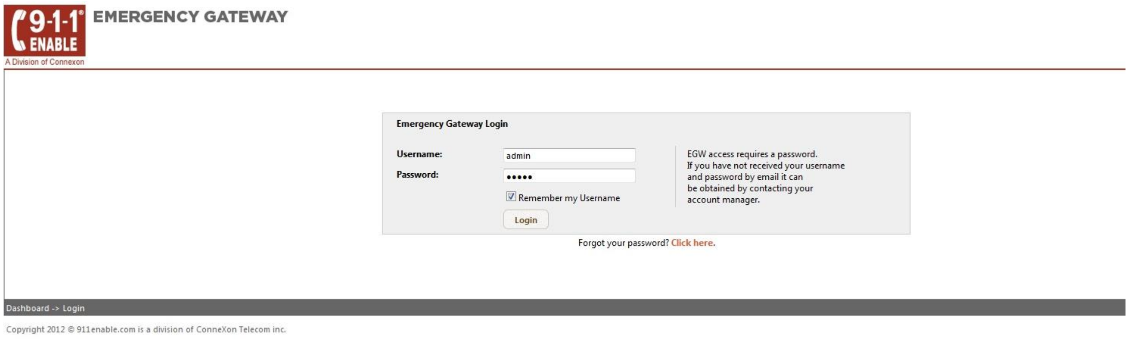
7. Configure 911 Enable Emergency Gateway (EGW)

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.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

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**.



Emergency Gateway Login

Username: admin

Password: •••••

☑ Remember my Username

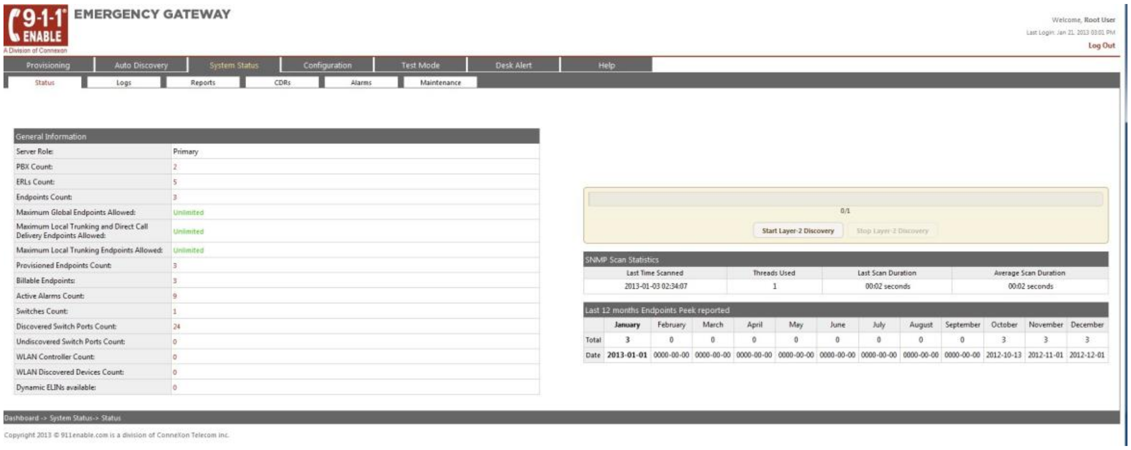
EGW access requires a password. If you have not received your username and password by email it can be obtained by contacting your account manager.

Copyright 2012 © 911enable.com is a division of ConneXon Telecom inc.

</td></tr>
<tr><td>2.</td><td>

Main Page

The main page of the EGW will appear.



Last Login: Jan 21, 2013 03:01 PM

<table>
<tr><th colspan="2">General Information</th></tr>
<tr><td>Server Role:</td><td>Primary</td></tr>
<tr><td>PBX Count:</td><td>2</td></tr>
<tr><td>ERLs Count:</td><td>5</td></tr>
<tr><td>Endpoints Count:</td><td>3</td></tr>
<tr><td>Maximum Global Endpoints Allowed:</td><td>Unlimited</td></tr>
<tr><td>Maximum Local Trunking and Direct Call Delivery Endpoints Allowed:</td><td>Unlimited</td></tr>
<tr><td>Maximum Local Trunking Endpoints Allowed:</td><td>Unlimited</td></tr>
<tr><td>Provisioned Endpoints Count:</td><td>3</td></tr>
<tr><td>Billable Endpoints:</td><td>3</td></tr>
<tr><td>Active Alarms Count:</td><td>9</td></tr>
<tr><td>Switches Count:</td><td>1</td></tr>
<tr><td>Discovered Switch Ports Count:</td><td>24</td></tr>
<tr><td>Undiscovered Switch Ports Count:</td><td>0</td></tr>
<tr><td>WLAN Controller Count:</td><td>0</td></tr>
<tr><td>WLAN Discovered Devices Count:</td><td>0</td></tr>
<tr><td>Dynamic ELINs available:</td><td>0</td></tr>
</table>

0/1

<table>
<tr><th colspan="4">SNMP Scan Statistics</th></tr>
<tr><td>Last Time Scanned</td><td>Threads Used</td><td>Last Scan Duration</td><td>Average Scan Duration</td></tr>
<tr><td>2013-01-03 02:34:07</td><td>1</td><td>00:02 seconds</td><td>00:02 seconds</td></tr>
</table>

<table>
<tr><th colspan="13">Last 12 months Endpoints Peek reported</th></tr>
<tr><td></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>December</td></tr>
<tr><td>Total</td><td>3</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>3</td><td>3</td><td>3</td></tr>
<tr><td>Date</td><td>2013-01-01</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>2012-10-13</td><td>2012-11-01</td><td>2012-12-01</td></tr>
</table>

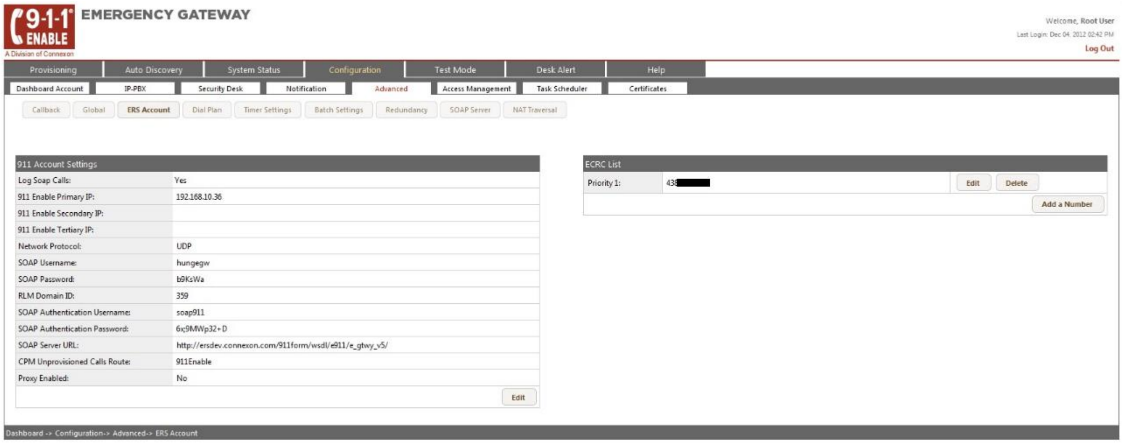
Copyright 2013 © 911enable.com is a division of ConneXon Telecom inc.

</td></tr>
</table>

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. For security reasons, the public IP addresses of the ERS are not shown but some digits are replaced by an x. 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, the full PSTN number is not shown.



911 Account Settings

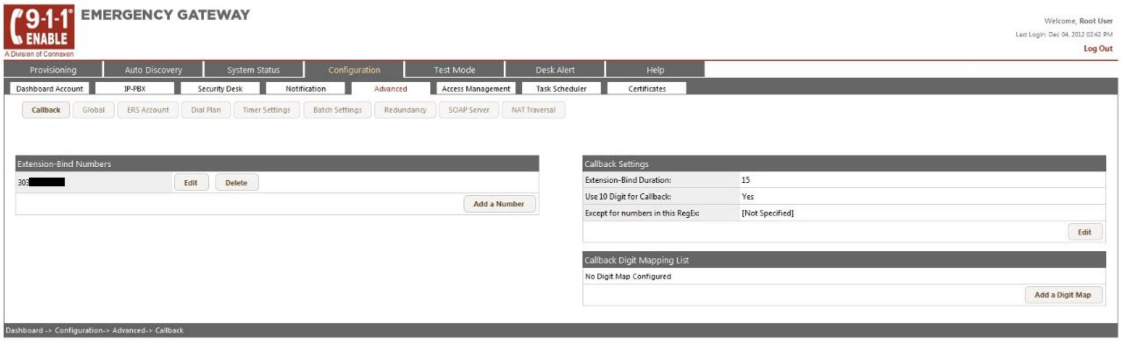
Log Soap Calls:	Yes
911 Enable Primary IP:	192.168.10.36
911 Enable Secondary IP:	
911 Enable Tertiary IP:	
Network Protocol:	UDP
SOAP Username:	hungegw
SOAP Password:	b9KsWa
RLM Domain ID:	359
SOAP Authentication Username:	soap911
SOAP Authentication Password:	6x9MWp32+D
SOAP Server URL:	http://ersdev.connexon.com/911form/wsdl/e911/e_gtwy_v5/
CPM Unprovisioned Calls Route:	911Enable
Proxy Enabled:	No

ECRC List

Priority 1:	43[redacted]

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 PSTN number is not shown.



Extension-Bind Numbers

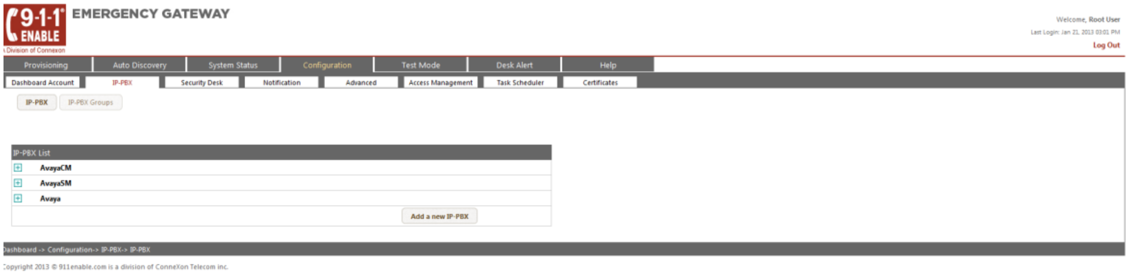
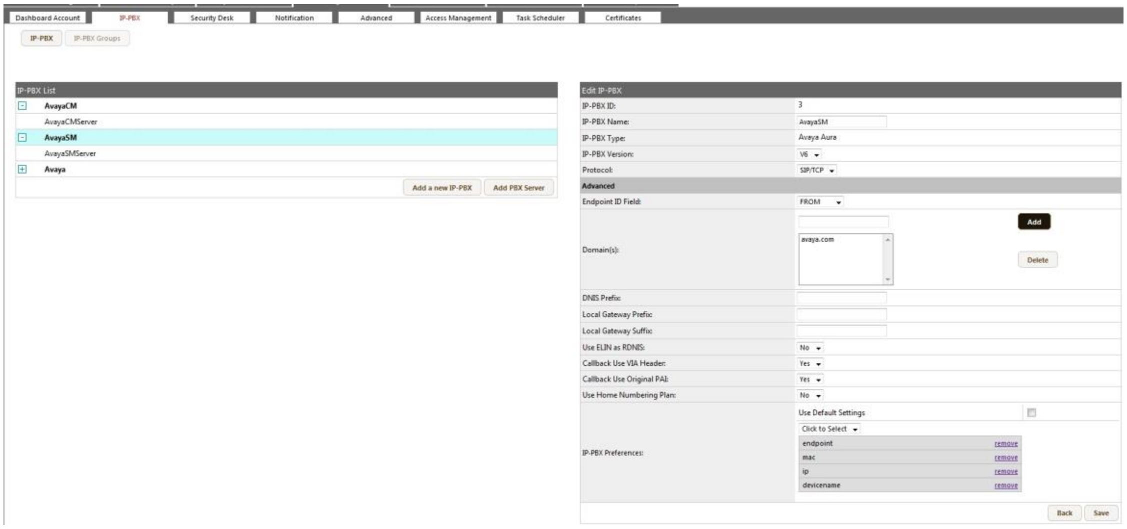
303[redacted]

Callback Settings

Extension-Bind Duration:	15
Use 10 Digit for Callback:	Yes
Except for numbers in this RegEx:	[Not Specified]

Callback Digit Mapping List

No Digit Map Configured

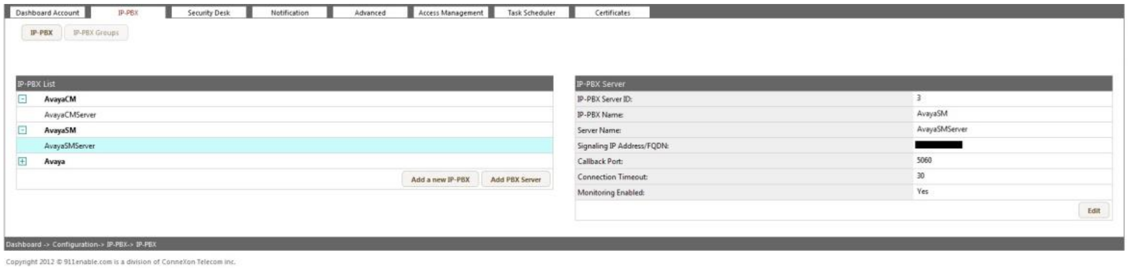
Step	Description
5.	**IP-PBX** **Steps 5 – 7** define the parameters needed to connect to Session Manager via an SIP trunk on the private side of the EGW. Navigate to **Configuration → IP-PBX** to configure these settings. First, an IP-PBX is defined by clicking the **Add a new IP-PBX** button. The example below shows the IP-PBX created for the compliance test. Click the IP-PBX name to view the details.  Last Login: Jan 21, 2013 03:01 PM Provisioning Auto Discovery System Status Configuration Test Mode Desk Alert Help Dashboard Account IP-PBX Security Desk Notification Advanced Access Management Task Scheduler Certificates IP-PBX List AvayaCM AvayaSM Avaya Dashboard -> Configuration-> IP-PBX-> IP-PBX Copyright 2013 © 911enable.com is a division of ConneXon Telecom inc.
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 **PBX-Type** to ***Avaya***. ▪ 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 5**, **Step 1**) and the ESL installation (**Section 5**, **Step 5**).  Dashboard Account IP-PBX Security Desk Notification Advanced Access Management Task Scheduler Certificates IP-PBX List AvayaCM AvayaCMServer AvayaSM AvayaSMServer Avaya Add a new IP-PBX Add PBX Server Edit IP-PBX IP-PBX ID: 3 IP-PBX Name: AvayaSM IP-PBX Type: Avaya Aura IP-PBX Version: V6 Protocol: SIP/TCP Advanced Endpoint ID Field: FROM Domain(s): avaya.com DNIS Prefix: Local Gateway Prefix: Local Gateway Suffix: Use ELIN as RDNIS: No Callback Use VIA Header: Yes Callback Use Original PAI: Yes Use Home Numbering Plan: No IP-PBX Preferences: Use Default Settings □ Click to Select endpoint remove mac remove ip remove devicename remove

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>

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 ***Avaya*** created for the compliance test. The list contains a single server named ***Server1***. Click the server name to see the details.

A server can be added by clicking the **Add a 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.



IP-PBX List

- ⊟ **AvayaCM**
  - AvayaCMServer
- ⊟ **AvayaSM**
  - AvayaSMServer
- ⊞ **Avaya**

IP-PBX Server

IP-PBX Server ID:	3
IP-PBX Name:	AvayaSM
Server Name:	AvayaSMServer
Signaling IP Address/FQDN:	[redacted]
Callback Port:	5060
Connection Timeout:	30
Monitoring Enabled:	Yes

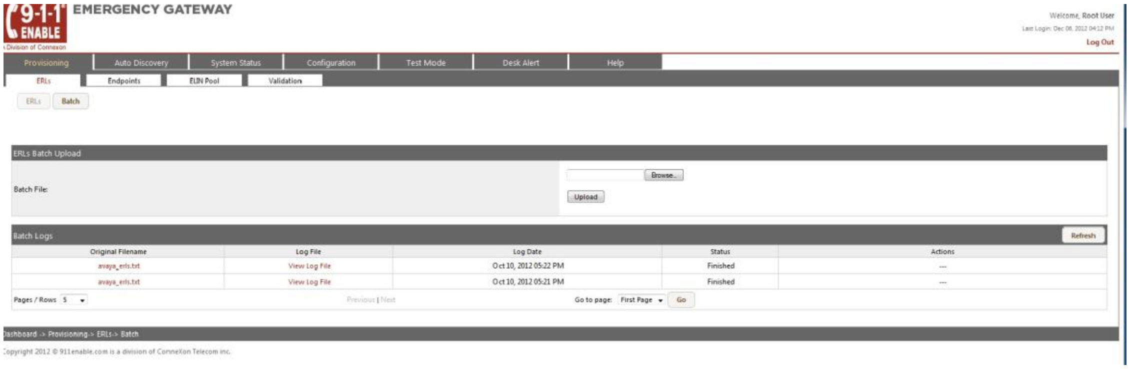
Dashboard -> Configuration-> IP-PBX-> IP-PBX

Copyright 2012 © 911enable.com is a division of ConneXon Telecom inc.

</td></tr>
<tr><td>8.</td><td>

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**.



ERLs Batch Upload

Batch File:

Batch Logs

Original Filename	Log File	Log Date	Status	Actions
avaya_erls.txt	View Log File	Oct 10, 2012 05:22 PM	Finished	---
avaya_erls.txt	View Log File	Oct 10, 2012 05:21 PM	Finished	---

Pages / Rows 5 Previous | Next Go to page: First Page

Dashboard -> Provisioning-> ERLs-> Batch

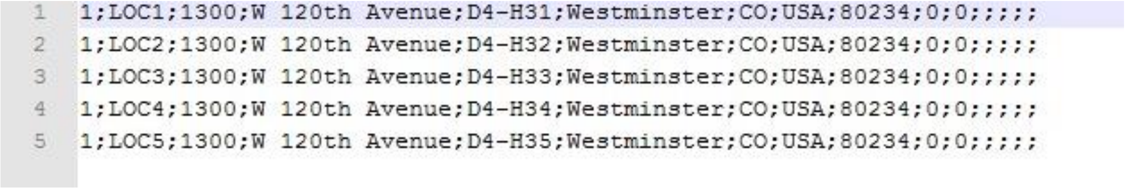
Copyright 2012 © 911enable.com is a division of ConneXon Telecom inc.

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>

Locations Batch File

The following is an example of the ERL batch file used for the compliance test. It shows that ERL LOC1 is associated with address 1300 W 120th Avenue, D4-H31, Westminster, CO 80234. Similarly, ERL LOC2, LOC3, LOC4 and LOC5 are also associated with the same address.

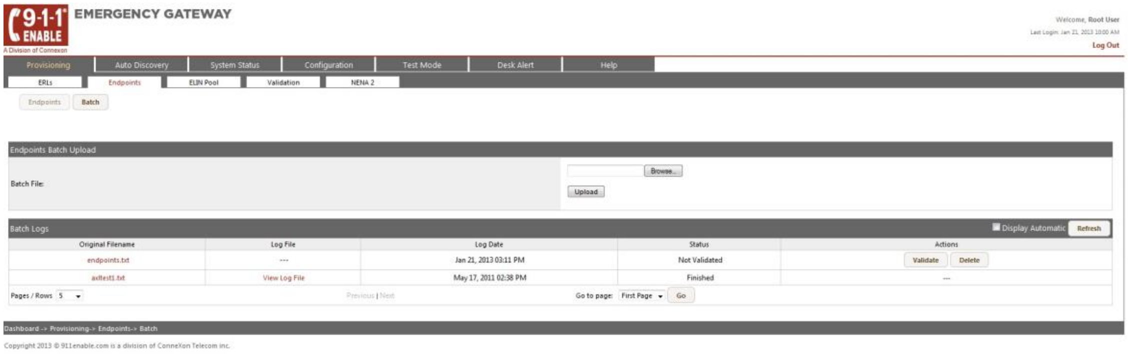


```
1;LOC1;1300;W 120th Avenue;D4-H31;Westminster;CO;USA;80234;0;0;;;;;
1;LOC2;1300;W 120th Avenue;D4-H32;Westminster;CO;USA;80234;0;0;;;;;
1;LOC3;1300;W 120th Avenue;D4-H33;Westminster;CO;USA;80234;0;0;;;;;
1;LOC4;1300;W 120th Avenue;D4-H34;Westminster;CO;USA;80234;0;0;;;;;
1;LOC5;1300;W 120th Avenue;D4-H35;Westminster;CO;USA;80234;0;0;;;;;
```

</td></tr>
<tr><td>10.</td><td>

Provisioned Endpoints

All endpoints that cannot 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**. An example of a provisioned endpoints batch file is shown in **Step 11**.



Endpoints Batch Upload

Batch File:

Batch Logs

Original Filename	Log File	Log Date	Status	Actions
endpoints.txt	---	Jan 21, 2013 03:11 PM	Not Validated	Validate Delete
axltest1.txt	View Log File	May 17, 2011 02:38 PM	Finished	---

Pages / Rows 5

Go to page: First Page

Dashboard -> Provisioning-> Endpoints-> Batch

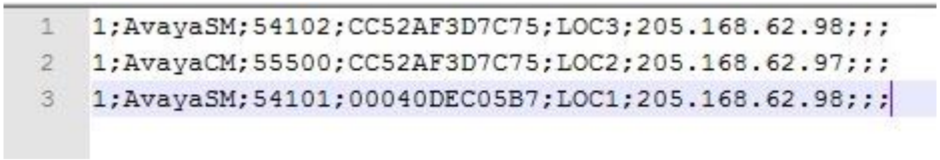
Copyright 2013 © 911enable.com is a division of ConneXon Telecom inc.

</td></tr>
</table>

Step | **Description**

11. **Provisioned Endpoints Batch File**

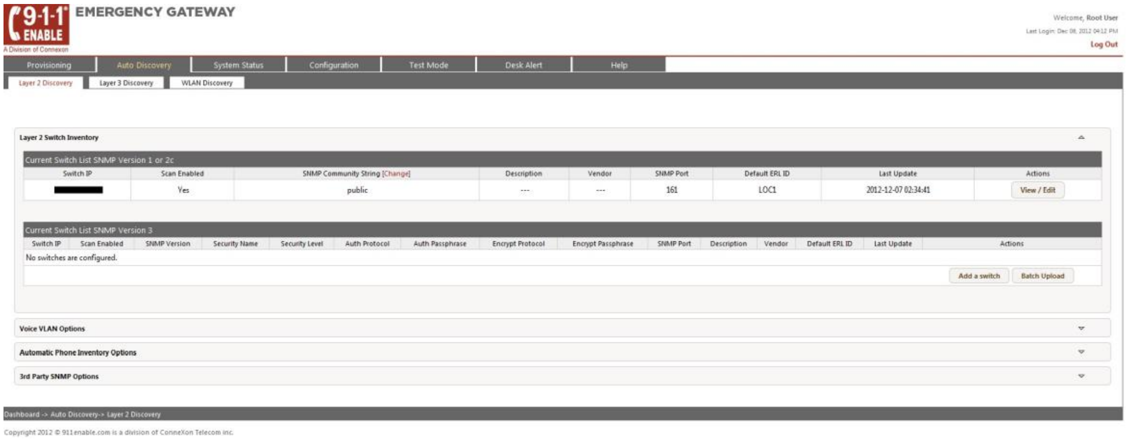
The following is an example of the provisioned endpoints batch file used for the compliance test. It contains the extensions associated with the digital and analog endpoints since these endpoints cannot be auto-discovered. In the case of the compliance test, the Avaya IP Telephone with extension 50023 also could not be auto-discovered due to the type of layer 2 switch to which it was connected. Thus, this extension should also be manually provisioned. However, for the purposes of the compliance test, this extension was not provisioned in order to test the EGW operation when the location of an extension is unknown. In this case, emergency calls from extension 50023 would get routed to an ECRC operator to collect location and callback information. The batch file shows that all the provisioned endpoints (extensions 52000, and 52003) are associated with the same ERL – LOC3.



```
1;AvayaSM;54102;CC52AF3D7C75;LOC3;205.168.62.98;;;
1;AvayaCM;55500;CC52AF3D7C75;LOC2;205.168.62.97;;;
1;AvayaSM;54101;00040DEC05B7;LOC1;205.168.62.98;;;
```

12. **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** tab to display the list of layer 2 switches. The example below shows the list used for the compliance test. All three switches in **Figure 1** were entered, even though the switch with IP address 192.50.10.253 was known to not support layer 2 discovery. 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.



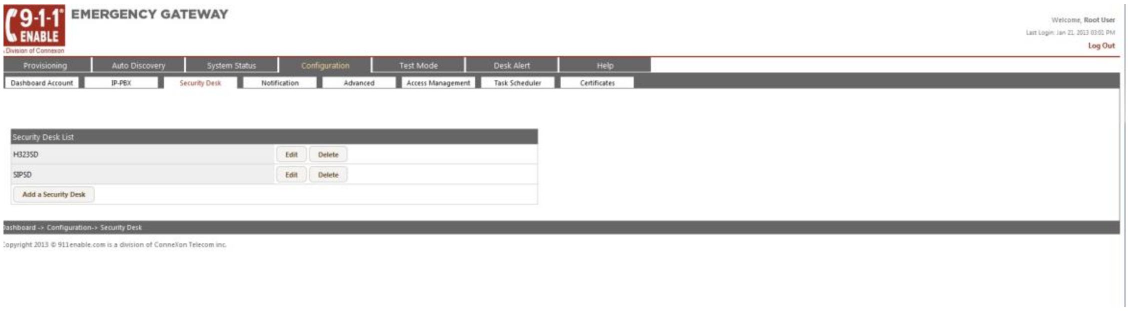
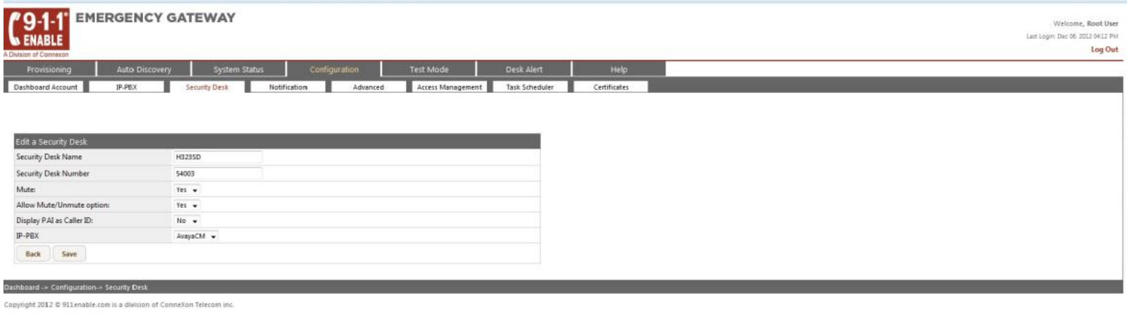
Layer 2 Switch Inventory

Current Switch List SNMP Version 1 or 2c

Switch IP	Scan Enabled	SNMP Community String [Change]	Description	Vendor	SNMP Port	Default ERL ID	Last Update	Actions
[redacted]	Yes	public	---	---	161	LOC1	2012-12-07 02:34:41	View / Edit

Current Switch List SNMP Version 3

Switch IP	Scan Enabled	SNMP Version	Security Name	Security Level	Auth Protocol	Auth Passphrase	Encrypt Protocol	Encrypt Passphrase	SNMP Port	Description	Vendor	Default ERL ID	Last Update	Actions
No switches are configured.														

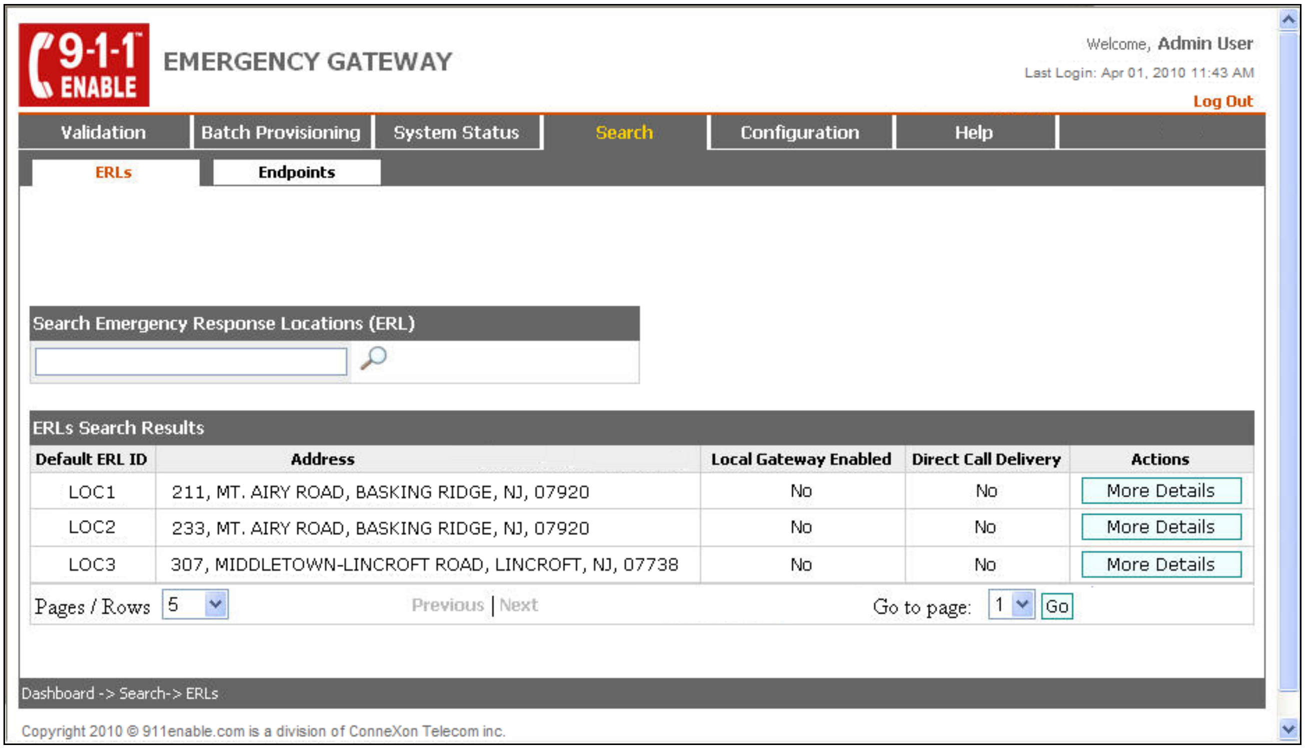
Step	Description
13.	**Security Desk** Emergency calls may be routed to a Security Desk extension as well as being sent to the Emergency Routing Service. Navigate to the **Configuration → Security Desk** tab to create the Security Desk List. To create a security desk, click **Add a Security Desk**. The example below shows the Security Desk created for the compliance test. Click the **Edit** button to view the details.  9-1-1 ENABLE A Division of Connexon EMERGENCY GATEWAY Welcome, Root User Last Login: Jan 21, 2013 03:01 PM Log Out Provisioning Auto Discovery System Status Configuration Test Mode Desk Alert Help Dashboard Account IP-PBX Security Desk Notification Advanced Access Management Task Scheduler Certificates Edit Delete Add a Security Desk Dashboard -> Configuration-> Security Desk Copyright 2013 © 911enable.com is a division of ConneXon Telecom inc. Security Desk List H323SD SIPSD
14.	**Security Desk – Continued** The Security Desk was created with the following parameters. Use default values for all other fields. ▪ Enter a descriptive name for the **Security Desk Name**. ▪ Set the **Security Desk Number** to the extension to call when any user dials an emergency call. This is in addition to the call that will be placed to the Emergency Routing Service. ▪ Set the **IP-PBX** field to the IP-PBX created in **Steps 5 - 6**.  9-1-1 ENABLE A Division of Connexon EMERGENCY GATEWAY Welcome, Root User Last Login: Dec 06, 2012 04:12 PM Log Out Provisioning Auto Discovery System Status Configuration Test Mode Desk Alert Help Dashboard Account IP-PBX Security Desk Notification Advanced Access Management Task Scheduler Certificates Back Save Dashboard -> Configuration-> Security Desk Copyright 2012 © 911enable.com is a division of ConneXon Telecom inc. Edit a Security Desk Security Desk Name: H323SD Security Desk Number: 54003 Mute: Yes Allow Mute/Unmute option: Yes Display P.AI as Caller ID: No IP-PBX: AvayaCM

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.

- On the EGW, verify the ERL information. Navigate to the **Search → ERLs** tab, verify that the locations provided in the batch file earlier in this section are displayed.



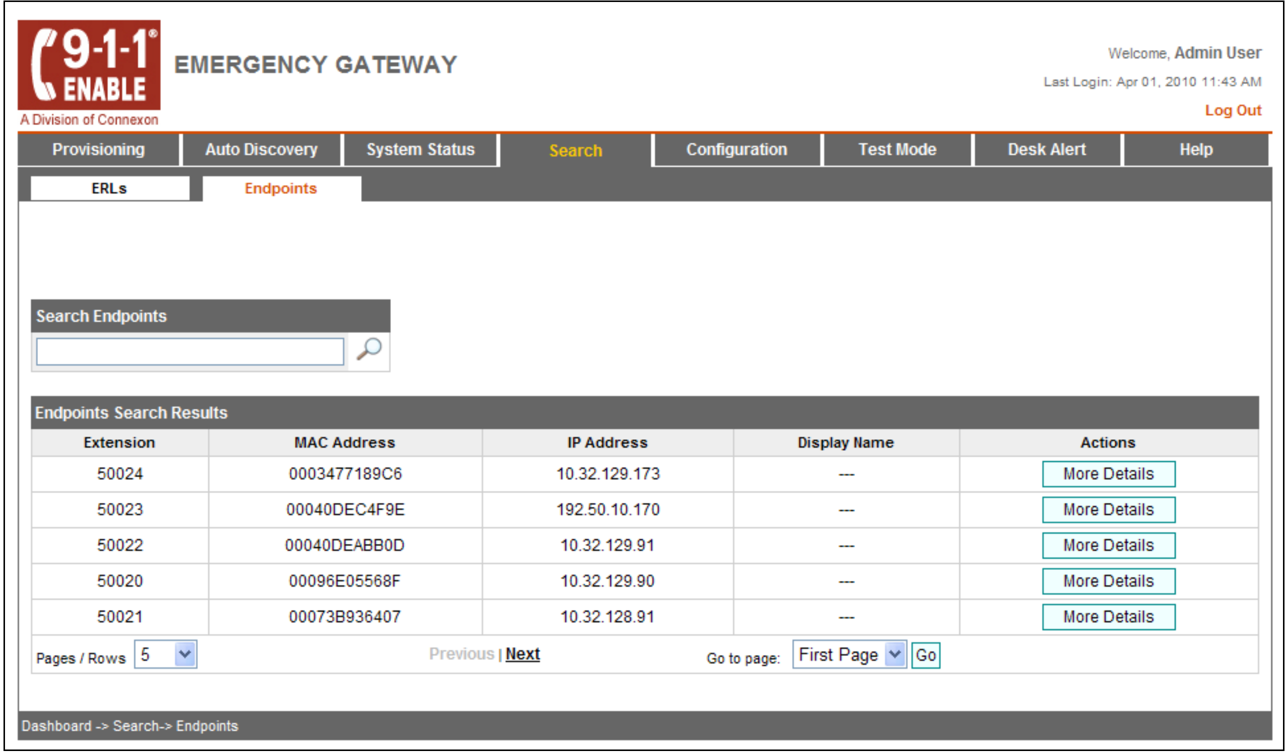
ERLs Search Results

Default ERL ID	Address	Local Gateway Enabled	Direct Call Delivery	Actions
LOC1	211, MT. AIRY ROAD, BASKING RIDGE, NJ, 07920	No	No	More Details
LOC2	233, MT. AIRY ROAD, BASKING RIDGE, NJ, 07920	No	No	More Details
LOC3	307, MIDDLETOWN-LINCROFT ROAD, LINCROFT, NJ, 07738	No	No	More Details

Pages / Rows 5
Previous | Next
Go to page: 1 Go
Dashboard -> Search-> ERLs
Copyright 2010 © 911enable.com is a division of ConneXon Telecom inc.

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

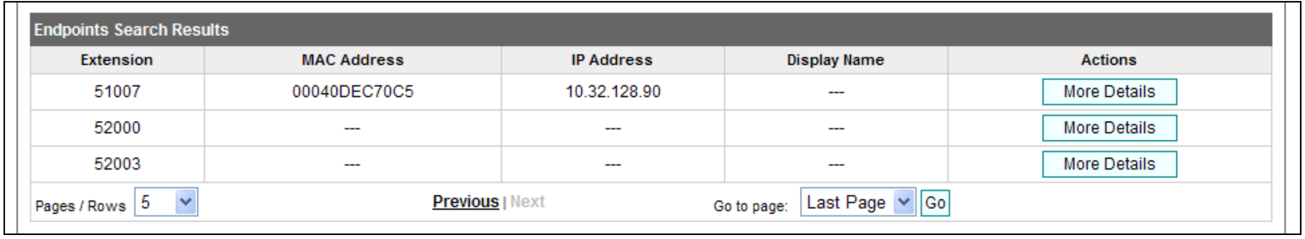
Page 1:



Endpoints Search Results

Extension	MAC Address	IP Address	Display Name	Actions
50024	0003477189C6	10.32.129.173	---	More Details
50023	00040DEC4F9E	192.50.10.170	---	More Details
50022	00040DEABB0D	10.32.129.91	---	More Details
50020	00096E05568F	10.32.129.90	---	More Details
50021	00073B936407	10.32.128.91	---	More Details

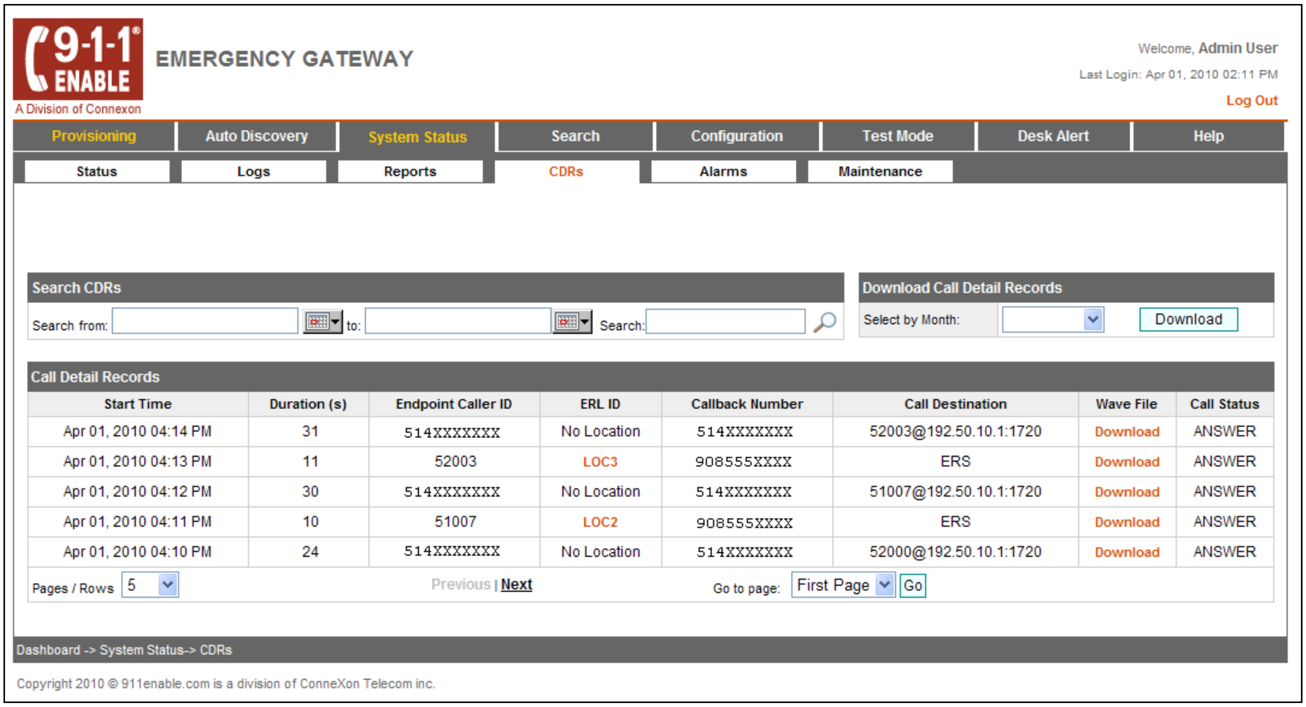
Page 2:



Endpoints Search Results

Extension	MAC Address	IP Address	Display Name	Actions
51007	00040DEC70C5	10.32.128.90	---	More Details
52000	---	---	---	More Details
52003	---	---	---	More Details

- 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.



Call Detail Records

Start Time	Duration (s)	Endpoint Caller ID	ERL ID	Callback Number	Call Destination	Wave File	Call Status
Apr 01, 2010 04:14 PM	31	514XXXXXXX	No Location	514XXXXXXX	52003@192.50.10.1:1720	Download	ANSWER
Apr 01, 2010 04:13 PM	11	52003	LOC3	908555XXXX	ERS	Download	ANSWER
Apr 01, 2010 04:12 PM	30	514XXXXXXX	No Location	514XXXXXXX	51007@192.50.10.1:1720	Download	ANSWER
Apr 01, 2010 04:11 PM	10	51007	LOC2	908555XXXX	ERS	Download	ANSWER
Apr 01, 2010 04:10 PM	24	514XXXXXXX	No Location	514XXXXXXX	52000@192.50.10.1:1720	Download	ANSWER

Pages / Rows 5
Previous | Next
Go to page: First Page Go
Dashboard -> System Status-> CDRs
Copyright 2010 © 911enable.com is a division of ConneXon Telecom inc.

9. Conclusion

911 Enable Emergency Gateway and Emergency Routing Service passed compliance testing. These Application Notes describe the procedures required to configure the connectivity between Avaya Aura® Session Manager and the 911 Enable equipment and service as shown in **Figure 1**.

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 6.2, Document 03-3005089, Issue 7.0, December 2012
[2] Administering Avaya Aura® Session Manager, Release 6.2, Document 03-603324, July 2012
[3] 911Enable Emergency Gateway System Guide 2.6.
[4] ESL Configuration Guide Rev. A, February 15, 2010.

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.