Avaya Solution & Interoperability Test Lab

Application Notes for Configuring 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Session Manager 6.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the 911 Enable Emergency Gateway and Emergency Routing Service with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Session Manager 6.0.

The 911 Enable Emergency Gateway and Emergency Routing Service offers an E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. Communication 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 various endpoint types 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) and Emergency Routing Service (ERS) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The 911 Enable Emergency Gateway and Emergency Routing Service offers an E911 call routing and location provisioning solution for enterprises using both legacy and IP phone deployments. Communication 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 various endpoint types connected to different network equipment to verify that their location and callback number could be properly determined.

1.1. 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 H.323 and SIP Telephones that support the PUSH API.
- Layer 3 discovery of Avaya IP one-X® Communicator (H323 and SIP) 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, calls were routed back via Session Manager to Communication Manager routed emergency calls to the ECRC via the PSTN.
- If the primary ERS was not available, the EGW routed emergency calls to the secondary ERS.
- If the primary and secondary ERS were not available, the EGW routed emergency calls to the ECRC via Session Manager and Communication Manager.
- Two Communication Managers were used to make sure that Layer 2 discovery was done properly by the EGW. Additionally, if same IP phone extension was configured on both Communication Managers, it was verified that the callback from PSAP is routed to the correct Communication Manager extension.

See **Section 8** for complete test results and any observations or limitations.

1.2. Support

For technical support on the EGW, contact 911 Enable at www.911enable.com.

2. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the 911 Enable Emergency Routing Service (ERS) via the 911 Enable Emergency Gateway (EGW). The ERS can send calls to the Public Service Answering Point (PSAP) or to the ECRC.

Located at the enterprise site is a pair of Avaya S8800 Servers running Communication Manager using an Avaya G650 Media Gateway. Session Manager is also present at the enterprise to support the SIP endpoints at the enterprise and provide routing between Communication Manager and EGW using SIP Trunks. Endpoints include Avaya 96xx Series IP Telephones (H.323 and SIP), Avaya 46xx Series IP Telephones (H.323), an Avaya IP Avaya one-X® Communicator (H.323 and SIP), an Avaya 6408D Digital Telephone, and an Avaya 6211 Analog Telephone. These endpoints were connected to two different Extreme models (x250p-24t and 400-24p) and Avaya C364T-PWR switches. An ISDN-PRI trunk connects the Avaya Media Gateway to the PSTN.

At the edge of the enterprise resides a redundant pair of EGWs. Each EGW connects to the Session Manager via a SIP trunk. All 911 emergency calls from the enterprise are routed to EGW. If the primary EGW is unavailable then Session Manager will route the emergency call to the secondary EGW.

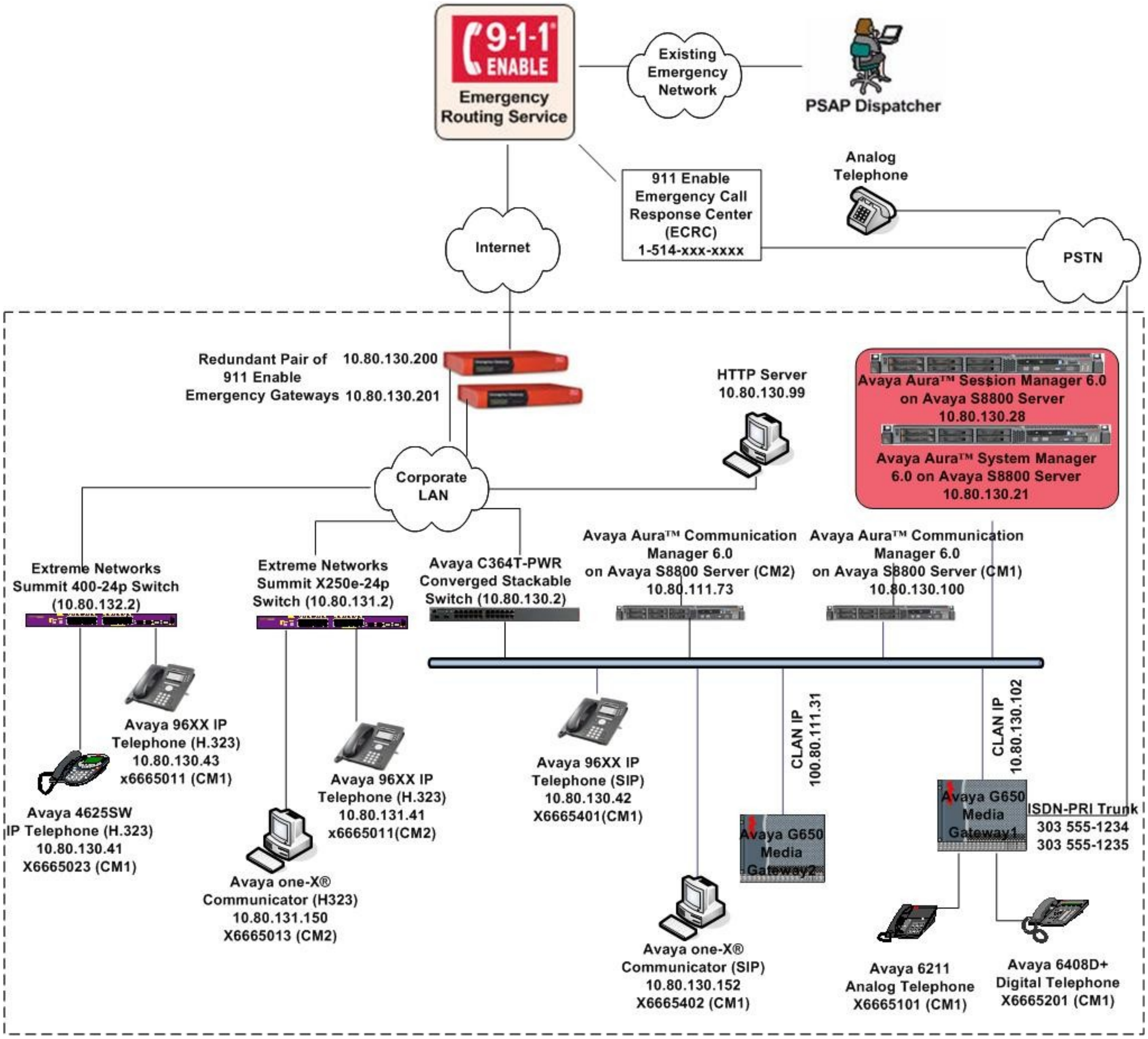


Figure 1: Test Configuration

The endpoints in **Figure 1** were divided into 3 locations. The first location, provisioned as LOC1, includes extensions 6665101 (Analog), 6665201 (Digital), 6665401 (SIP Deskphone) and 6665402 (SIP one-X Communicator). The second location, provisioned as LOC2, includes extensions 6665011 (H323) and 6665013 (H323 one-X Communicator). The last location, provisioned as LOC3, includes extension 6665011 (H323) 6665023 (H323).

For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes. Instead, some of the digits in these values have been replaced with an "x" to represent any value. An example is the ECRC phone number is **Figure 1**.

2.1. Auto-Discovery of Endpoints

The EGW attempts to auto discover the presence and location of Avaya 4600 and 9600 Series H.323 and SIP Telephones by correlating data obtained through two mechanisms. 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 this reference configuration, three different types of layer 2 switches were used. Endpoints connected to the Extreme Networks Summit X250e-24t and 400-24p switches and Avaya C364T-PWR Converged Stackable Switch were automatically discovered. The data obtained from layer 2 discovery includes the MAC address of the device connected to each port of the switch. 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 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 presence and location of the Avaya one-X® Communicator users are done 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 PC where Avaya one-X® Communicator is installed.

All digital and analog endpoints must be manually provisioned.

Note: All switches are not capable of doing layer 2 discovery. For the switches which do not support the layer 2 discovery, endpoints have to be manually provisioned in the EGW.

2.2. 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 temporary 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 this compliance test, duplicate extensions on two different Communication Managers needed to be assigned a separate DID as EGW does not specify the domain from where the 911 call was originated. For all other extensions a single temporary DID was used for CBN.

2.3. 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 → Communication Manager → 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 → Communication Manager → Session Manager → EGW → Session Manager → Communication 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 → Communication Manager → Session Manager → Communication 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 Communication Manager reroutes the call out the PSTN. For the compliance test, the call flow was from User Extension → Communication Manager → Session Manager → EGW (rejects the call), then the call is rerouted from EGW → Session Manager → Communication 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 → Communication Manager → 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 Communication Manager. The call flows from User Extension → Communication Manager → Session Manager → EGW followed by EGW → Session Manager → Communication 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 → Communication Manager → Session Manager →EGW (no response), then the call is rerouted by Session Manager → Communication Manager → PSTN → ECRC → PSAP. The callback call flows would be the same as the callback call flows described in scenario 2 above.

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with patch 18444
Avaya G650 Media Gateway	
Avaya S8800 Server	Avaya Aura® System Manager 6.0 (6.0.0.0.556-3.0.6.1)
Avaya S8800 Server	Avaya Aura® Session Manager 6.0 (6.0.0.0.600020)
Avaya 4610SW IP Telephone (H.323)	2.9.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X Deskphone Edition 3.11
Avaya 9620 IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.5
Avaya one-X® Communicator (SIP and H323)	6.0.0.26
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
911 Enable Emergency Gateway	3.1
911 Enable E911 Softphone Locator Software	1.2
911 Enable Emergency Routing Service	2.11

4. Configure Avaya Aura® Session Manager

These Application Notes assume that basic administration on System Manager and Session Manager has already been performed. Consult **[1]** and **[2]** for further details if necessary. Configuration of Session Manager is performed from System Manager. To invoke the System Manager Common Console, launch a web browser, enter https://<*IP address of System Manager server*>/SMGR as the URL, and log in with the appropriate credentials.

4.1. Background

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as "SIP Entities" and the connections/trunks between Session Manager and those components are represented as "Entity Links". Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely Avaya Aura® System Manager.

When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as "Adaptations", are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of "normalizing" the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed "Dial Patterns", and determines the destination SIP Entities based on "Routing Policies" specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

4.2. Routing Policies

Routing Policies define how Session Manager routes calls between SIP network elements. Routing Policies are dependent on the administration of several inter-related items:

- SIP Entities – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- Entity Links – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- SIP Domains – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined SIP proxy or one discovered through DNS).
- Locations – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.

- Adaptations – Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. For example, an AT&T-specific Adaptation is used in these Application Notes to remove SIP History-Info headers from SIP messages sent to the AT&T IP Flexible Reach service network. As another example, basic "Digit Conversion" Adaptations are used in this reference configuration to convert digit strings in "destination" (e.g., Request-URI) and "origination" (e.g. P-Asserted Identity) type headers of SIP messages sent to and received from SIP Entities.
- Dial Patterns – A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one[1] of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- Time Ranges – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. In the reference configuration no restrictions were placed on calling times.

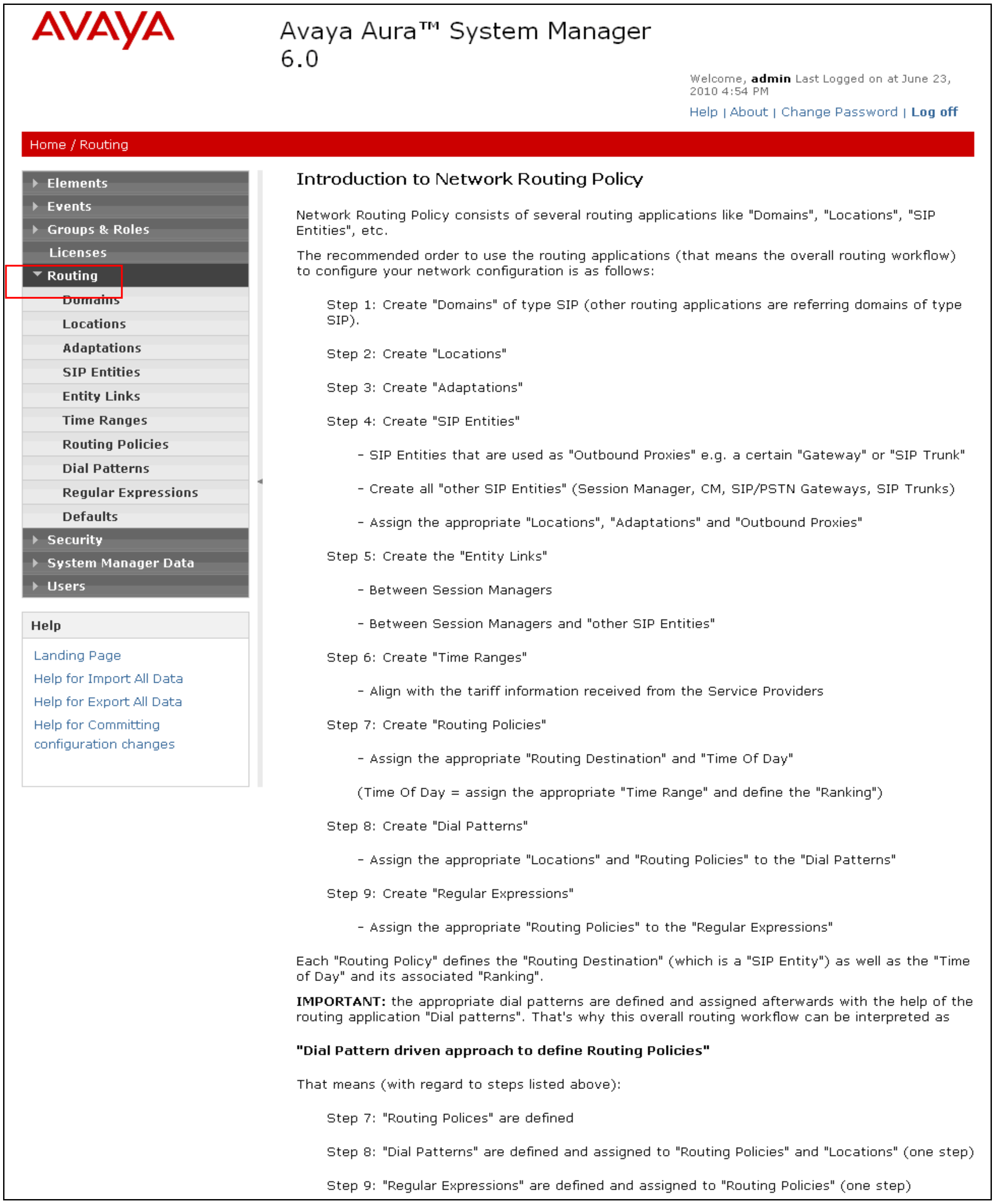
The general strategy employed in this reference configuration with regard to Called Party Number manipulation and matching, and call routing is as follows:

- Use common number formats and uniform numbers in matching called party numbers for routing decisions.
- On ingress to Session Manager, apply any called party number modifications necessary to "normalize" the number to a common format or uniform number as defined in the Dial Patterns.
- On egress from SM, apply any called party number modifications necessary to conform to the expectations of the next-hop SIP Entity. For example, on egress from Session Manager to Communication Manager, modify the called party number such that the number is consistent with the dial plan on Communication Manager.

Of course, the items above are just several of many possible strategies that can be implemented with Session Manager.

---

[1] The Routing Policy in effect at that time with highest ranking is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

Step	Description
1.	**Network Routing Policy** To view the sequenced steps required for configuring network routing policies, click on "Routing" in the left pane of the System Manager Common Console. 

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

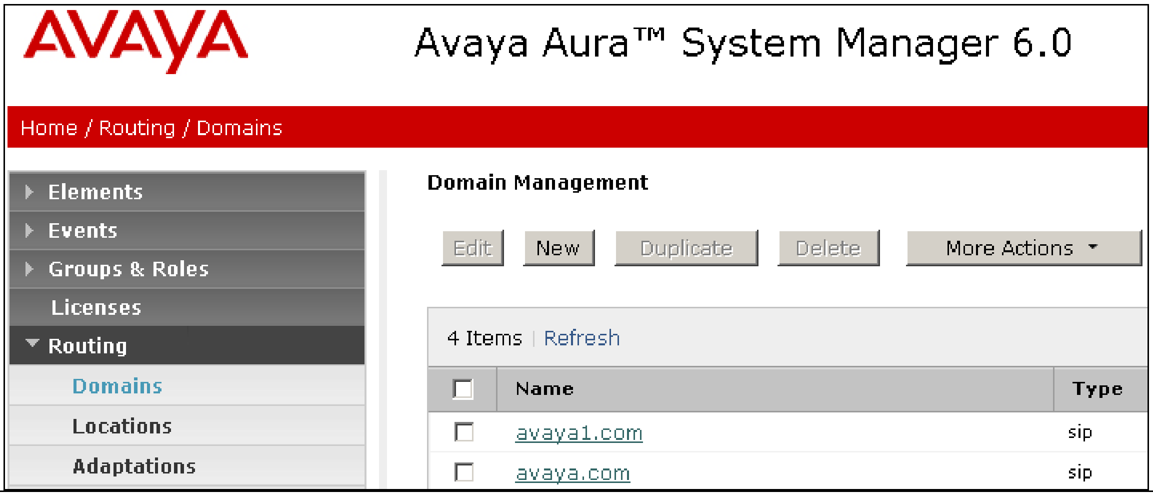
Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

SIP Domains

The following screen displays the two domains (***avaya.com*** and ***avaya1.com***) configured for this compliance testing.

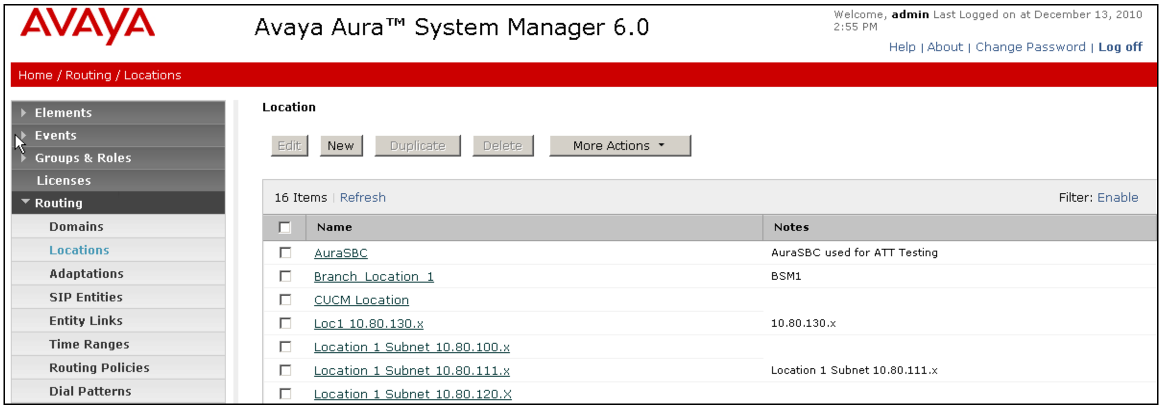


<table>
<tr><th>☐</th><th>Name</th><th>Type</th></tr>
<tr><td>☐</td><td>avaya1.com</td><td>sip</td></tr>
<tr><td>☐</td><td>avaya.com</td><td>sip</td></tr>
</table>

</td></tr>
<tr><td>3.</td><td>

Locations

The following screen displays the locations (**Loc1 10.80.130.x**, **Location 1 Subnet 10.80.120.x**, **Location 1 Subnet 10.80.111.x**) configured for this compliance testing.



<table>
<tr><th>☐</th><th>Name</th><th>Notes</th></tr>
<tr><td>☐</td><td>AuraSBC</td><td>AuraSBC used for ATT Testing</td></tr>
<tr><td>☐</td><td>Branch_Location_1</td><td>BSM1</td></tr>
<tr><td>☐</td><td>CUCM Location</td><td></td></tr>
<tr><td>☐</td><td>Loc1 10.80.130.x</td><td>10.80.130.x</td></tr>
<tr><td>☐</td><td>Location 1 Subnet 10.80.100.x</td><td></td></tr>
<tr><td>☐</td><td>Location 1 Subnet 10.80.111.x</td><td>Location 1 Subnet 10.80.111.x</td></tr>
<tr><td>☐</td><td>Location 1 Subnet 10.80.120.X</td><td></td></tr>
</table>

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

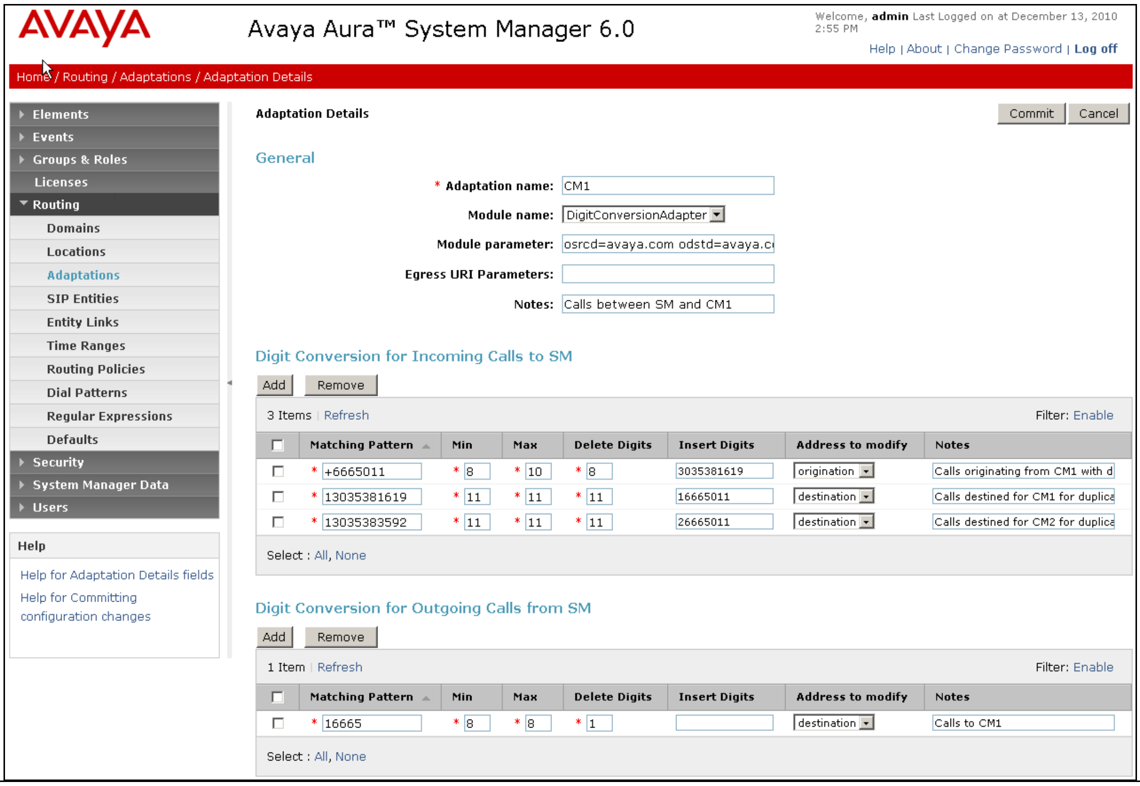
Step	Description
4.	**Adaptations for calls to first Communication Manager**

The following screen displays the adaptation used for calls between Session Manager and first Communication Manager.

- **Adaptation name** – Any descriptive string
- **Module name** - Selected ***DigitConversionAdapter*** from the drop-down list
- **Module parameter** – Parameter ***osrcd*** replaces any domain/IP Address in the PAI header with ***avaya.com*** for outbound request and parameter ***odstd*** replaces any domain/IP Address in the Request URI with ***avaya.com***.
- In the **Digit Conversion for Incoming Calls to SM** section,
  a) Matching pattern ***+6665011*** was for the calls coming from Communication Manager for a duplicate extension configured in both Communication Managers. A unique DID was assigned for this extension so that EGW is able to present the right DID for the call back from PSAP attendant.
  b) Matching pattern ***13035381619*** was for the callback from PSAP attendant destined for the duplicate extension on first Communication Manager
  c) Matching pattern ***13035383592*** was for the callback from PSAP attendant destined for the duplicate extension on second Communication Manager

Note: All the callbacks from PSAP attendant terminated on first Communication Manager as there was only one PRI trunk configured for this compliance testing. All the callbacks were routed to the proper Communication Manager by the Session Manager.

- In the **Digit Conversion for Outgoing Calls from SM** section, only one entry was configured to route the duplicate extensions call to the first Communication Manager.



Adaptation Details

General

* Adaptation name: CM1

Module name: DigitConversionAdapter

Module parameter: osrcd=avaya.com odstd=avaya.c

Egress URI Parameters:

Notes: Calls between SM and CM1

Digit Conversion for Incoming Calls to SM

3 Items

☐	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* +6665011	* 8	* 10	* 8	3035381619	origination	Calls originating from CM1 with d
☐	* 13035381619	* 11	* 11	* 11	16665011	destination	Calls destined for CM1 for duplica
☐	* 13035383592	* 11	* 11	* 11	26665011	destination	Calls destined for CM2 for duplica

Digit Conversion for Outgoing Calls from SM

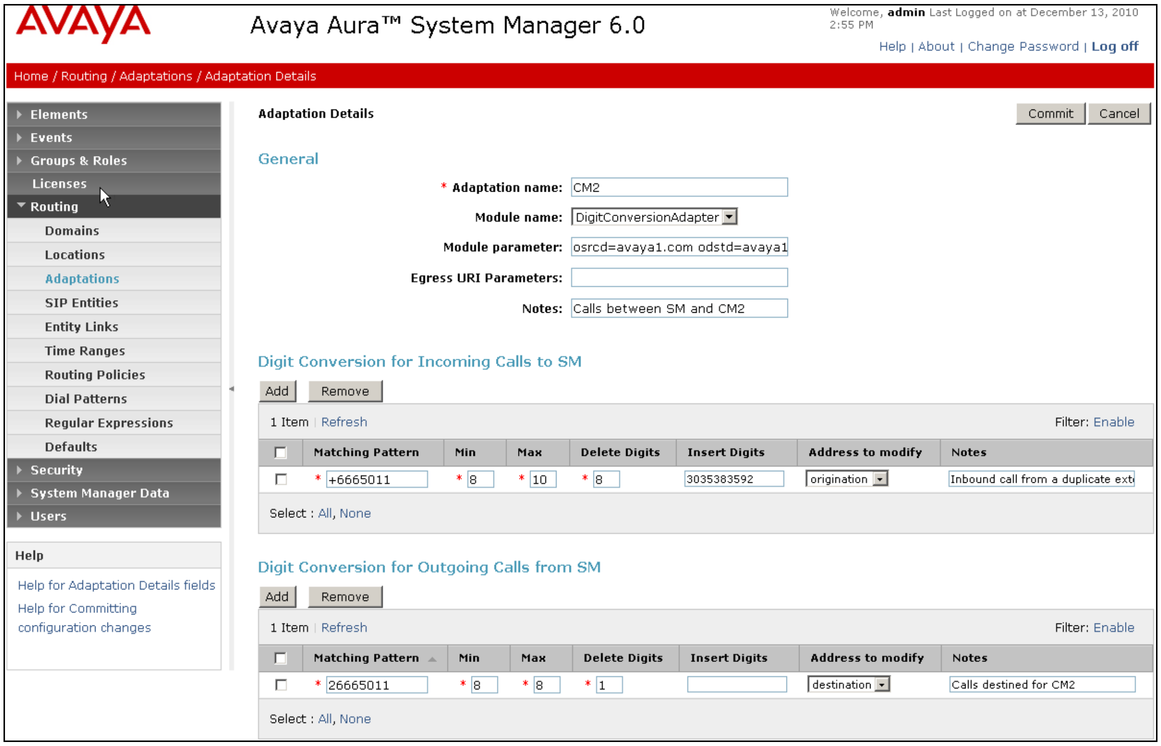
1 Item

☐	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 16665	* 8	* 8	* 1		destination	Calls to CM1

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

Adaptations – Continued

The following screen displays the adaptations used for second Communication Manager.



Adaptation Details

General

* Adaptation name: CM2

Module name: DigitConversionAdapter

Module parameter: osrcd=avaya1.com odstd=avaya1

Egress URI Parameters:

Notes: Calls between SM and CM2

Digit Conversion for Incoming Calls to SM

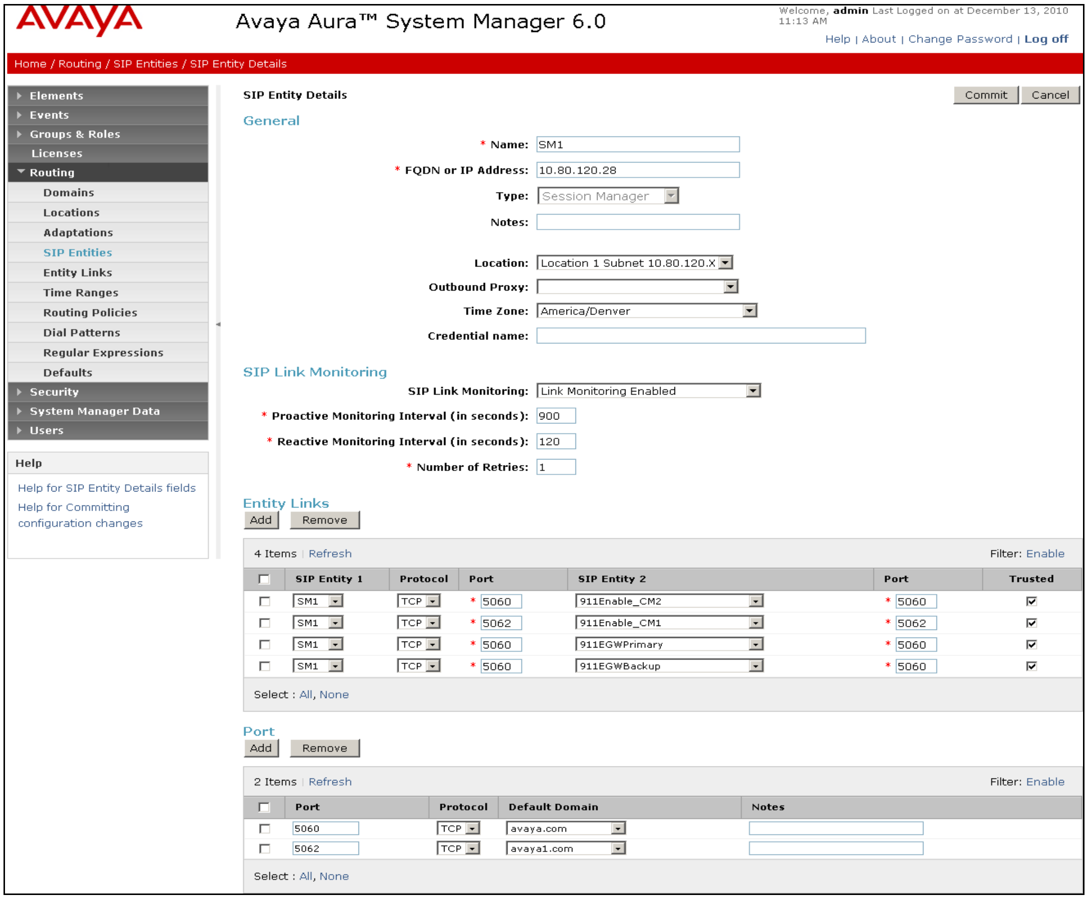
<table>
<tr><th>☐</th><th>Matching Pattern</th><th>Min</th><th>Max</th><th>Delete Digits</th><th>Insert Digits</th><th>Address to modify</th><th>Notes</th></tr>
<tr><td>☐</td><td>* +6665011</td><td>* 8</td><td>* 10</td><td>* 8</td><td>3035383592</td><td>origination</td><td>Inbound call from a duplicate ext</td></tr>
</table>

Digit Conversion for Outgoing Calls from SM

<table>
<tr><th>☐</th><th>Matching Pattern</th><th>Min</th><th>Max</th><th>Delete Digits</th><th>Insert Digits</th><th>Address to modify</th><th>Notes</th></tr>
<tr><td>☐</td><td>* 26665011</td><td>* 8</td><td>* 8</td><td>* 1</td><td></td><td>destination</td><td>Calls destined for CM2</td></tr>
</table>

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

Step	Description
6.	**SIP Entity – Session Manager** The following screen shot shows the Session Manager entry configured for this compliance test: • **Name** – Any descriptive name • **FQDN or IP Address** –IP Address of the Network Interface for the Session Manager • **Type** – Selected ***Session Manager*** from the drop-down list • **Location** – Selected from the list of locations configure in **Step 3** • **Time Zone** – Selected the time zone from a drop-down list • In the SIP Link Monitoring section, **SIP Link Monitoring** field was set to ***Link Monitoring Enabled*** • The **Entity Links** section displays the links configured for this compliance testing. Entity links are displayed only after the links are established. The entity link configuration is shown in **Steps 11 - 14**. Additional entity links can be defined upon configuration of additional entities. • The **Port** section displays the ports used for each protocol/domain configuration used for this compliance testing. Two separate domains (avaya.com and avaya1.com) were used for the two Communication Managers used for this compliance testing. Default Domain was selected from the configuration done in **Step 2**. Note that separate port numbers are required to handle separate domains.



SIP Entity Details

General

* Name: SM1
* FQDN or IP Address: 10.80.120.28
Type: Session Manager
Notes:
Location: Location 1 Subnet 10.80.120.X
Outbound Proxy:
Time Zone: America/Denver
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled
* Proactive Monitoring Interval (in seconds): 900
* Reactive Monitoring Interval (in seconds): 120
* Number of Retries: 1

Entity Links

4 Items

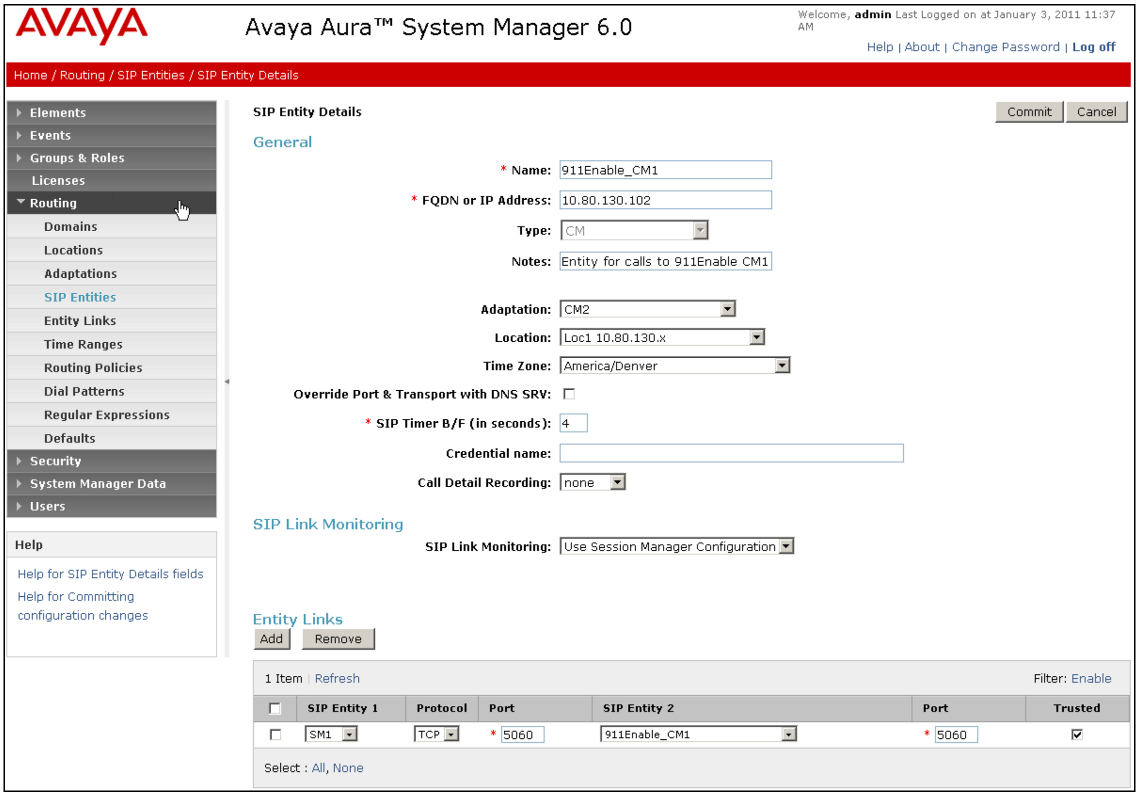
☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5060	911Enable_CM2	* 5060	☑
☐	SM1	TCP	* 5062	911Enable_CM1	* 5062	☑
☐	SM1	TCP	* 5060	911EGWPrimary	* 5060	☑
☐	SM1	TCP	* 5060	911EGWBackup	* 5060	☑

Port

2 Items

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5062	TCP	avaya1.com	

Step	Description
7.	**SIP Entity – Continued** The following screen shows the SIP Entity configured for the first Communication Manager along with the entity link to the Session Manager: • **Name** – Any descriptive name • **FQDN or IP Address** – IP address of the CLAN interface for the Communication Manager • **Type** – Selected CM from the drop-down list • **Adaptation** – Selected **CM1** from the drop-down list of adaptations configured in **Step 4** • **Location** - Selected from the drop-down list of locations configure in **Step 3** • **Time Zone** – Selected the time zone from a drop-down list • In the SIP Link Monitoring section, **SIP Link Monitoring** field was set to ***Use Session Manager Configuration*** • The **Entity Links** section displays the links configured for this compliance testing. Entity links are displayed only after the links are established. The entity link configuration is shown in **Step 11**



SIP Entity Details

General

* Name: 911Enable_CM1

* FQDN or IP Address: 10.80.130.102

Type: CM

Notes: Entity for calls to 911Enable CM1

Adaptation: CM2

Location: Loc1 10.80.130.x

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

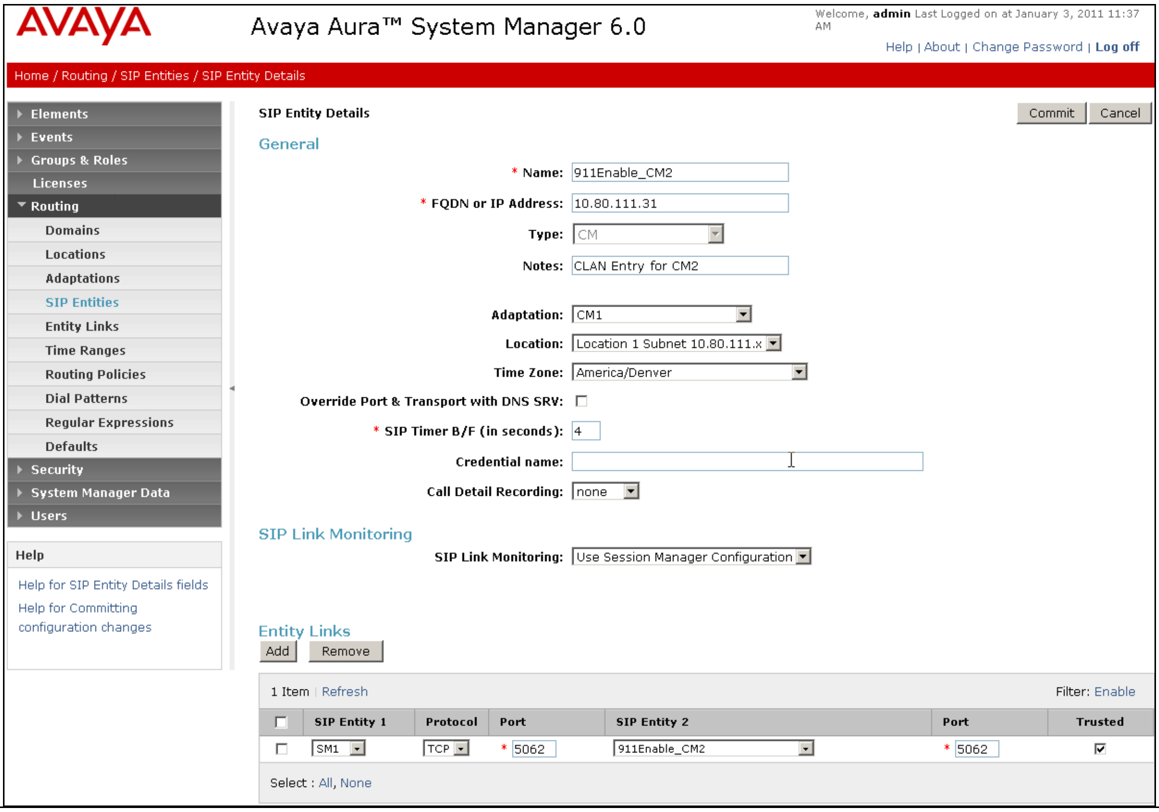
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5060	911Enable_CM1	* 5060	☑

Step	Description
8.	**SIP Entity – Continued** The following screen shows the SIP Entity configured for the second Communication Manager along with the entity link to the Session Manager. The entity link is displayed in **Step 12**. 

SIP Entity Details

General

* Name: 911Enable_CM2
* FQDN or IP Address: 10.80.111.31
Type: CM
Notes: CLAN Entry for CM2
Adaptation: CM1
Location: Location 1 Subnet 10.80.111.x
Time Zone: America/Denver
Override Port & Transport with DNS SRV: ☐
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

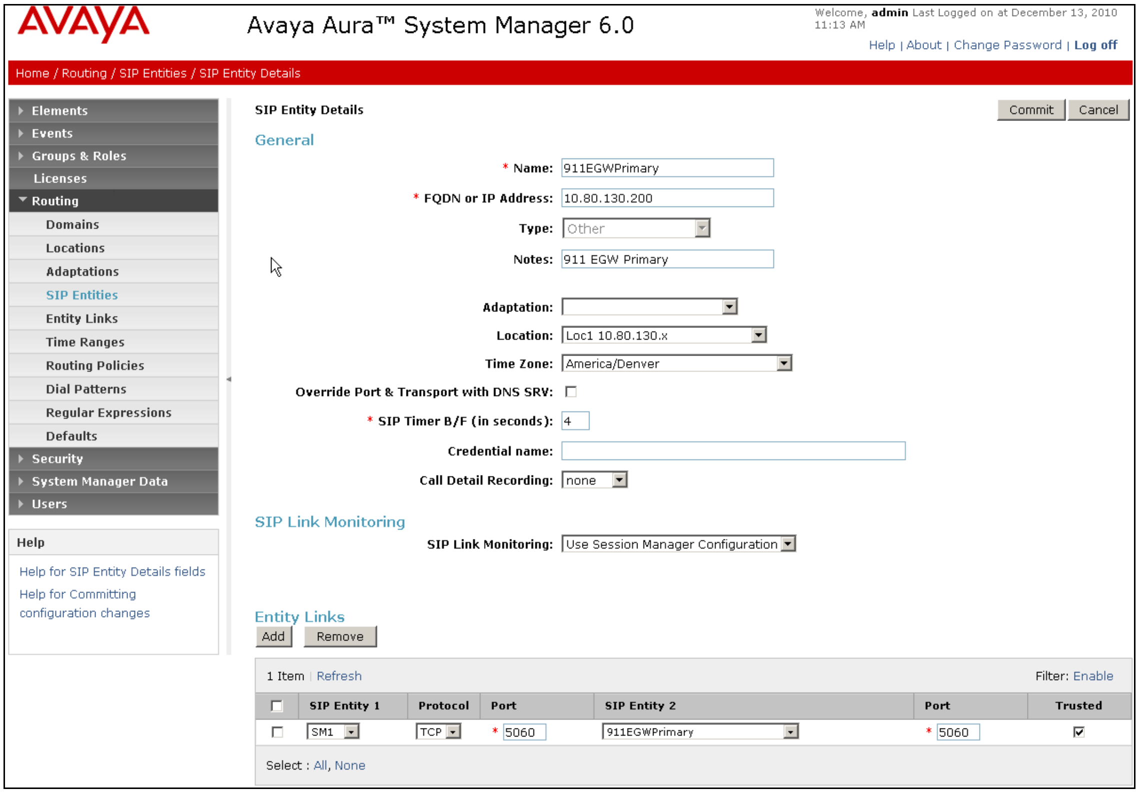
SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

1 Item

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5062	911Enable_CM2	* 5062	☑

Step	Description
9.	**SIP Entity – Continued** The following screen shows the SIP Entity configured for the primary EGW along with the entity link to the Session Manager. The entity link is displayed in **Step 13**. 

SIP Entity Details

General

* Name: 911EGWPrimary

* FQDN or IP Address: 10.80.130.200

Type: Other

Notes: 911 EGW Primary

Adaptation:

Location: Loc1 10.80.130.x

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

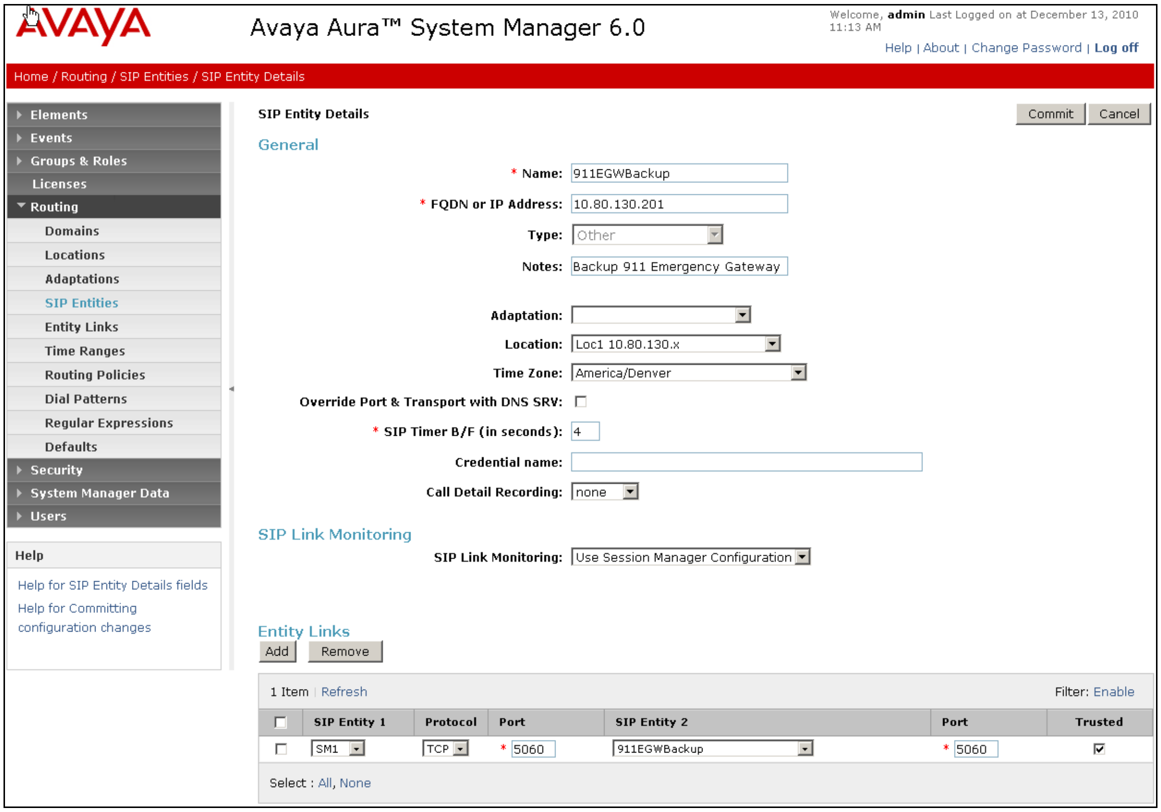
SIP Link Monitoring: Use Session Manager Configuration

Entity Links

1 Item

☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5060	911EGWPrimary	* 5060	☑

Select : All, None

Step	Description
10.	**SIP Entity – Continued** The following screen shows the SIP Entity configured for the backup EGW along with the entity link to the Session Manager. The entity link is displayed in **Step 14**. 

SIP Entity Details

General

* Name: 911EGWBackup

* FQDN or IP Address: 10.80.130.201

Type: Other

Notes: Backup 911 Emergency Gateway

Adaptation:

Location: Loc1 10.80.130.x

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

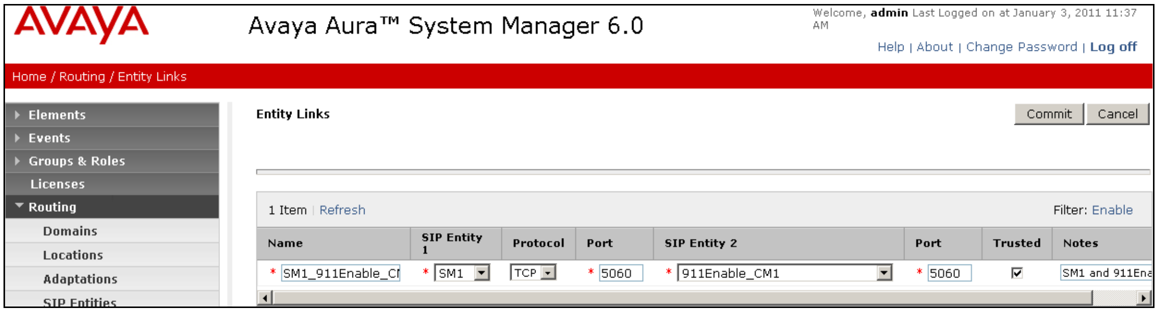
1 Item | Refresh Filter: Enable

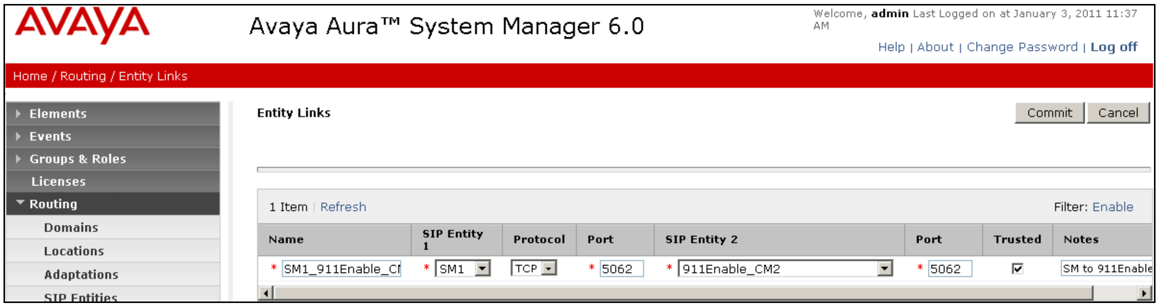
☐	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
☐	SM1	TCP	* 5060	911EGWBackup	* 5060	☑

Select : All, None

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>11.</td><td>
Entity Links
The following screen shows the SIP Entity Link configured between Session Manager and first Communication Manager. This link along with other links also appears in the screen shown in Step 6. In the left pane under Routing, click on “Entity Links”. On the Entity Links page, click on SM1-911Enable_CM1 entity (not shown) to display the screen below:

Name – Any descriptive name for the link between Session Manager and first Communication Manager
SIP Entity 1 – SIP entity link for Session Manager displayed in Step 6. SIP Entity 1 field always contain the Session Manager entity.
SIP Entity 1 Port – Set to <i>5060</i>
SIP Entity 2 –Selected the SIP Entity administered in Step 7 for the first Communication Manager
SIP Entity 2 Port – Set to <i>5060</i>
Trusted – A check in the box indicates that this is a trusted link
Protocol – Selected <i>TCP</i> from the drop-down list.



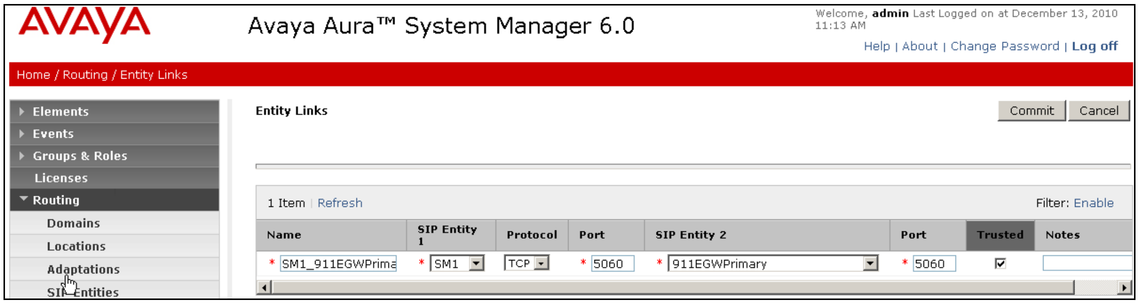
<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th><th>Notes</th></tr>
<tr><td>* SM1_911Enable_C</td><td>* SM1</td><td>TCP</td><td>* 5060</td><td>* 911Enable_CM1</td><td>* 5060</td><td>☑</td><td>SM1 and 911Ena</td></tr>
</table>
</td></tr>
<tr><td>12.</td><td>
Entity Links – Continued
The following screen shows the SIP Entity Link configured between Session Manager and second Communication Manager Entity displayed in Step 8.


<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th><th>Notes</th></tr>
<tr><td>* SM1_911Enable_C</td><td>* SM1</td><td>TCP</td><td>* 5062</td><td>* 911Enable_CM2</td><td>* 5062</td><td>☑</td><td>SM to 911Enable</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>13.</td><td>

Entity Links – Continued

The following screen shows the SIP Entity Link configured between Session Manager and primary EGW Entity displayed in **Step 9**.

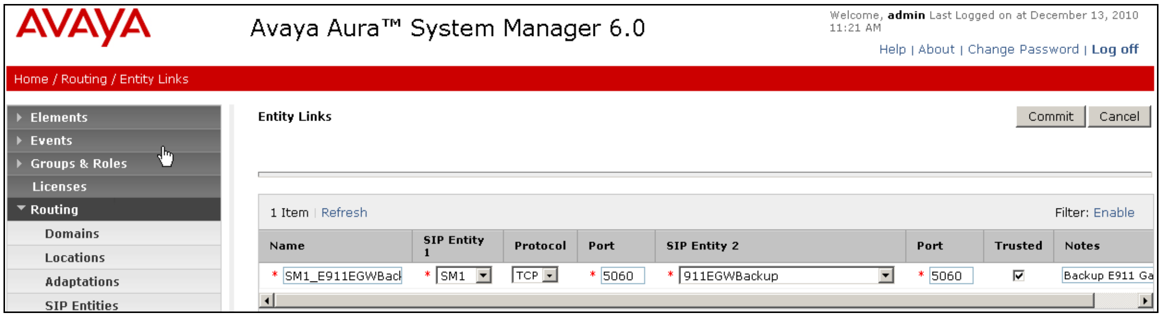


<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th><th>Notes</th></tr>
<tr><td>* SM1_911EGWPrima</td><td>* SM1</td><td>TCP</td><td>* 5060</td><td>* 911EGWPrimary</td><td>* 5060</td><td>☑</td><td></td></tr>
</table>

</td></tr>
<tr><td>14.</td><td>

Entity Links – Continued

The following screen shows the SIP Entity Link configured between Session Manager and backup EGW Entity displayed in **Step 10**.

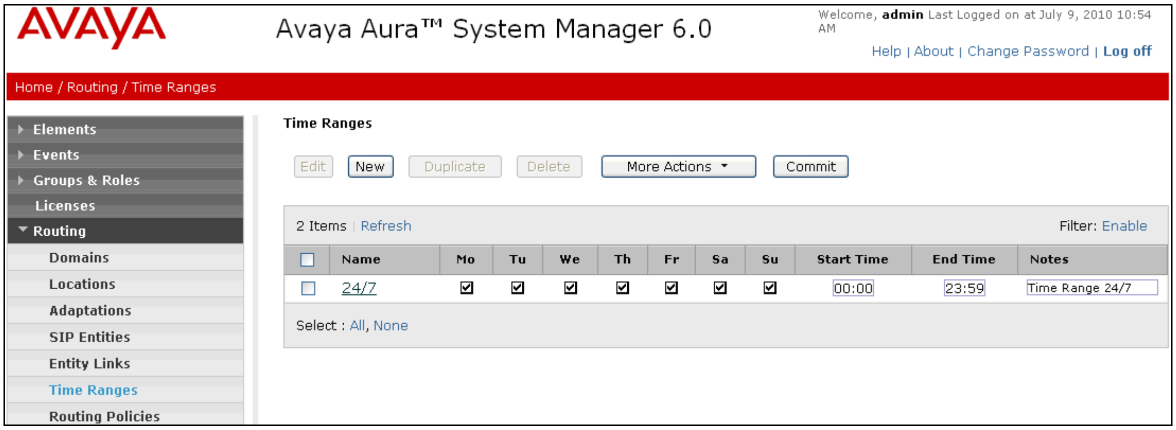


<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th><th>Notes</th></tr>
<tr><td>* SM1_E911EGWBac</td><td>* SM1</td><td>TCP</td><td>* 5060</td><td>* 911EGWBackup</td><td>* 5060</td><td>☑</td><td>Backup E911 Ga</td></tr>
</table>

</td></tr>
<tr><td>15.</td><td>

Time Ranges

The following screen displays the time range configured for this compliance testing. Additional time ranges can be entered if required.



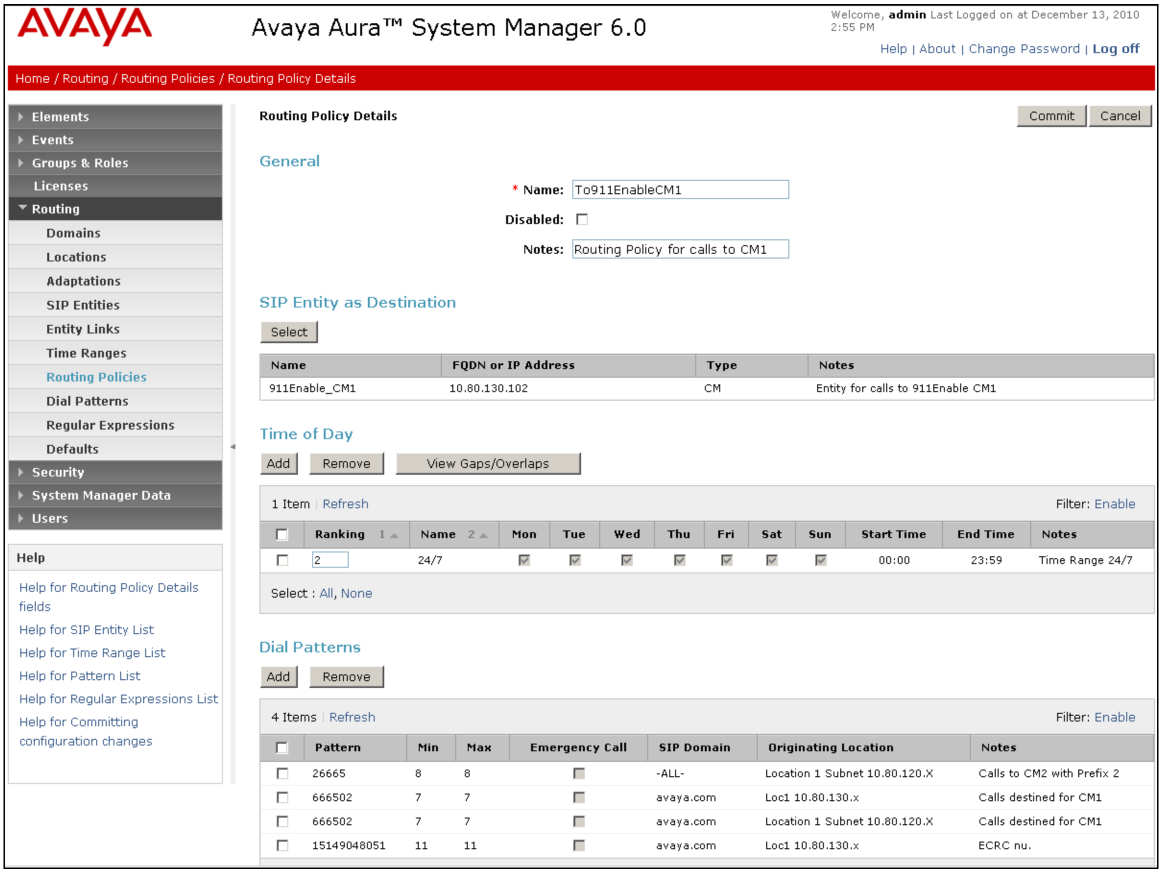
<table>
<tr><th>☐</th><th>Name</th><th>Mo</th><th>Tu</th><th>We</th><th>Th</th><th>Fr</th><th>Sa</th><th>Su</th><th>Start Time</th><th>End Time</th><th>Notes</th></tr>
<tr><td>☐</td><td>24/7</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>00:00</td><td>23:59</td><td>Time Range 24/7</td></tr>
</table>

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

Step	Description
16.	**Routing Policies Details**

The following screen displays the Routing Policy configured for calls to first Communication Manager:

- In the **General** section, a descriptive name for the policy was added along with notes in the optional **Notes** field
- In the **SIP Entity as Destination** section, SIP Entity configured in **Step 7** was selected
- In the **Time of Day** section, time range configured in **Step 15** was selected with **Ranking** field set to *2*. Ranking is used to set the order in which Session Manager looks at the routing policy to make a routing decision. A ranking of 0 indicates the highest priority.
- The **Dial Patterns** section displays the patterns configured for this compliance testing. Dial Patterns are displayed only after the pattern is configured as shown in **Steps 20 - 23**. Dial Patterns, once defined can be added or deleted from the **Routing Policy Details** page too.



Routing Policy Details

General

* Name: To911EnableCM1

Disabled: ☐

Notes: Routing Policy for calls to CM1

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
911Enable_CM1	10.80.130.102	CM	Entity for calls to 911Enable CM1

Time of Day

1 Item | Refresh Filter: Enable

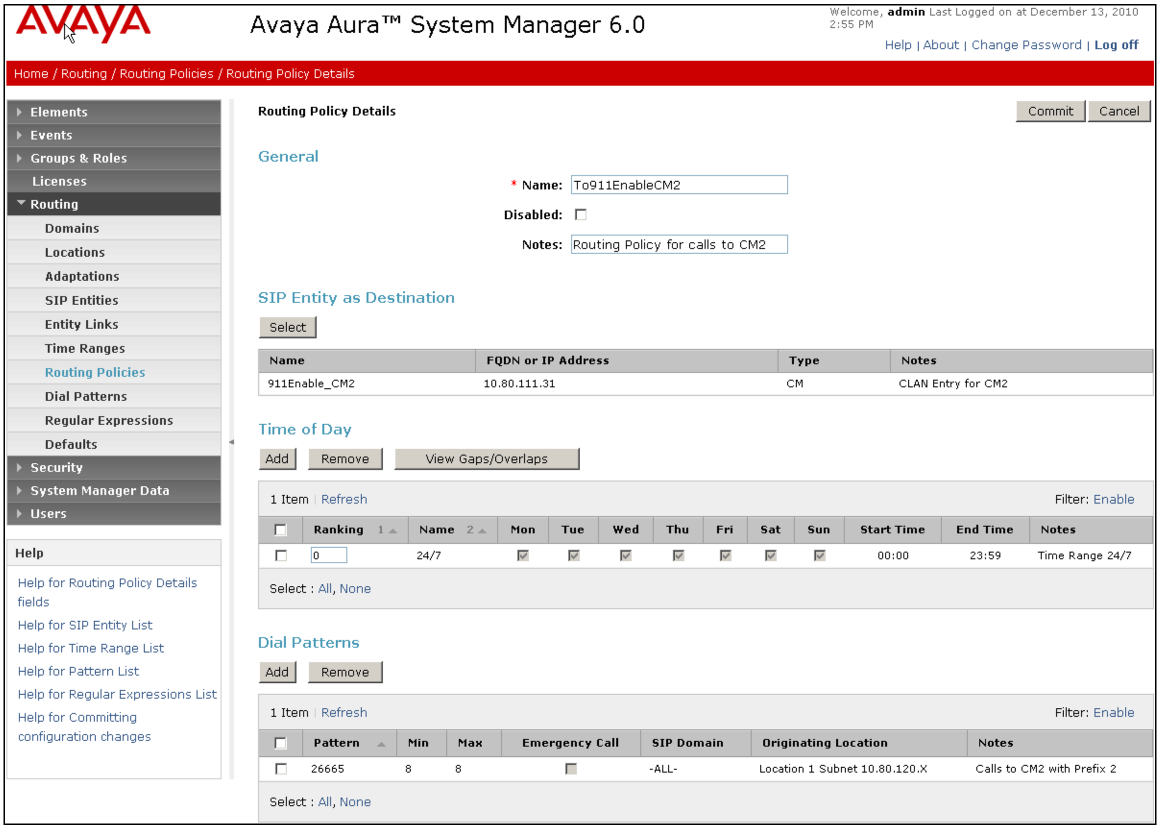
☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	2	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Dial Patterns

4 Items | Refresh Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	26665	8	8	☐	-ALL-	Location 1 Subnet 10.80.120.X	Calls to CM2 with Prefix 2
☐	666502	7	7	☐	avaya.com	Loc1 10.80.130.x	Calls destined for CM1
☐	666502	7	7	☐	avaya.com	Location 1 Subnet 10.80.120.X	Calls destined for CM1
☐	15149048051	11	11	☐	avaya.com	Loc1 10.80.130.x	ECRC nu.

Step	Description
17.	**Routing Policies Details - Continued** The following screen displays the Routing Policy and corresponding Dial Patterns configured for calls to second Communication Manager.



Routing Policy Details

General

* Name: To911EnableCM2

Disabled: ☐

Notes: Routing Policy for calls to CM2

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
911Enable_CM2	10.80.111.31	CM	CLAN Entry for CM2

Time of Day

1 Item | Refresh Filter: Enable

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

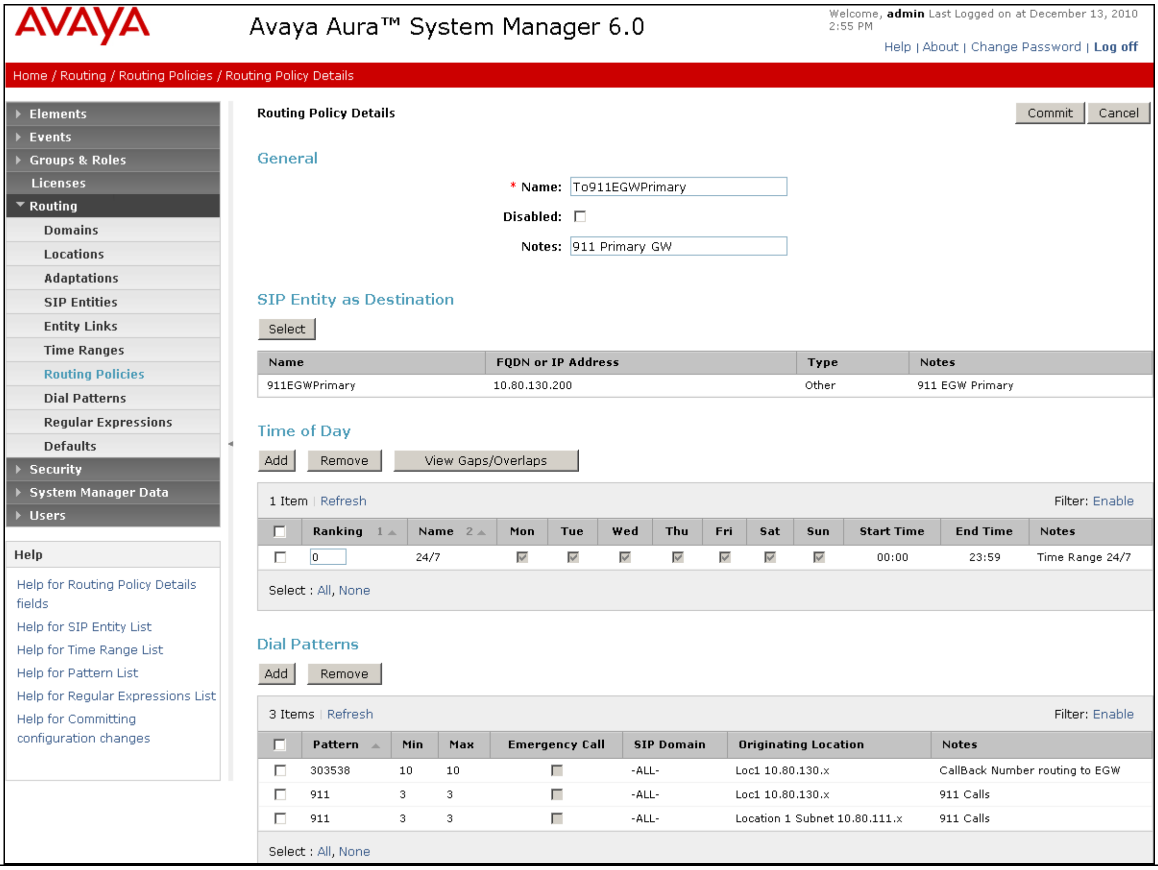
Select : All, None

Dial Patterns

1 Item | Refresh Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	26665	8	8	☐	-ALL-	Location 1 Subnet 10.80.120.X	Calls to CM2 with Prefix 2

Select : All, None

Step	Description
18.	**Routing Policies Details - Continued** The following screen displays the Routing Policy and corresponding Dial Patterns configured for calls to Primary EGW. 

Routing Policy Details

General

* Name: To911EGWPrimary

Disabled: ☐

Notes: 911 Primary GW

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
911EGWPrimary	10.80.130.200	Other	911 EGW Primary

Time of Day

1 Item | Refresh   Filter: Enable

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

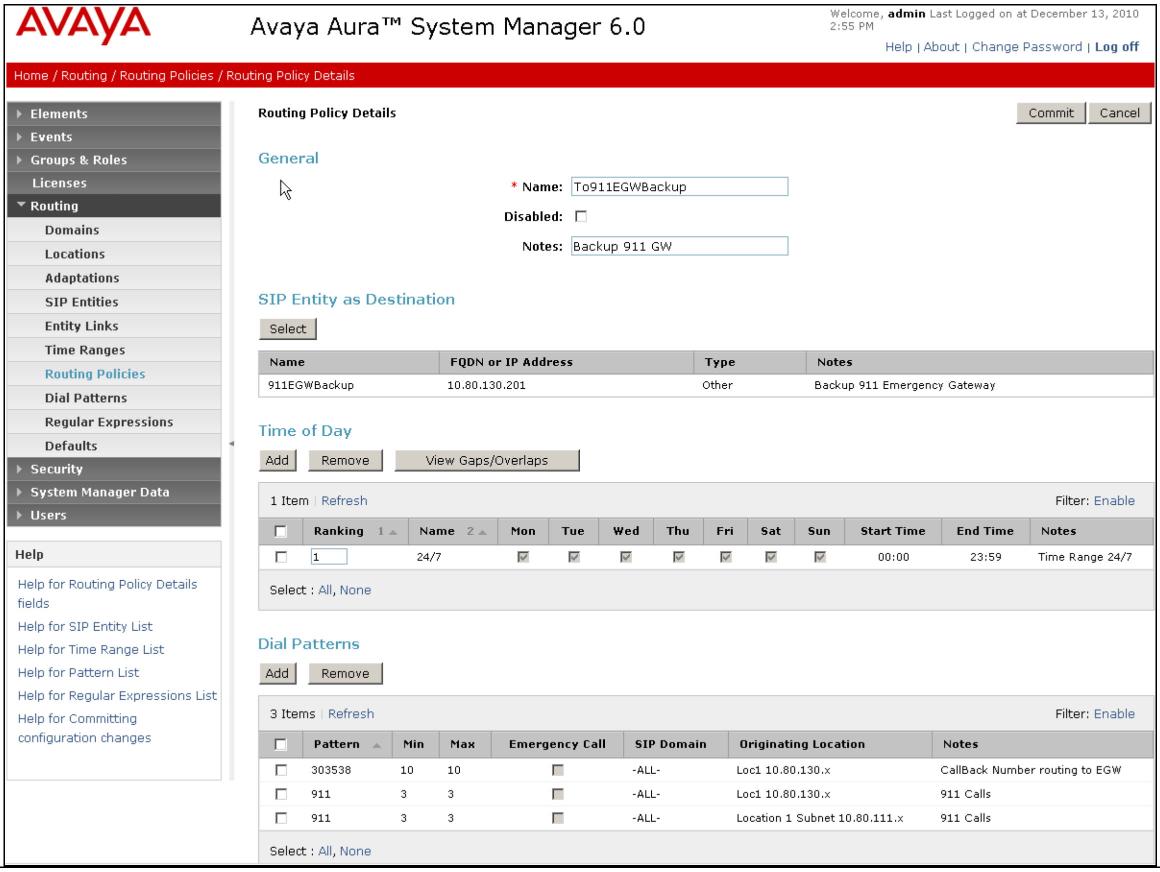
Select : All, None

Dial Patterns

3 Items | Refresh   Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	303538	10	10	☐	-ALL-	Loc1 10.80.130.x	CallBack Number routing to EGW
☐	911	3	3	☐	-ALL-	Loc1 10.80.130.x	911 Calls
☐	911	3	3	☐	-ALL-	Location 1 Subnet 10.80.111.x	911 Calls

Select : All, None

Step	Description
19.	**Routing Policies Details - Continued** The following screen displays the Routing Policy and corresponding Dial Patterns configured for calls to Backup EGW. 

Routing Policy Details

General

* Name: To911EGWBackup

Disabled: ☐

Notes: Backup 911 GW

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
911EGWBackup	10.80.130.201	Other	Backup 911 Emergency Gateway

Time of Day

1 Item | Refresh Filter: Enable

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

Select : All, None

Dial Patterns

3 Items | Refresh Filter: Enable

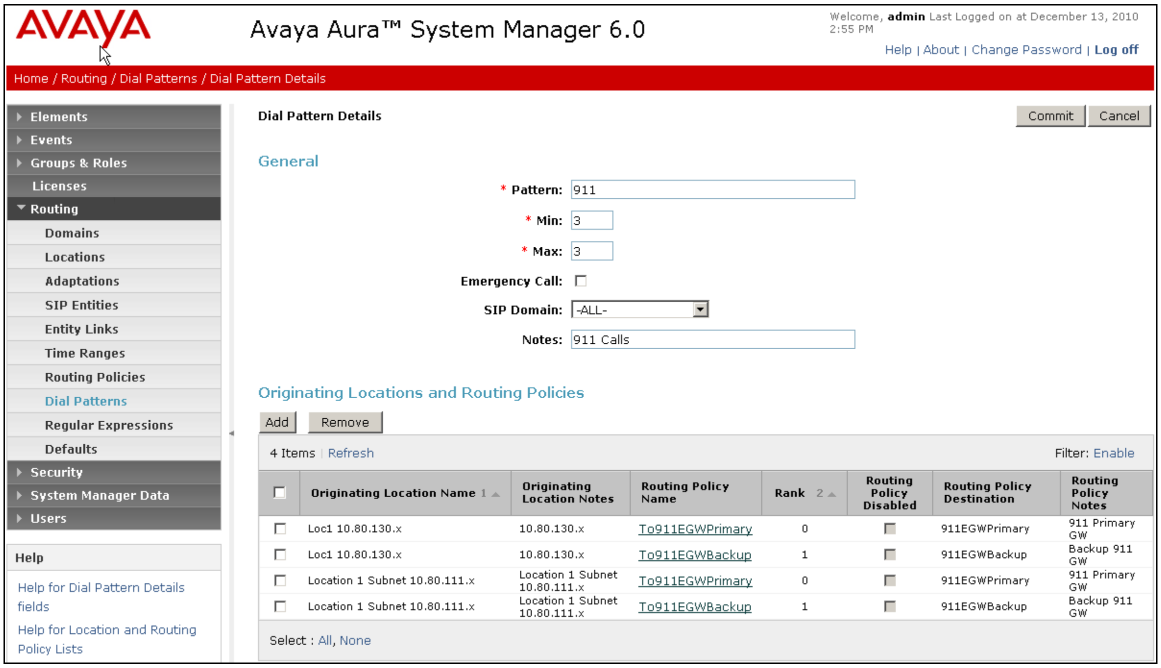
☐	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	303538	10	10	☐	-ALL-	Loc1 10.80.130.x	CallBack Number routing to EGW
☐	911	3	3	☐	-ALL-	Loc1 10.80.130.x	911 Calls
☐	911	3	3	☐	-ALL-	Location 1 Subnet 10.80.111.x	911 Calls

Select : All, None

Step | **Description**

20\. **Dial Patterns - 911**

The following screen displays the Dial Pattern for 911 calls along with the routing policy and originating location and destination of the calls. The 911 calls originate from the endpoints configured on the two Communication Managers and are routed to the primary or backup EGW.



Dial Pattern Details

General

* Pattern: 911

* Min: 3

* Max: 3

Emergency Call: ☐

SIP Domain: -ALL-

Notes: 911 Calls

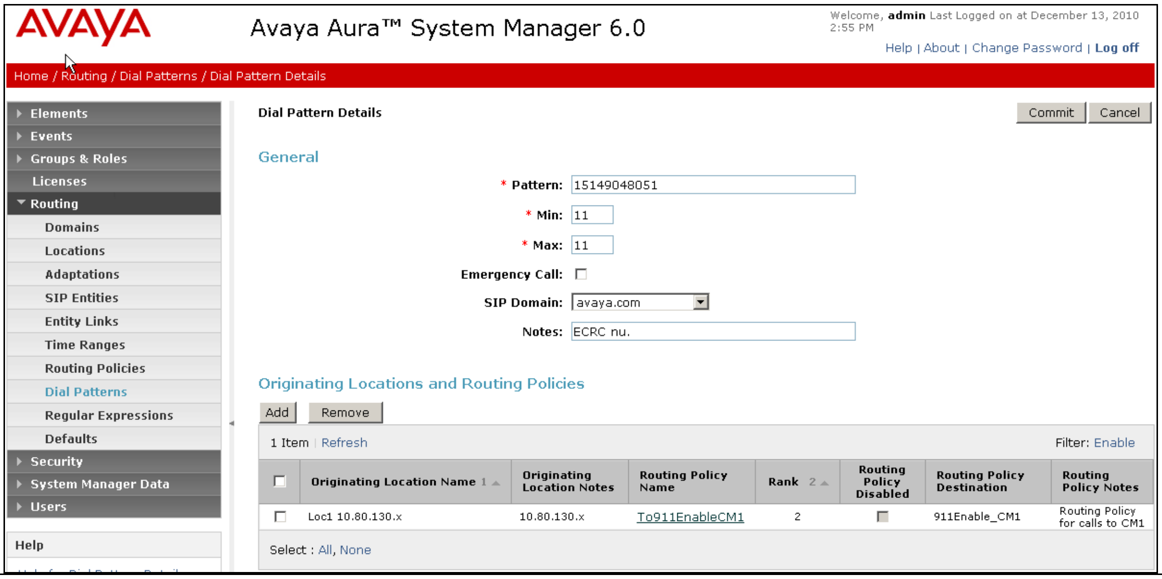
Originating Locations and Routing Policies

4 Items

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Loc1 10.80.130.x	10.80.130.x	To911EGWPrimary	0	☐	911EGWPrimary	911 Primary GW
☐	Loc1 10.80.130.x	10.80.130.x	To911EGWBackup	1	☐	911EGWBackup	Backup 911 GW
☐	Location 1 Subnet 10.80.111.x	Location 1 Subnet 10.80.111.x	To911EGWPrimary	0	☐	911EGWPrimary	911 Primary GW
☐	Location 1 Subnet 10.80.111.x	Location 1 Subnet 10.80.111.x	To911EGWBackup	1	☐	911EGWBackup	Backup 911 GW

21\. **Dial Patterns – Calls to ECRC**

The following screen displays the calls routed by EGW back to the Communication Manager to be routed over the PRI trunk to ECRC. This happens when the ERS service is down.



Dial Pattern Details

General

* Pattern: 15149048051

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes: ECRC nu.

Originating Locations and Routing Policies

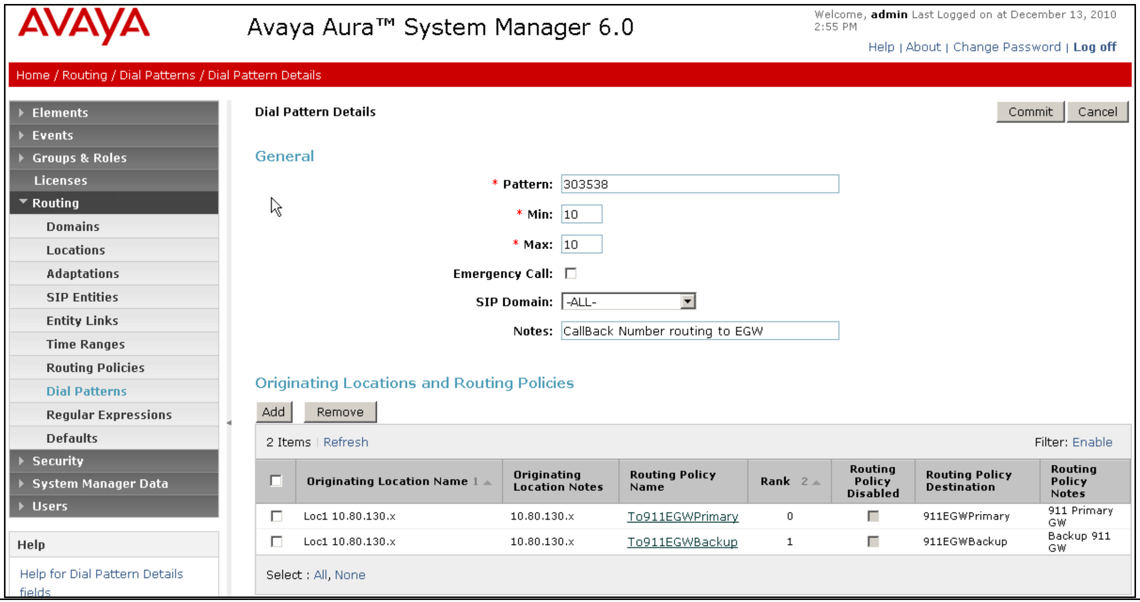
1 Item

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Loc1 10.80.130.x	10.80.130.x	To911EnableCM1	2	☐	911Enable_CM1	Routing Policy for calls to CM1

Step	Description

22. **Dial Patterns – Call back from ERS**

The following screen displays the Dial Pattern used to handle the calls received by the PSAP attendant. This call is routed to EGW which retrieves the extension from where the 911 call was originated.



Dial Pattern Details

General

* Pattern: 303538

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: CallBack Number routing to EGW

Originating Locations and Routing Policies

Add | Remove

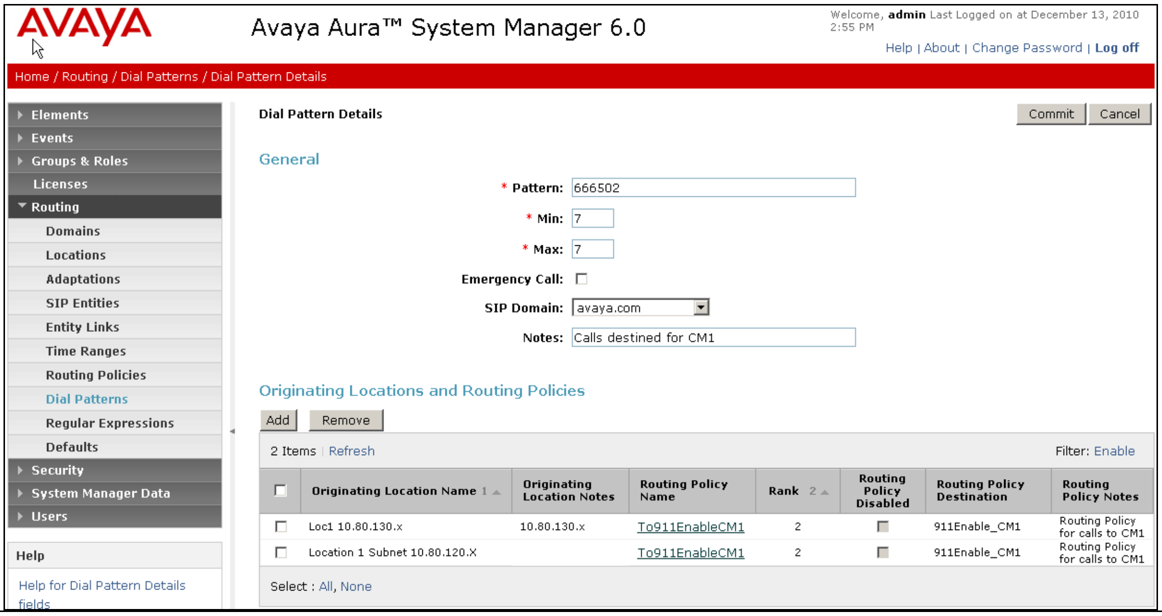
2 Items | Refresh   Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Loc1 10.80.130.x	10.80.130.x	To911EGWPrimary	0	☐	911EGWPrimary	911 Primary GW
☐	Loc1 10.80.130.x	10.80.130.x	To911EGWBackup	1	☐	911EGWBackup	Backup 911 GW

Select : All, None

23. **Dial Patterns – Calls to first Communication Manager**

The following screen displays the Dial Pattern used to route the call to first Communication Manager after EGW has determined (**Step 22**) which extension the 911 call was originated. A similar route can be configured for calls destined for the second Communication Manager.



Dial Pattern Details

General

* Pattern: 666502

* Min: 7

* Max: 7

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Calls destined for CM1

Originating Locations and Routing Policies

Add | Remove

2 Items | Refresh   Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Loc1 10.80.130.x	10.80.130.x	To911EnableCM1	2	☐	911Enable_CM1	Routing Policy for calls to CM1
☐	Location 1 Subnet 10.80.120.X		To911EnableCM1	2	☐	911Enable_CM1	Routing Policy for calls to CM1

Select : All, None

5. Configure Avaya Aura® Communication Manager

Two Communication Managers were used in this compliance testing. Since the configuration is similar on both the Communication Managers, this section only describes the steps to configure one Communication Manager. Differences, if any are pointed out in relevant sections. It assumes all other components of **Figure 1** have already been configured. For more detailed information on any other Communication Manager and Phone configuration shown in **Figure 1**, consult **[3]** through **[8].**

This section is divided into two parts. **Section 5.1** describes the configuration of the SIP trunks between the Communication Manager and the Session Manager and **Section 5.2** will describe the station settings to properly send Emergency Location information to the EGW via Session Manager.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent. For all the fields where no entry was made, default values were used.

5.1. SIP Trunk Related Configuration

This section summarizes the configuration of the SIP trunks that connects the Communication Manager to Session Manager.

Step	Description
1.	**System Parameters – Customer Options** Use the **display system-parameters customer-options** command to verify that the options highlighted below are enabled. The **IP Trunks** and **ISDN-PRI** options are required to support SIP trunks in general. In addition, the **ISDN Feature Plus** option is required for EGW interoperability.

```
display system-parameters customer-options                       Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? y
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? n
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? n                 Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? n                   Multifrequency Signaling? y
      Global Call Classification? n            Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y         Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? n              Multimedia IP SIP Trunking? y
                       IP Trunks? y

            IP Attendant Consoles? n
```

Step	Description
2.	**Node Names** Use the **display node-names ip** command to verify that node names for each Session Manager, CLAN and MEDPRO exist. The example below shows the node names and IP addresses used for the compliance test. These node names will be used in the administration of other forms on Communication Manager. For the second Communication Manager, CLAN with IP address of ***10.80.111.31*** was used.

```
display node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM1                 10.80.120.28
CLAN-1A02           10.80.130.102
MEDPRO-1B07         10.80.130.105
Default             0.0.0.0
Gateway1            10.80.130.1
procr               10.80.111.100
```

Step	Description
3.	**IP network region** The Communication Manager, Session Manager and VoIP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. ▪ **Authoritative Domain** – ***avaya.com*** was used for first Communication Manager and **avaya1.com** for second Communication Manager ▪ **Name** – Any descriptive name string ▪ **IP-IP Direct Audio** (shuffling) was enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. This was done for both intra-region and inter-region IP-IP Direct Audio. This is the default setting. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ **Codec Set** - Set to the IP codec set to be used for calls within this IP network region. In this case, IP codec set 1 was selected.

```
display ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: CM1-SM
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step	Description
4.	**Codecs** Use the **change ip-codec-set 1** command to define the codecs used by IP codec set 1. The EGW only supports the G.711MU codec. Thus for the compliance test, only ***G.711MU*** was set in the codec list.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
```

Step	Description
5.	**Signaling Group** Enter the **add signaling-group *n*** command, where ***n*** is an unused signaling group, to create a new signaling group for the SIP trunk to Session Manager. For the compliance test, signaling group 1 was created for the trunk to the Session Manager. Signaling group 1 was configured using the parameters highlighted below: ▪ **Group Type** – Set to ***sip***. ▪ **Transport Method** – Set to ***tcp***. ▪ Verify that **Peer Detection Enabled** is ***y*** and that **Peer Server** is ***SM***. ▪ **Near-end Node Name** – Set to the node name of the CLAN i.e. **CLAN-1A02** noted in **Step 2**. ▪ **Far-end Node Name** – Set to the node name of Session Manager i.e. **SM1** noted in **Step 2**. ▪ **Near-end Listen Port** and **Far-end Listen Port** – set to "**5060**". ▪ **Far-end Network Region** – Set to the IP network region **1**, as defined in **Step 3**. ▪ **Far-end Domain** – Set to ***avaya.com***. This is the domain inserted by Session Manager. For the second Communication Manager, this value was set ***avaya1.com***. ▪ **DTMF over IP** – Set to ***rtp-payload*** to enable Communication Manager to use DTMF according to RFC 2833. ▪ **Direct IP-IP Audio Connections** – Set to ***y***, indicating that the RTP paths should be optimized to reduce the use of Communication Manager audio resources when possible.

```
add signaling-group 1                                            Page   1 of   1
                                  SIGNALING GROUP

Group Number: 1               Group Type: sip
 IMS Enabled? n         Transport Method: tcp
      Q-SIP? n                                                SIP Enabled LSP? n
    IP Video? n                                      Enable SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: SM

 Near-end Node Name: CLAN-1A02             Far-end Node Name: SM1
Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1

Far-end Domain: avaya.com

                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                       IP Audio Hairpinning? n
         Enable Layer 3 Test? n                      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n               Alternate Route Timer(sec): 6
```

Step	Description

6.

Trunk Group

Use the **add trunk-group *n*** command, where ***n*** is an unused trunk group, to create a new trunk group for SIP trunk to Session Manager as follows:

On **Page 1**:

- Set the **Group Type** to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** to ***public-ntwrk***.
- Set the **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group configured in the previous step.
- Set the **Number of Members** field to the number of channels available in this trunk.

```
add trunk-group 1                                               Page   1 of  21
                                TRUNK GROUP
Group Number: 20                   Group Type: sip          CDR Reports: y
  Group Name: 911 calls                   COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

7.

Public Unknown Numbering

Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created that will be used by the trunk groups defined in previous step. In the example shown below, all calls originating from a 7-digit extension beginning with 6665 and routed over trunk group 1.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN            CPN
Len Code          Grp(s)    Prefix         Len
                                                     Total Administered: 3
 5  5             56         90855         10           Maximum Entries: 240
 7  6665          1                         7
 8  16665         1                         8
```

Step	Description
8.	**Automatic Route Selection (ARS)** For the compliance test, ARS was used to route emergency calls to the EGW via Session Manager. The dialed string of ***9*** was configured as the feature access code (FAC) for ARS. Use the **change ars analysis** command to create an entry in the ARS table. Two entries were created in the ARS table so that calls dialed with or without the ARS feature access code were routed to the EGW (e.g., 9911 or 911). In either case, the preceding ***9*** is removed by ARS before searching the table for a matching entry. The two resulting entries (for 11 and 911) are highlighted below. **Note**: Accessing ARS without first dialing the FAC, is only possible if the **ARS/AAR Dialing without FAC** field is enabled. Use the **display system-parameters customer-options** command to view its current state. A third entry is highlighted below which is used to route emergency calls to the ECRC. This is used if the ERS is unavailable and the EGW initiates a call to the ECRC number 1514904xxxx. The ECRC number begins with the dialed string of ***1514904***. This dialed string is mapped to route pattern ***11*** which routes calls to a PRI trunk ***11*** connected to the PSTN.

```
change ars analysis 11                                          Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    3

          Dialed           Total     Route     Call   Node   ANI
          String         Min  Max  Pattern     Type   Num    Reqd
    11                   2    2     1          emer          n
    911                  3    3     1          emer          n
    303538xxxx           10   10    12         natl          n
    1514904              11   11    11         natl          n
```

Step	Description
9.	**Route Patterns** Use the **change route pattern *n*** command, where ***n*** is an unused route pattern, to create a separate route pattern for each of the dialed strings used for emergency calls in the ARS table. Two separate entries were created for the 911 calls to be routed properly. The first entry relates to the call being routed to EGW via Session Manager. If EGW is down, the call is routed via a PRI trunk using the second entry in this route pattern. • **Pattern Name** – Set to any descriptive name • **Grp No 1:**– Set to 1 for 911 calls routed to EGW via Session Manager. In this example, up to first three digits are deleted and 911 inserted to cater for calls made by dialing 911 or 9911 because first ***9*** is absorbed as a Facility Access Code for ARS. • **Grp No 2:**- Set to 11 for 911 calls to be sent directly to ECRC via PSTN. Note that trunk group 11 is a PRI trunk configured for calls to PSTN. • **LAR** – Set to **next**. This enables Communication Manager to route the call to ECRC if the 911 calls fails to establish because EGW is down. Note: Details for configuration of the PRI trunk are not provided here. Consult **[3]** for further details.

```
change route-pattern 1                                       Page   1 of   3
                    Pattern Number: 1   Pattern Name: 911 calls
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    0                   3    911                                   n   user
 2: 11   0                   3    1514904xxxx                           n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

Step	Description
10.	**Route Pattern – PSTN Trunk** In cases where the EGW is operational but it can not reach the ERS due to a WAN failure, the EGW routes the call back to Communication Manager via Session Manager. Communication Manager then routes the call out the PSTN trunk using the route pattern configured below.

```
change route-pattern 11                                         Page   1 of   3
                    Pattern Number: 11  Pattern Name: PSTN
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 11   0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

11.	**Inbound Call Routing – Temporary Callback Numbers** When the PSAP uses the callback number, it must be routed to the correct destination. If the callback number is a DID number temporarily assigned by the EGW as a callback number, then the call must get routed to the EGW to determine the associated internal extension. Use the **change inc-call-handling-trmt trunk-group *n*** command, where ***n*** is the trunk group to the PSTN, to insert a 9 in front of all the DID numbers used by the EGW as temporary DIDs. The preceding 9 (which is the ARS feature access code) will instruct Communication Manager to process the digits using ARS to determine the route.

```
change inc-call-handling-trmt trunk-group 11                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert           Per Call Night
 Feature        Len      Digits                          CPN/BN   Serv
 netwrk         10   303538xxxx         9
```

Step	Description
12.	**Routing Callback Calls to the EGW** Use the **change ars analysis** command to add an entry in the ARS table for each DID used by the EGW. Each entry matches the inbound DID number and maps it to a route pattern that routes the call to the EGW via Session Manager. In the example below, the dialed string 303538xxxx uses route pattern 12 to route the call to EGW via Session Manager.

```
change ars analysis 11                                          Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    3

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    11                    2    2     1        emer         n
    911                   3    3     1        emer         n
    303538xxxx            10   10    12       natl         n
    1514904               11   11    11       natl         n
```

Step	Description
13.	**Callback Route Pattern** Use the **change route pattern** command to create a route for the callback calls using the EGW assigned DID numbers. These calls must be directed to the EGW. Thus, the route pattern is created the same as the route pattern 1 in **Step 9** with the following exceptions: • **Pattern Name** – Enter and descriptive name. • Remove the second trunk choice shown in route pattern 11. This route pattern is similar to one in **Step 9** except there is no additional entry for a call to go back to PSTN if EGW fails to respond.

```
change route-pattern 12                                         Page   1 of   3
                    Pattern Number: 12    Pattern Name: Callback calls
                               SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                     next
 2: y y y y y n  n            rest                                     none
 3: y y y y y n  n            rest                                     none
 4: y y y y y n  n            rest                                     none
 5: y y y y y n  n            rest                                     none
 6: y y y y y n  n            rest                                     none
```

5.2. Station Configuration

This section will describe the settings required of each of the different station types to support the EGW functionality. Each station is required to have an Emergency Location Extension configured.

Step	Description
1.	**H.323 and SIP Telephones** The example below shows the Emergency Location Extension configuration for an Avaya IP Telephone (H.323). Use the **display station *n*** command, where ***n*** is the station extension, to view the settings. By default, the Emergency Location Extension is the same as the station extension and the **Always Use** field is set to ***y***. If the **Always Use** field is set to ***n***, then the Emergency Location Extension will be taken from the IP network map form if an extension is configured there.

```
display station 6665011                                        Page   2 of   4
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe            Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
             CDR Privacy? n                             Data Restriction? n
   Redirect Notification? y                   Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? n                     Restrict Last Appearance? y
  Active Station Ringing: single
                                                          EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                        EC500 State: enabled
         Multimedia Mode: enhanced                  Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
                                                Direct IP-IP Audio Connections? y
  Emergency Location Ext: 666-5011      Always Use? y IP Audio Hairpinning? n
```

Step	Description
2.	**Digital and Analog Telephones** The example below shows the Emergency Location Extension configuration for a digital telephone. Use the **display station *n*** command, where ***n*** is the station extension, to view the settings. By default, the Emergency Location Extension is the same as the station extension. There is no **Always Use** field as there was for the H.323/SIP telephones. All digital and analog telephones are configured in a similar way.

```
display station 6665201                                         Page   2 of   4
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                         Call Waiting Indication: y
 Per Button Ring Control? n                    Att. Call Waiting Indication: y
   Bridged Call Alerting? n                       Distinctive Audible Alert? y
        Switchhook Flash? y                             Adjunct Supervision? y
    Ignore Rotary Digits? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
         Multimedia Mode: basic                     Audible Message Waiting? n
    MWI Served User Type:
              AUDIX Name:
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
                                                Direct IP-IP Audio Connections? y
  Emergency Location Ext: 666-5201                     IP Audio Hairpinning? n
```

Step	Description
3.	**Avaya IP one-X® Communicator** The example shows the settings for an Avaya IP one-X® Communicator (H.323 and SIP). Use the **display station *n*** command, where ***n*** is the station extension, to view the settings. It contains an additional field named **Remote Softphone Emergency Calls**. In the case of the compliance test, the Avaya IP one-X® Communicator was treated the same as any other IP telephone on the enterprise, so the **Remote Softphone Emergency Calls** field was left with the default value of ***as-on-local***. This setting instructs the Communication Manager to use the value in the **Emergency Location Ext** field as the Emergency Location Extension. This value can still be overwritten by the value on the IP network map form if permitted by the setting of the **Always Use** field. Additionally, the ESL software was loaded on the desktop where Avaya IP one-X® Communicator was installed which automatically reports its location to EGW.

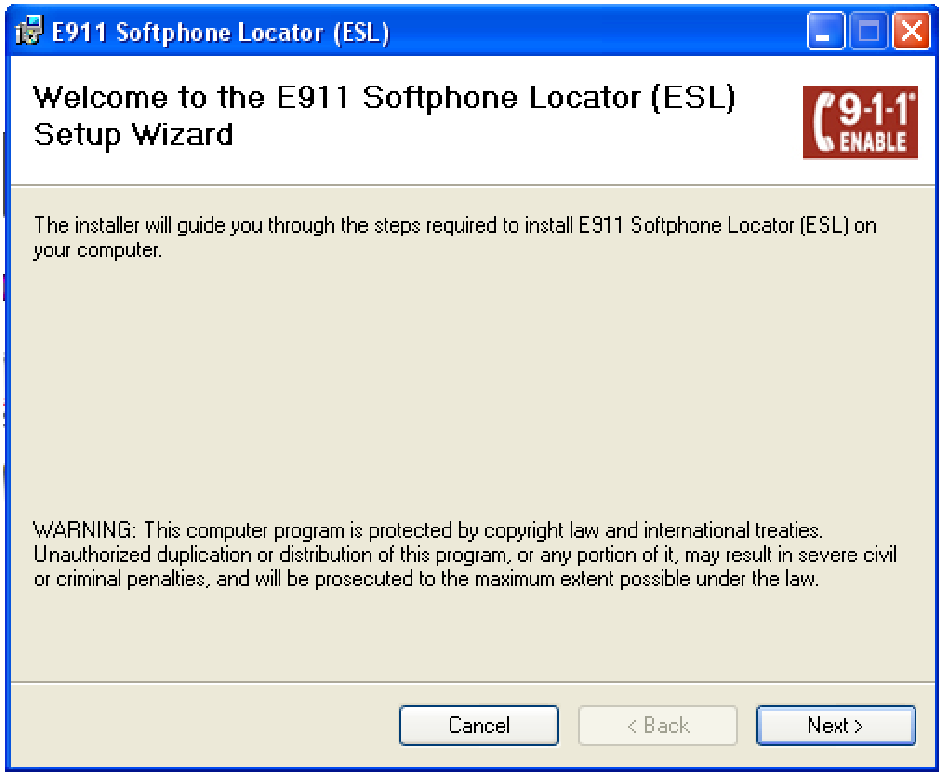
```
display station 6665023                                        Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? n
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                     EC500 State: enabled
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
              AUDIX Name:                      Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 666-5023      Always Use? y IP Audio Hairpinning? n
```

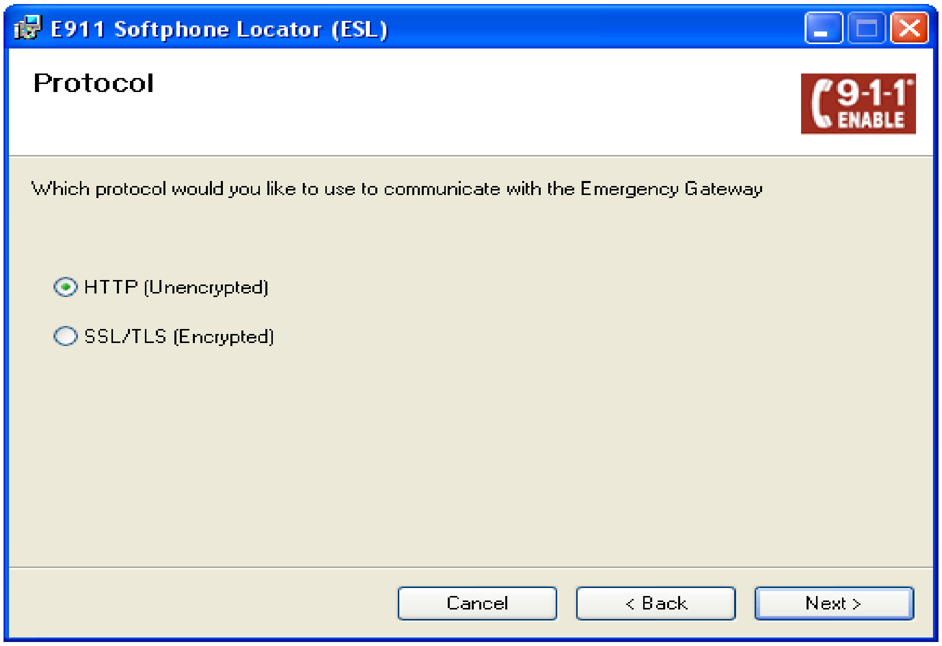
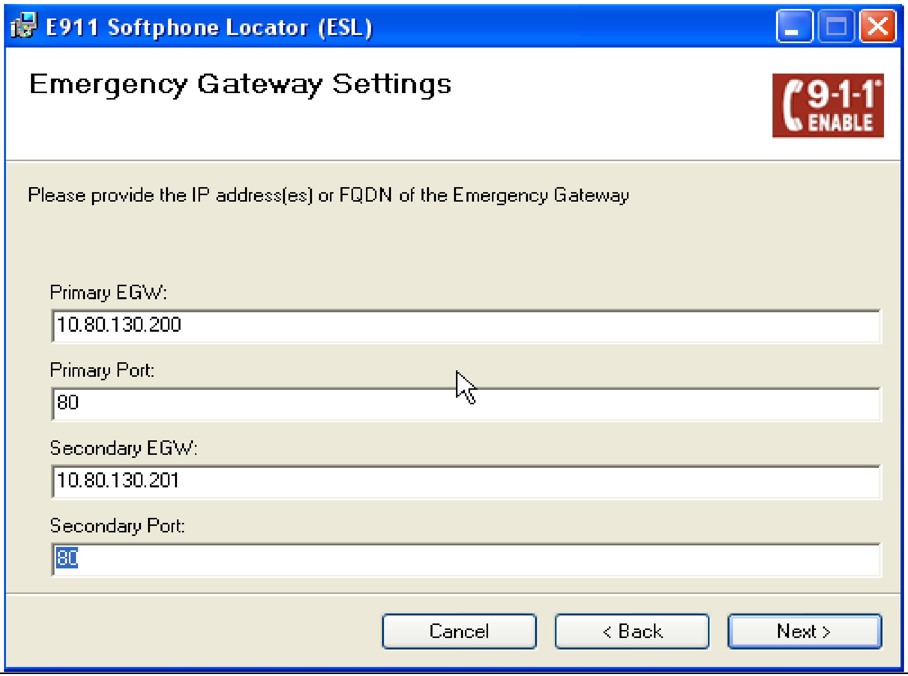
6. Configure the Avaya Endpoints

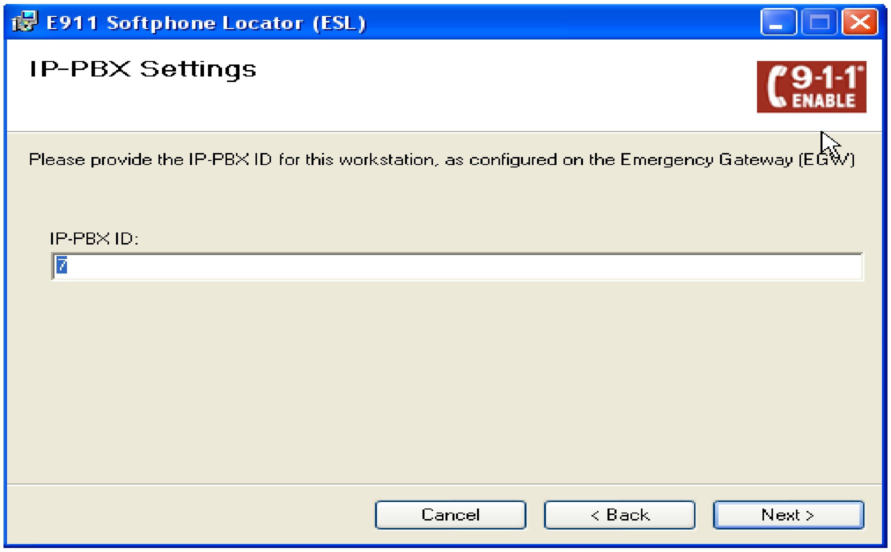
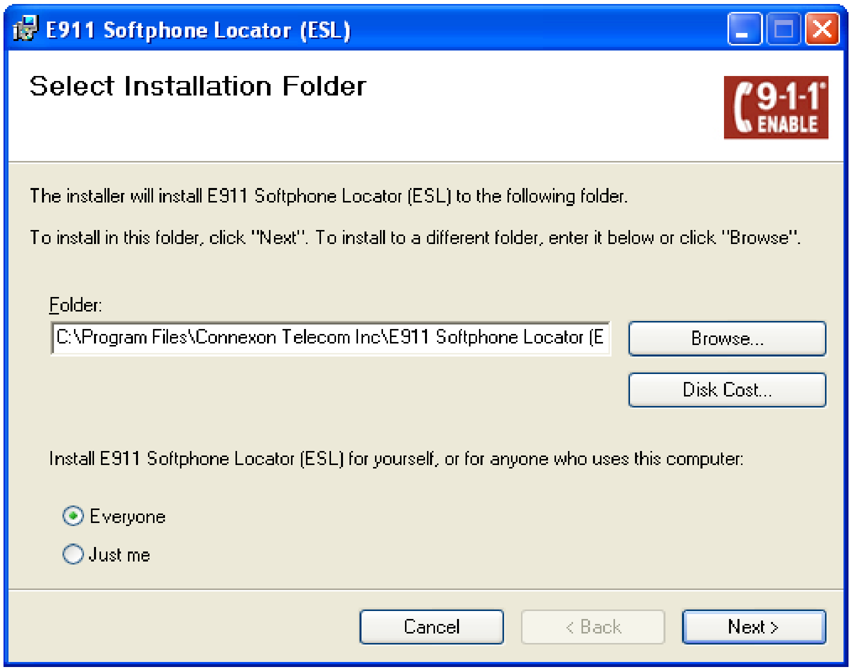
This section describes the configuration required of Avaya endpoints to support the EGW functionality. Avaya H.323 and SIP telephones require additions to the 46xxsettings.txt file to support layer 3 discovery. The PC running Avaya IP one-X® Communicator requires installation of the ESL software on it.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

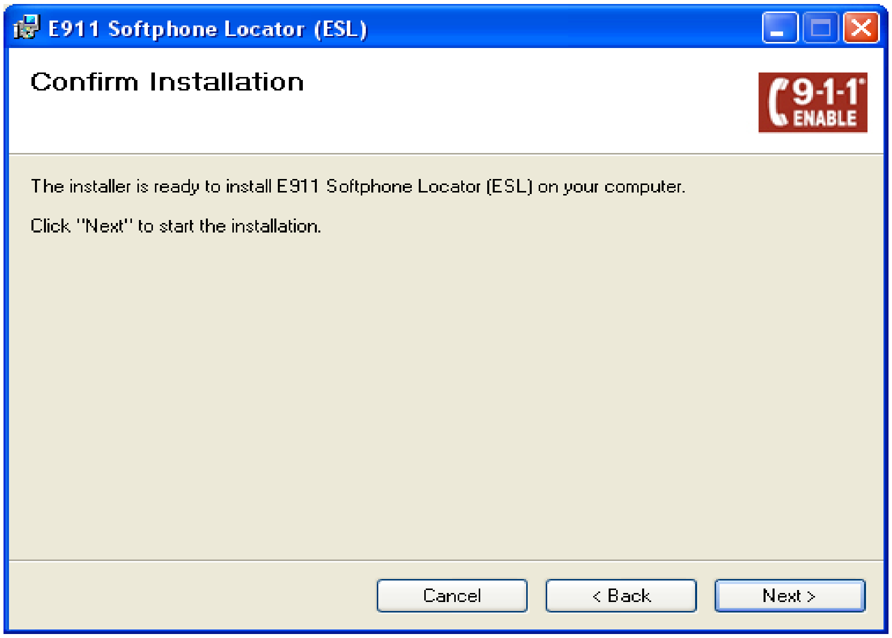
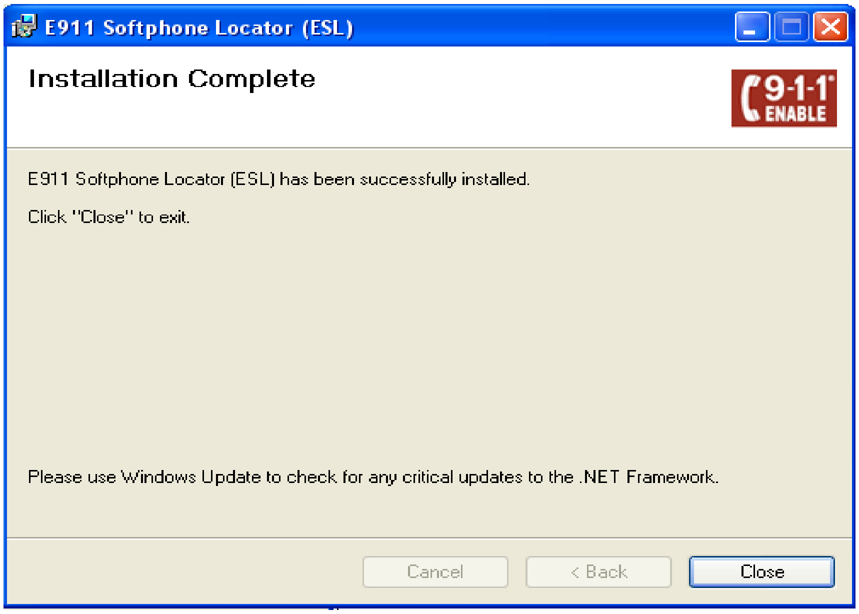
Step	Description
1.	**Avaya H.323 and SIP Telephone Configuration File** In order to support layer 3 discovery, the following lines need to be added to the 46xxsettings.txt configuration file for Avaya H.323 and SIP telephones. The two highlighted parameters in the **SUBSCRIBELIST** and **WMLHOME** URLs must be modified for a specific installation. The first parameter (***10.80.130. 200***) represents the IP address of the private side of the primary EGW. The second parameter *IP-PBX-ID* is set to (*7*) number created in **Section 7**, **Step 5**. Since two separate Communication Managers were used in this compliance testing, for the IP endpoints registered to the second Communication Managers used *IP-PBX ID* of ***11***.

```
## 911 Enable Settings
SET TPSLIST /
SET SUBSCRIBELIST http://10.80.130.200/IP-PBX ID/r
SET SNMPADD “”
SET SNMPSTRING public
SET PUSHPORT 80
SET PUSHCAP 2222
SET WMLHOME http://10.80.130.200/wml/IP-PBX ID/service.html (Needs to
be set for each phone type being used)
```

Step	Description
2.	**Avaya IP one-X® Communicator – ESL software installation** On the PC running the Avaya IP one-X® Communicator, launch the ESL setup application. A welcome screen will appear. Click **Next** to proceed.  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.

Step	Description
3.	**ESL Installation – Select Protocol** Select the desired protocol. HTTP was used for the compliance test. Click **Next**.  E911 Softphone Locator (ESL) Protocol Which protocol would you like to use to communicate with the Emergency Gateway ● HTTP (Unencrypted) ○ SSL/TLS (Encrypted)
4.	**ESL Installation – EGW Settings** Enter the IP addresses for both EGWs. Use the default port ***80*** for HTTP. Click **Next**.  E911 Softphone Locator (ESL) Emergency Gateway Settings Please provide the IP address(es) or FQDN of the Emergency Gateway Primary EGW: 10.80.130.200 Primary Port: 80 Secondary EGW: 10.80.130.201 Secondary Port: 80

Step	Description
5.	**ESL Installation – IP-PBX Settings** Enter the **IP-PBX ID** from **Section 7**, **Step 5**. 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: 7
6.	**ESL Installation – Installation Folder** 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

Step	Description
7.	**ESL Installation – Confirm** 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.
8.	**ESL Installation – Complete** 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.

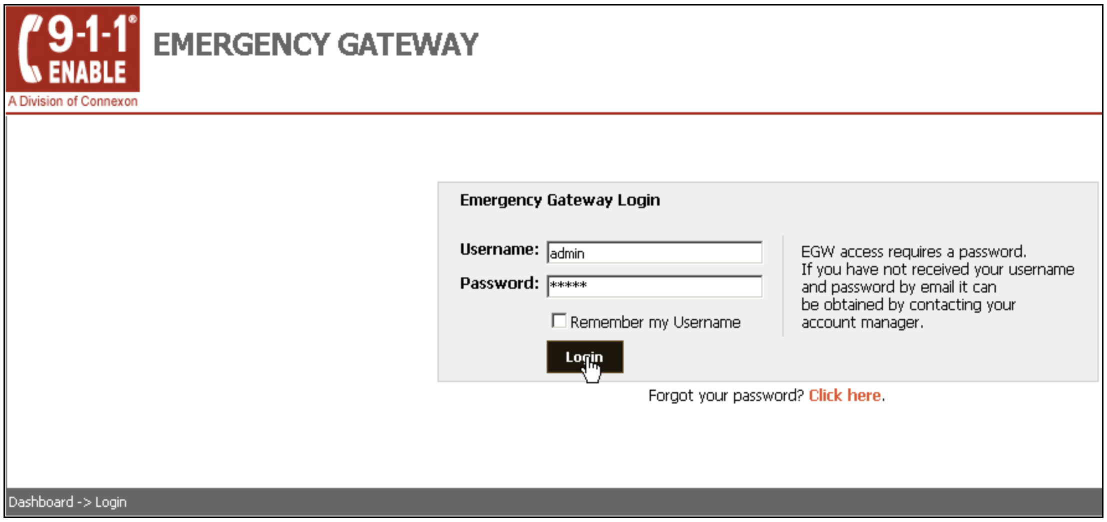
7. Configure 911 Enable Emergency Gateway (EGW)

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

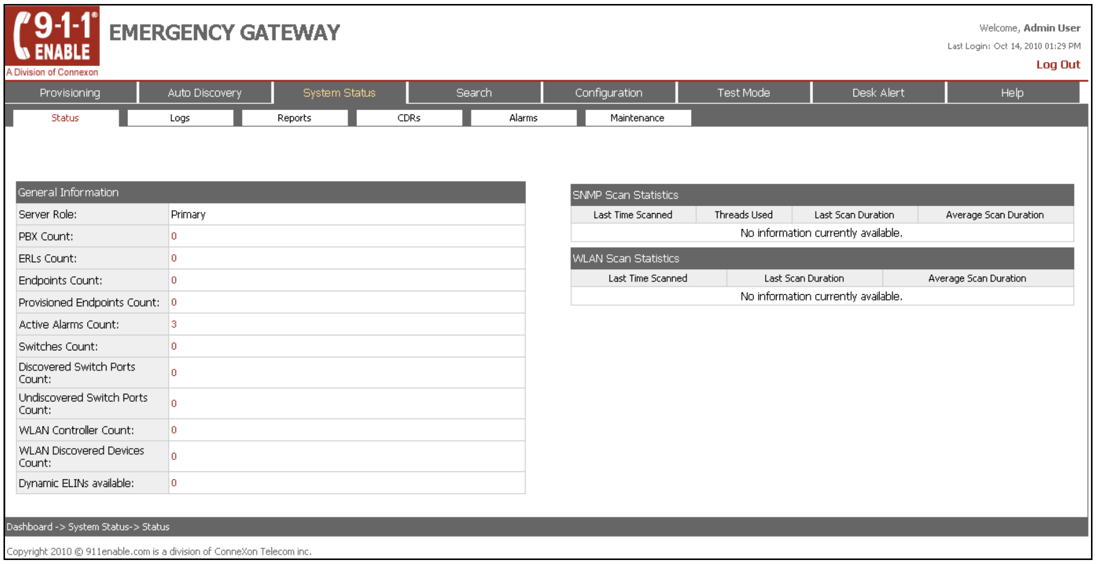
EGW access requires a password. If you have not received your username and password by email it can be obtained by contacting your account manager.

Forgot your password? Click here.

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

Main Page

The main page of the EGW will appear.



Welcome, **Admin User**

Last Login: Oct 14, 2010 01:29 PM

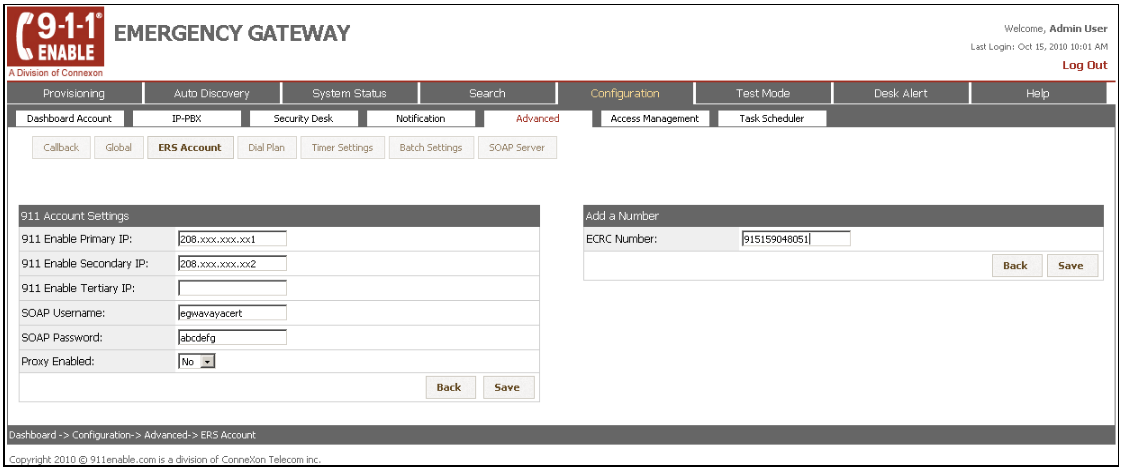
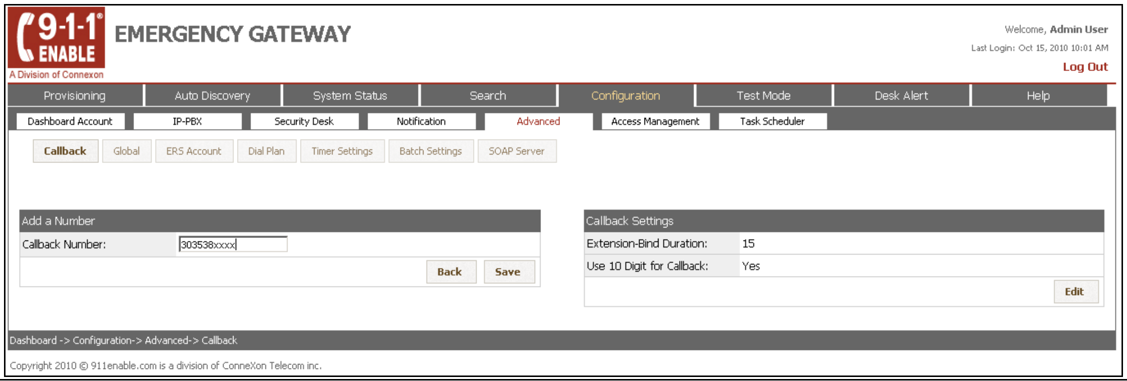
<table>
<tr><th colspan="2">General Information</th></tr>
<tr><td>Server Role:</td><td>Primary</td></tr>
<tr><td>PBX Count:</td><td>0</td></tr>
<tr><td>ERLs Count:</td><td>0</td></tr>
<tr><td>Endpoints Count:</td><td>0</td></tr>
<tr><td>Provisioned Endpoints Count:</td><td>0</td></tr>
<tr><td>Active Alarms Count:</td><td>3</td></tr>
<tr><td>Switches Count:</td><td>0</td></tr>
<tr><td>Discovered Switch Ports Count:</td><td>0</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>

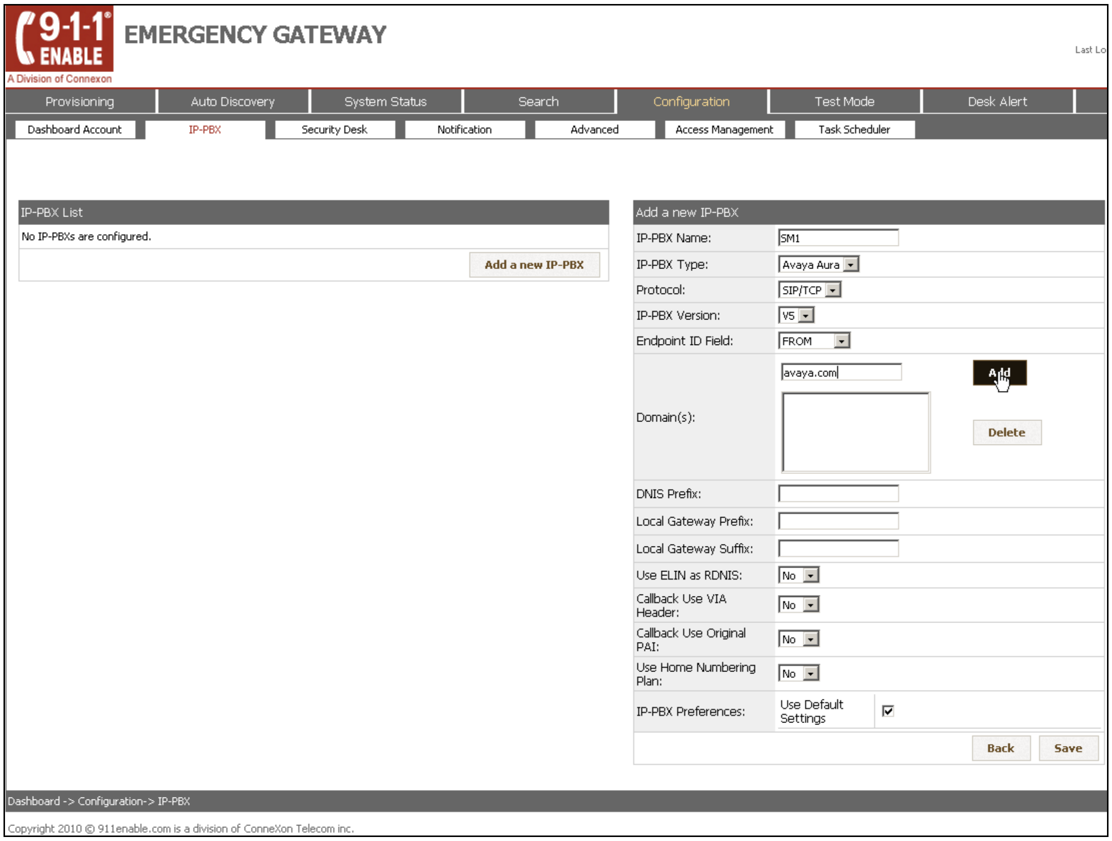
<table>
<tr><th colspan="4">SNMP Scan Statistics</th></tr>
<tr><td>Last Time Scanned</td><td>Threads Used</td><td>Last Scan Duration</td><td>Average Scan Duration</td></tr>
<tr><td colspan="4">No information currently available.</td></tr>
</table>

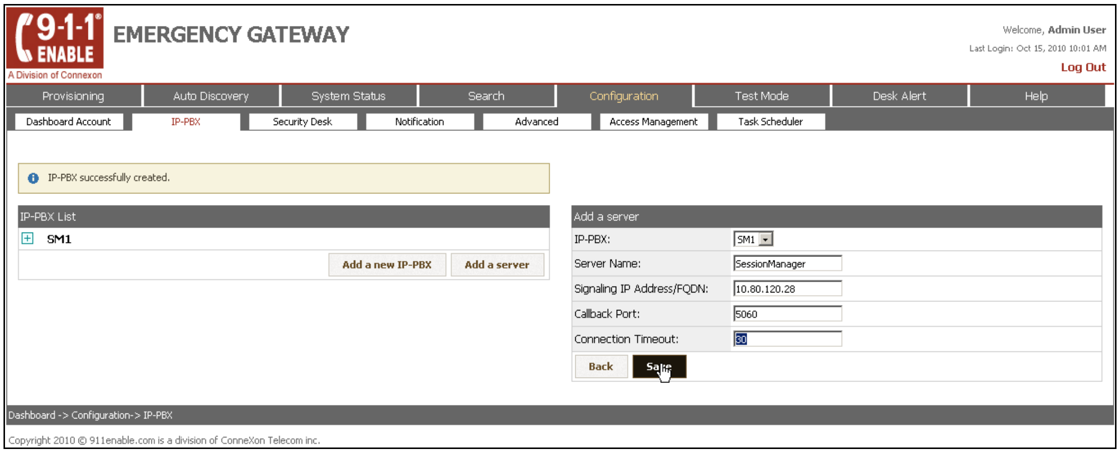
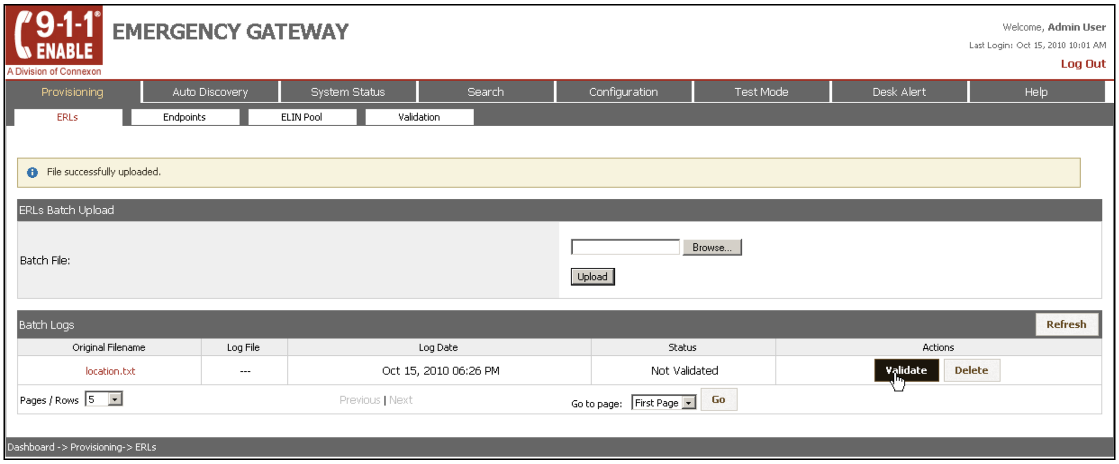
<table>
<tr><th colspan="3">WLAN Scan Statistics</th></tr>
<tr><td>Last Time Scanned</td><td>Last Scan Duration</td><td>Average Scan Duration</td></tr>
<tr><td colspan="3">No information currently available.</td></tr>
</table>

Copyright 2010 © 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 Connexon 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 Communication Manager so it contains the preceding 9 (ARS feature access code) followed by the 11-digit number.  911 Account Settings 911 Enable Primary IP: 208.xxx.xxx.xx1 911 Enable Secondary IP: 208.xxx.xxx.xx2 911 Enable Tertiary IP: SOAP Username: egwavayacert SOAP Password: abcdefg Proxy Enabled: No Add a Number ECRC Number: 915159048051 Dashboard -> Configuration-> Advanced-> ERS Account Copyright 2010 © 911enable.com is a division of ConneXon Telecom inc.
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 this 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 [not shown]. Enter the number in the subsequent window shown below and click **Save**. Each callback number is a by 10-digits number. For security reasons, the full PSTN number is not shown below but some digits are replaced by an x.  Add a Number Callback Number: 303538xxxx Callback Settings Extension-Bind Duration: 15 Use 10 Digit for Callback: Yes Dashboard -> Configuration-> Advanced-> Callback Copyright 2010 © 911enable.com is a division of ConneXon Telecom inc.

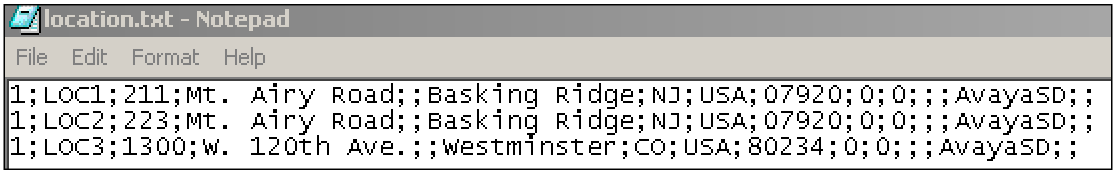
Step	Description
5.	**IP-PBX** Navigate to **Configuration → IP-PBX** to configure as follows: • Click on **Add a new IP-PBX** button and the right side of the screen shows up. • **IP-PBX Name** – Set to any descriptive name • **Protocol** – Set to ***SIP/TCP*** • **IP-PBX Version** – Select ***V5*** • **Domain(s): -** Enter ***avaya.com*** and click on **Add** • **Callback Use VIA Header** – Set to ***Yes*** [not shown] • **Callback Use Original PAI** – Set to ***Yes*** [not shown]  IP-PBX List No IP-PBXs are configured. Add a new IP-PBX IP-PBX Name: SM1 IP-PBX Type: Avaya Aura Protocol: SIP/TCP IP-PBX Version: V5 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: No Callback Use Original PAI: No Use Home Numbering Plan: No IP-PBX Preferences: Use Default Settings ☑

Step	Description
6.	**IP-PBX – Continued** Click on the **Add a server** button to display the screen on the right and configure as follows: • **IP-PBX** – Select the PBX configured in previous step • **Signaling IP Address (FQDN)** – Enter the IP address of the Session Manager configured in **Section 4**, **Step 6**. • Use default for all other values  IP-PBX successfully created. IP-PBX List: SM1 IP-PBX: SM1 Server Name: SessionManager Signaling IP Address/FQDN: 10.80.120.28 Callback Port: 5060 Connection Timeout: 30 Dashboard -> Configuration-> IP-PBX Copyright 2010 © 911enable.com is a division of ConneXon Telecom inc.
7.	**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 next step.  File successfully uploaded. Original Filename: location.txt Log File: --- Log Date: Oct 15, 2010 06:26 PM Status: Not Validated Dashboard -> Provisioning-> ERLs

Step **Description**

8. **Locations Batch File**

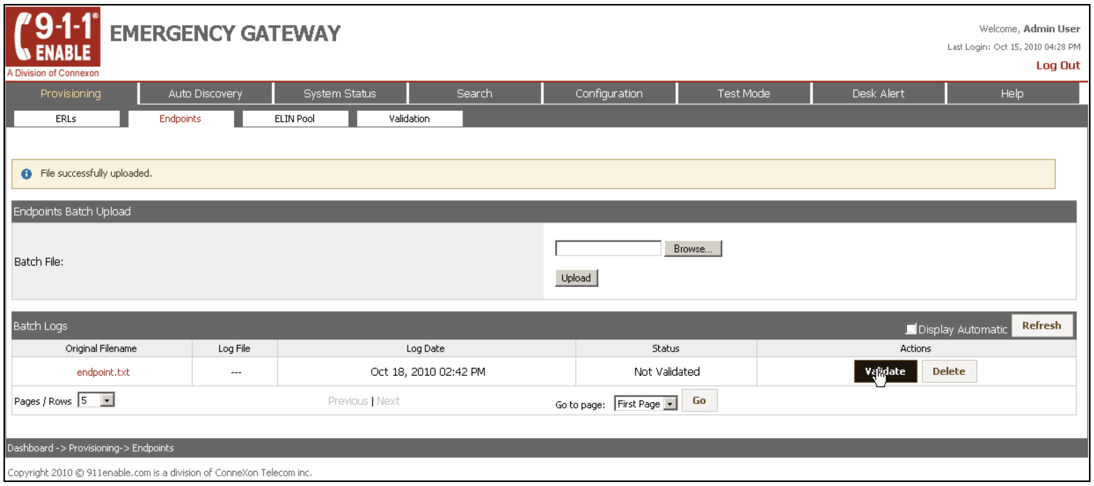
The following is an example of the ERL batch file used for the compliance test. All locations also share a single security desk location named **AvayaSD** and defined in **Step 12**. For complete details on each of the fields in the ERL Batch File, see **[10]**.



```
1;LOC1;211;Mt. Airy Road;;Basking Ridge;NJ;USA;07920;0;0;;;AvayaSD;;
1;LOC2;223;Mt. Airy Road;;Basking Ridge;NJ;USA;07920;0;0;;;AvayaSD;;
1;LOC3;1300;W. 120th Ave.;;Westminster;CO;USA;80234;0;0;;;AvayaSD;;
```

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**. An example of a provisioned endpoints batch file is shown in **Step 10**.



File successfully uploaded.

Endpoints Batch Upload

Batch File:

Batch Logs

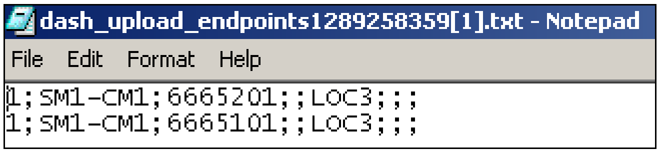
Original Filename	Log File	Log Date	Status	Actions
endpoint.txt	---	Oct 18, 2010 02:42 PM	Not Validated	Validate Delete

Pages / Rows: 5

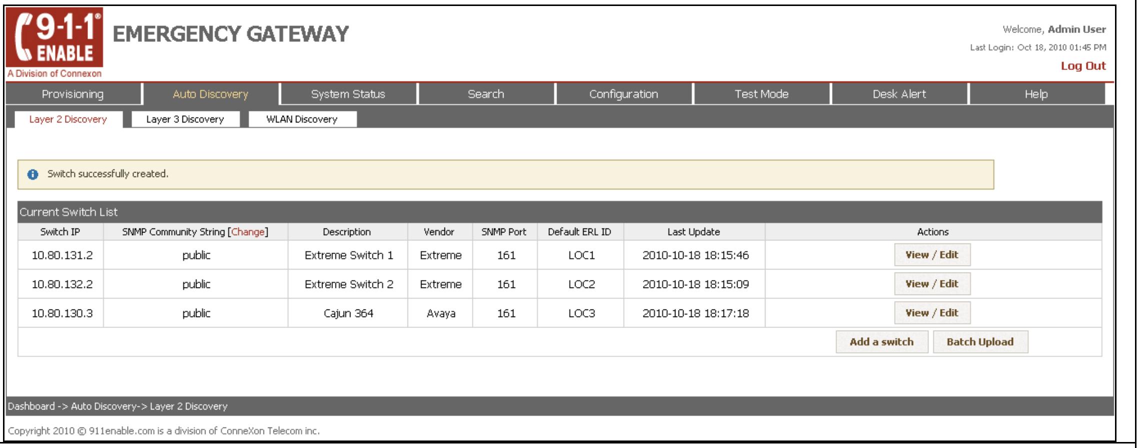
Go to page: First Page

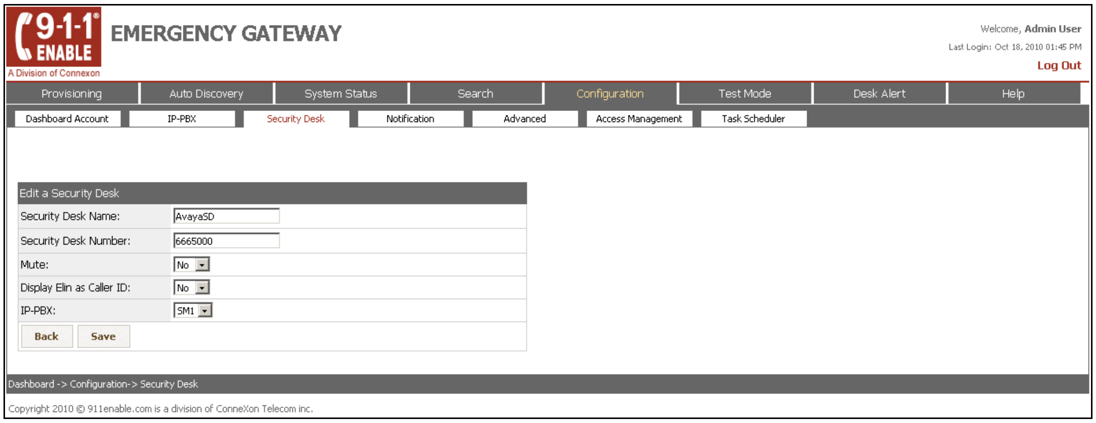
10. **Provisioned Endpoints Batch File**

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 that can not be auto-discovered.



```
1;SM1-CM1;6665201;;LOC3;;;
1;SM1-CM1;6665101;;LOC3;;;
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>11.</td><td>
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. 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.


Switch successfully created.
Current Switch List
<table>
<tr><th>Switch IP</th><th>SNMP Community String [Change]</th><th>Description</th><th>Vendor</th><th>SNMP Port</th><th>Default ERL ID</th><th>Last Update</th><th>Actions</th></tr>
<tr><td>10.80.131.2</td><td>public</td><td>Extreme Switch 1</td><td>Extreme</td><td>161</td><td>LOC1</td><td>2010-10-18 18:15:46</td><td>View / Edit</td></tr>
<tr><td>10.80.132.2</td><td>public</td><td>Extreme Switch 2</td><td>Extreme</td><td>161</td><td>LOC2</td><td>2010-10-18 18:15:09</td><td>View / Edit</td></tr>
<tr><td>10.80.130.3</td><td>public</td><td>Cajun 364</td><td>Avaya</td><td>161</td><td>LOC3</td><td>2010-10-18 18:17:18</td><td>View / Edit</td></tr>
</table>
</td></tr>
<tr><td>12.</td><td>
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 [not shown]. The example below shows the Security Desk created for the compliance test. The Security Desks number rings each time a 911 call is made using EGW.


Edit a Security Desk
Security Desk Name: AvayaSD
Security Desk Number: 6665000
Mute: No
Display Elin as Caller ID: No
IP-PBX: SM1
</td></tr>
</table>

8. Interoperability Compliance Testing

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

8.1. General Test Approach

The general test approach was to make emergency calls from different endpoints types connected to a variety of layer 2 switches and verify the location and callback information provided to the ERS.

8.2. Test Results

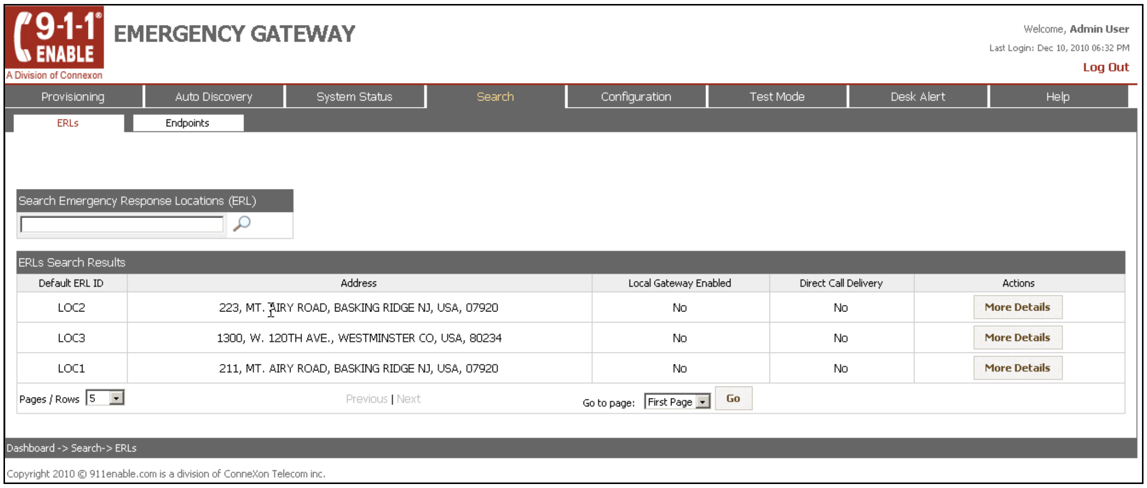
The features described in **Section 1.1** were tested. All test cases passed successfully. The following observations were made during testing:

- Once the ESL is installed and the Avaya one-X® Communicator is run for the first time, the ESL pulls the necessary information (such as the Avaya one-X® Communicator extension) from the Windows registry. This information remains in the registry and continues to be reported, even if the Avaya one-X® Communicator is later shut down. If the Avaya one-X® Communicator is moved to another location its location in the EGW will be updated once the user logs in for the first time in the new location.
- If an endpoint is registered to one PBX and then the registration is changed to another PBX, both registrations continue to show in the EGW.
- For 46XX phones, the phone information is not pushed to EGW if the phone is not pointing to the HTTP server.
- EGW requires domain names for Avaya one-X® Communicator to register properly otherwise the location information is not properly populated on the EGW.
- EGW does not send the domain name when the calls are routed back for the callback so for the same extensions configured on two separate Communication Managers, a dedicated DID should be assigned for all such extensions. The callbacks to these extensions do not flow back to EGW via Session Manager, instead, they are routed from Session Manager back to the Communication Manager extension.

9. Verification Steps

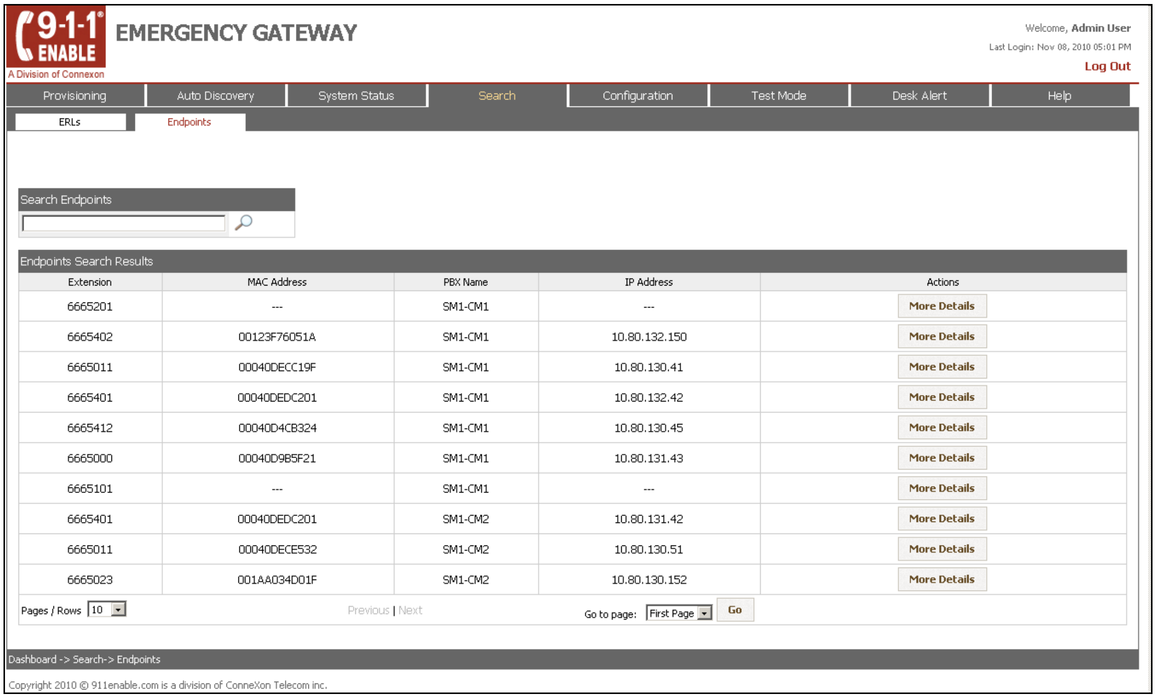
The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- On the EGW, verify the ERL information. Navigate to the **Search → ERLs** tab, verify that the locations provided in the batch file in **Section 7, Step 8** are displayed.



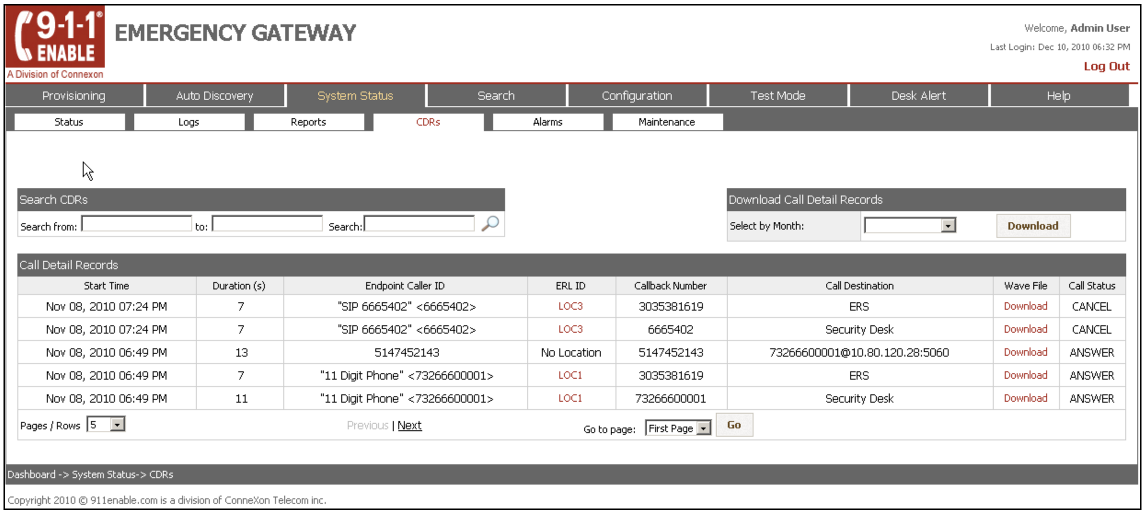
Default ERL ID	Address	Local Gateway Enabled	Direct Call Delivery	Actions
LOC2	223, MT. AIRY ROAD, BASKING RIDGE NJ, USA, 07920	No	No	More Details
LOC3	1300, W. 120TH AVE., WESTMINSTER CO, USA, 80234	No	No	More Details
LOC1	211, MT. AIRY ROAD, BASKING RIDGE NJ, USA, 07920	No	No	More Details

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



Extension	MAC Address	PBX Name	IP Address	Actions
6665201	---	SM1-CM1	---	More Details
6665402	00123F76051A	SM1-CM1	10.80.132.150	More Details
6665011	00040DECC19F	SM1-CM1	10.80.130.41	More Details
6665401	00040DEDC201	SM1-CM1	10.80.132.42	More Details
6665412	00040D4CB324	SM1-CM1	10.80.130.45	More Details
6665000	00040D9B5F21	SM1-CM1	10.80.131.43	More Details
6665101	---	SM1-CM1	---	More Details
6665401	00040DEDC201	SM1-CM2	10.80.131.42	More Details
6665011	00040DECE532	SM1-CM2	10.80.130.51	More Details
6665023	001AA034D01F	SM1-CM2	10.80.130.152	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 several emergency 911 calls as represented by the value ***ERS*** in the **Call Destination** field. The example also shows a 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
Nov 08, 2010 07:24 PM	7	"SIP 6665402" <6665402>	LOC3	3035381619	ERS	Download	CANCEL
Nov 08, 2010 07:24 PM	7	"SIP 6665402" <6665402>	LOC3	6665402	Security Desk	Download	CANCEL
Nov 08, 2010 06:49 PM	13	5147452143	No Location	5147452143	73266600001@10.80.120.28:5060	Download	ANSWER
Nov 08, 2010 06:49 PM	7	"11 Digit Phone" <73266600001>	LOC1	3035381619	ERS	Download	ANSWER
Nov 08, 2010 06:49 PM	11	"11 Digit Phone" <73266600001>	LOC1	73266600001	Security Desk	Download	ANSWER

10. 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® Communication Manager, Avaya Aura® Session Manager and the 911 Enable equipment and service as shown in **Figure 1**.

11. 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] *Installing and Configuring Avaya Aura® Session Manager,* Doc ID 03-603473 Release 6.0

[2] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Release 6.0, June 2010

[3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.

[5] *Avaya Aura® Communication Manager Screen Reference,* May 2009, Document Number 03-602878

[6] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507

[7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698

[8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.0,* Dec 2007, 16-601944

[9] *911Enable Emergency Gateway System Guide 2.6.*

[10] *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.