RedSky

Interface Control Document

for

Avaya ACM with AES

E911MANAGER

Revision History

Date	Version	Revision	Made By
7/29/2012	1.5	• Updated port requirements	Steve Madlock
8/1/2012	1.6	• Added revision history • Added IP_API details • Updated emergency call diagram	Steve Madlock
8/14	1.7	• Added Table of Figures • Edit ACM/E911 diagram • Added Deployment Consideration section	Steve Madlock
8/16	1.8	• Added Logging Levels and TDM Phones	Steve Madlock
8/20	1.9	• Various spelling and grammatical updates	Jason Forehand
3/1/2016	2.0	• Updated Permissions and Licensing Requirements	Ryan Olsen
3/27/2017	2.1	• Added documentation on Emergency Location Extension Forwarding • Various screenshot refreshes	Adam Skweres
2/20/2018	2.2	• Updated call back section	Ryan Olsen
12/29/2020	2.3		Ryan Olsen

Table of Contents

Table of Figures

Introduction

This document details the technical aspects of the integration between RedSky's E911 Manager and Avaya ACM in conjunction with AES. E911 Manager provides an automated solution for Enhanced 9-1-1 Services with the Avaya Aura® platform. E911 Manager tracks the location of TDM and IP phones and updates ACM with the appropriate location information. Additionally, E911 Manager integrates with the Local Exchange Carriers (LECs) to ensure the proper location information is received by emergency responders.

This document is intended for Avaya ACM and E911 Administrators. After reading this document an administrator should be able to fully prepare the enterprise's environment for integration with E911 Manager.

Solution Design

E911 Manager requires IP connectivity to both the ACM Servers and the AES Server. A single AES instance may be used to integrate to multiple ACM servers. E911 Manager performs three major functions for the Avaya platform:

Periodic Downloads - this action may be scheduled and collects the appropriate data to process TDM endpoints as well as dial plan options.

Monitoring of Registration Events - When E911 Manager processes a registration event for IP phones, the application will determine the location of the endpoint. Once the location has been found, E911 Manager sends an update to ACM allowing that endpoint to out pulse an Emergency Line Identification Number (ELIN) associated with that location.

Monitoring of Emergency Calls - When an emergency call is placed, ACM sends a crisis alert message to E911 Manager. The application then processes this message and sends the appropriate EON, SMS, or email messages to the users configured for alerts.

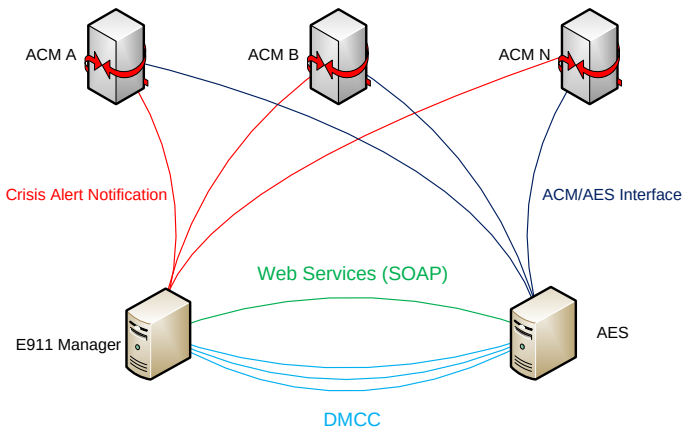

Figure 1: Solution Design

Requirements

System Versions

E911 Manager integrates with an approved Avaya Call Servers using AES, including:

Avaya ACM	• Version 4.x • Version 5.x • Version 6.x • Version 7.x • Version 8.x
Avaya AES	• Version 5.2.1 (or higher)

System Requirements

Device and Media Call Control – DMCC	DMCC Exposes the powerful feature set of your Avaya telephony server through an open, standards based, Java and Extensible Markup Language (XML) programming interface. Emergency On-site Notification requires one DMCC license per Crisis Alert station monitored by E911 Manager. E911 Manager's Active/Active solution requires a DMCC license for each instance of E911 Manager. Avaya IP_API_A license, which was the predecessor of DMCC, can also be used.
IP Phone – Crisis Alert Station	E911 Manager will register to the extension to monitor for crisis alerts. The DMCC license will be used to control this phone.
System Management Service – SMS	Provides a way for applications to programmatically access and administer a subset of administration objects on Avaya Aura Communication Manager.

Network Requirements

The RedSky support team will require remote access to the server, the below list outlines the necessary ports and protocols.

SSH/SFTP	TCP	22	• E911 Manager Linux Server Admin
SSH	TCP	5022	• ACM
HTTP	TCP	80	• AES SOAP (Unsecured)
HTTPS	TCP	443	• E911 Manager Web Interface • Web/Real time updates to ALI providers • AES SOAP (Secured)
SNMP	UDP	161	• Layer 2 Network Discovery
CMAPI (DMCC)	TCP	4721	• Crisis Alert phone registration (Unsecure)
CMAPI (DMCC) Secure	TCP	4722	• Crisis Alert phone registration (Secure)

Application Requirements

The following information will be required to configure the E911 Manager application.

ACM Username and Password	• Access to the following commands: Display, Status and Change Station List Extension-Type List Public Unknown Numbering Table List History
ACM IP Address	• Processor Ethernet IP address
AES Username and Password	•
AES Switch Connection Name	•
AES Connection Type	• Secure or unsecure
Emergency Trunk Group	• Trunk group used for routing emergency calls. • Multiple trunk groups can be specified.
Crisis Alerts extension and password (Optional)	• If your deployment includes Emergency Onsite Notification (EON), then a Crisis Alert Extension will be needed.
DMCC Registration Type (Optional)	• Secure or unsecure • DMCC is only used where EON is deployed.
Building, Room and Floor field mapping (Optional)	• This is used for TDM environments.

Avaya ACM Configuration

For use with E911 Manager, the following elements will need configured:

- Automatic Route Selection (ARS)
- Route Pattern
- Trunk Group
- Public Unknown Numbering Table (PUNT)
- Crisis Alert Station (Optional)

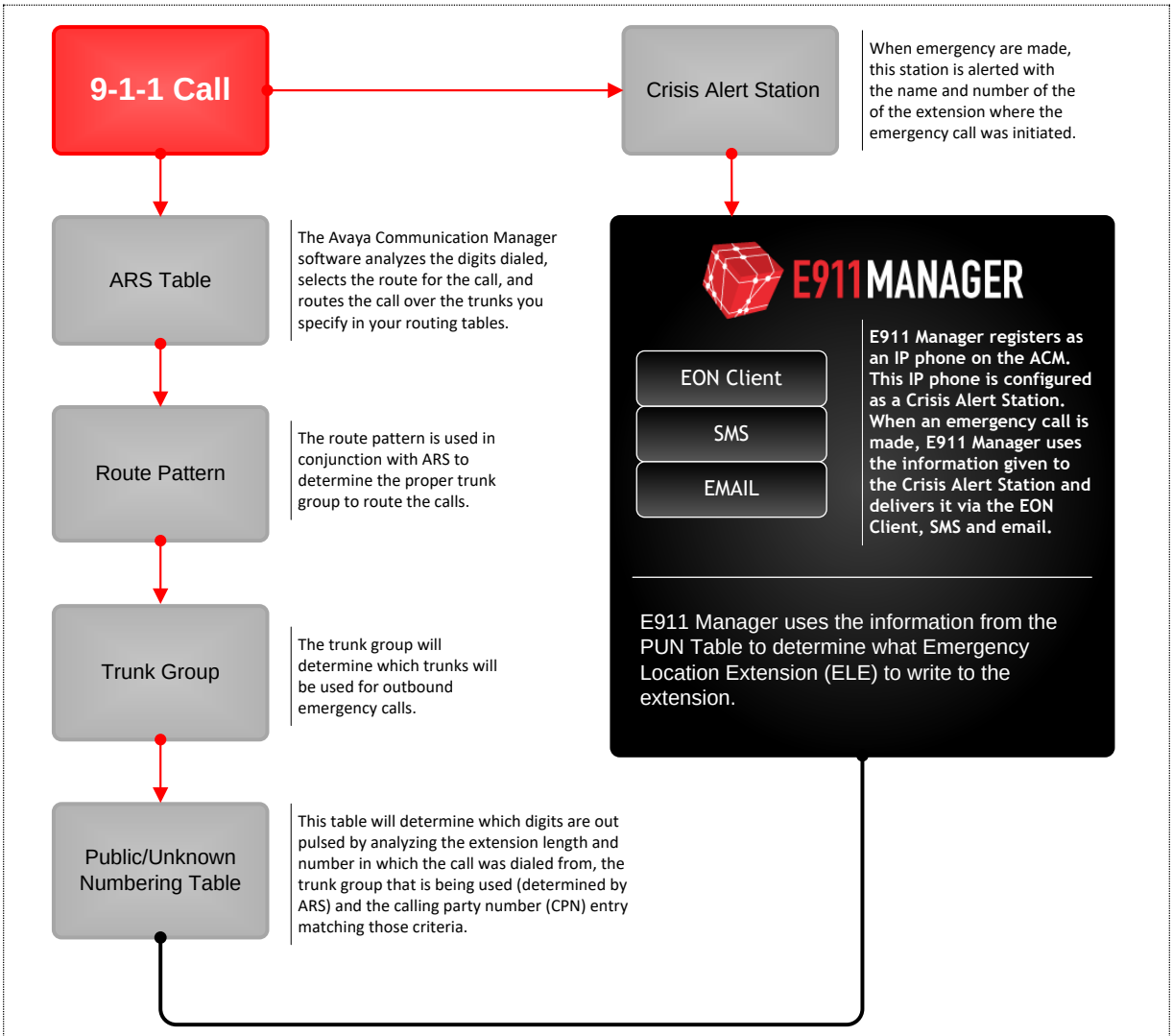

Figure 2: Avaya ACM/E911 Manager Configuration Overview

ARS Dial Analysis Table

1. In the ARS Digit Analysis table must specify the following:
    - The dial string for emergency calls.
    - The min and max number of digits for the dial string.
    - The route pattern the call will follow.
    - Call type. E911 Manager required the call type to be “alrt” if EON, SMS, or email alerts are used.

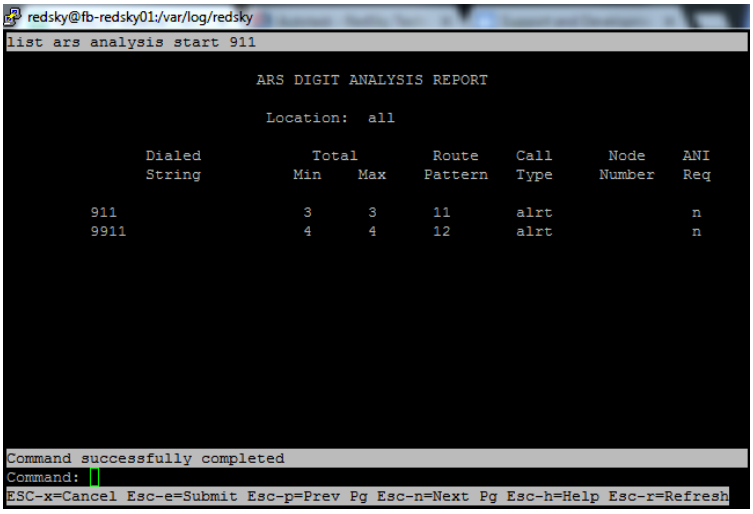

Figure 3: ARS Digit Analysis Table Example

Emergency Route Pattern

1. The route pattern must specify the trunk group used for emergency calls and must correlate to emergency call configuration in the ARS Digit Analysis table.

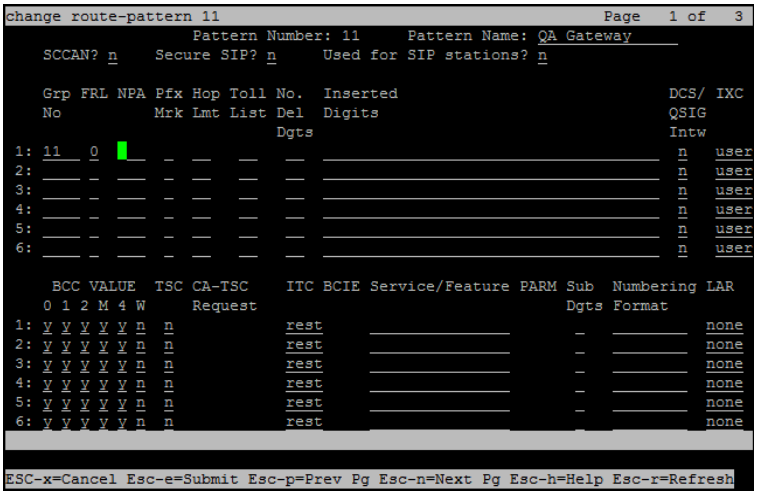

Figure 4: Emergency Route Pattern Example

Emergency Call Trunk Group

1. There is no specific trunk group configuration needed. However, there should be a trunk group defined for emergency call routing.

```
display trunk-group 11                                        Page   1 of  21
                              TRUNK GROUP

Group Number: 11                   Group Type: sip           CDR Reports: y
  Group Name: RedSky                        COR: 1        TN: 1        TAC: 311
   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: 11
                                                      Number of Members: 200

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Figure 5: Emergency Call Trunk Group

Public Unknown Number Table (PUNT)

E911 Manager uses the Public Unknown Number Table to determine what digits should be written to the Emergency Location Extension (ELE) field so that the proper ELIN can be out pulsed.

Public Unknown Number Table Requirements

- Extension length must equal to the length of the ELE that E911 Manager will write back.
- Extension code must specify the leading digit(s) of the ELE that E911 Manager will write back.
- The appropriate emergency trunk group must be specified.
- CPN Prefix combined with the ELE must match an ELIN that is configured in E911 Manager.

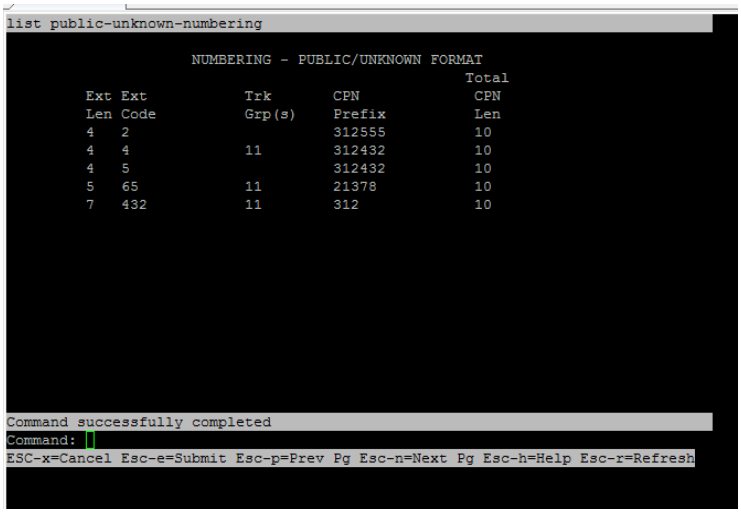

Figure 6: Public Unknown Number Table Example

Example PUN Table Entries

ELIN	PUN Table Entry					E911 Manager ELE Write Back
	Ext Len	Ext Code	Trk Grp	CPN Prefix	Total CPN Len	
3125552010	4	2	11	312555	10	2010
3124324010	4	4	11	312432	10	4010
3124325000	4	5	11	312432	10	5000
2137865000	5	65	11	21378	10	65000
3124328763	7	432	11	312	10	4328763

Note: The ELE being written back to extension must be valid in the ACM dial plan.

Emergency Location Extension (ELE) Determination

The diagram below displays how E911 Manager determines and writes the ELE to the extension.

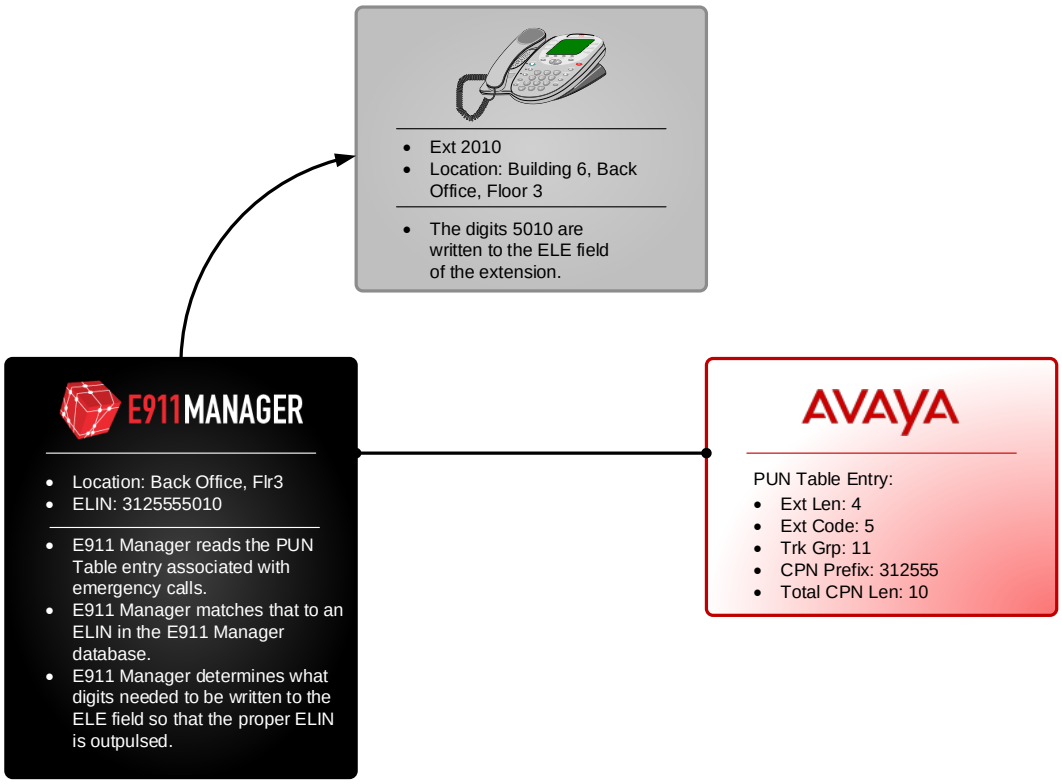

Figure 7: Emergency Location Extension (ELE) Determination Diagram

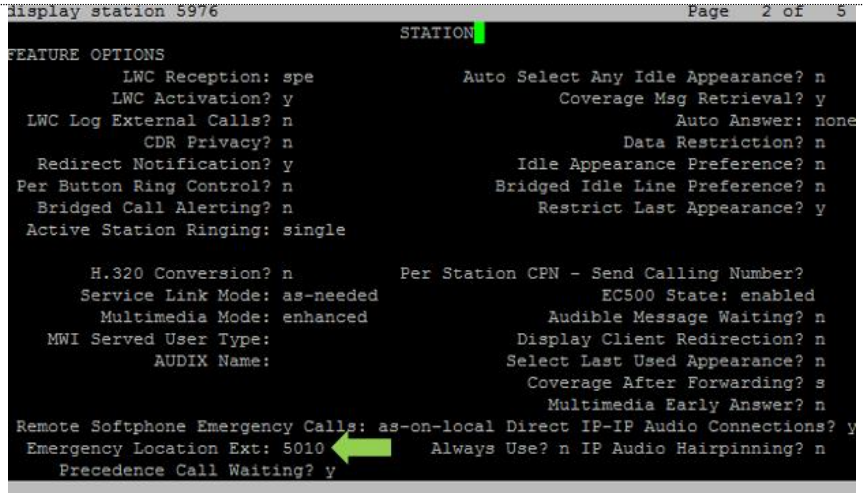

Figure 8: Emergency Location Extension (ELE) – Display Station Page 2

Crisis Alerts Station Configuration

1. A crisis alert station will need to be created in order to monitor emergency calls. Create a new virtual IP phone to use for this purpose. This phone can be any IP phone type that supports use with a softphone.

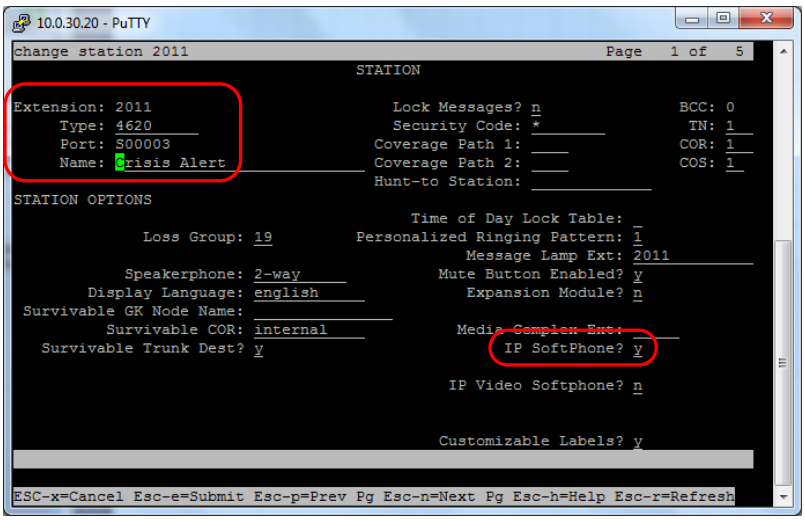

Figure 9: Crisis Alerts Station Configuration Example – Page 1

2. On page 4 of 5 add **crss-alert** to a button of your choice.

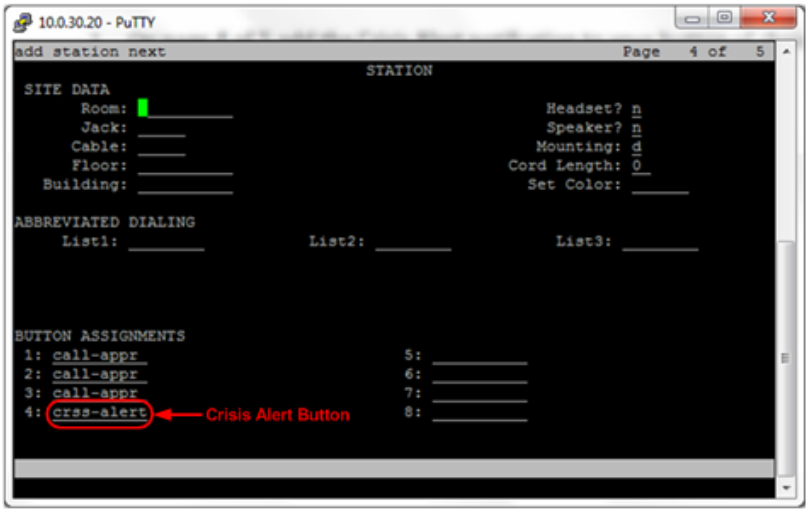

Figure 10: Crisis Alerts Station Configuration Example – Page 2

System Parameters – Crisis Alert

1. In the Crisis Alert System Parameters change the Every User Responds to “y”. This ensures that the physical telephones configured with “crss-alert” buttons will continue to be alerted audibility and visually after the RedSky EON server acknowledges the Crisis Alert.

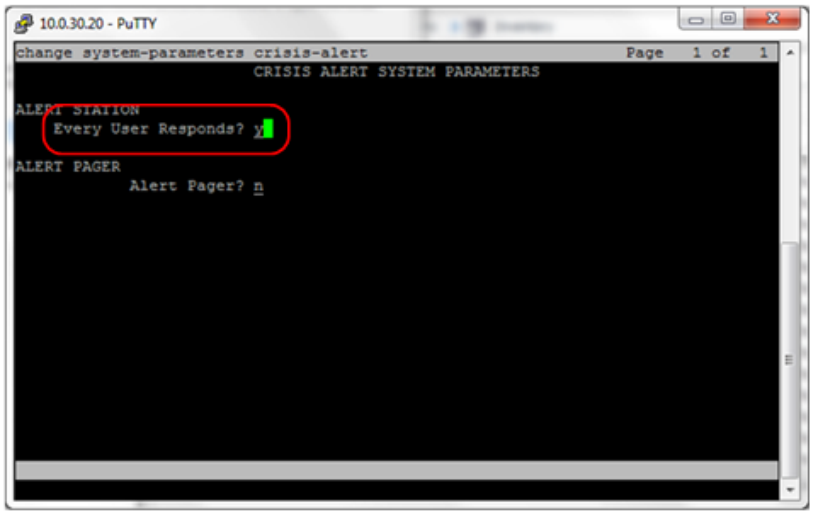

Figure 11: System Parameters – Crisis Alert Screen

TDM/IP as TDM

1. If using TDM phones the Site Data page must be utilized to determine the phones location.
2. E911 Manager reads the Building, Room, and Floor fields to map the location.
3. In order to properly identify the location of a TDM phone, the Building field should match the Building ID that is configured in E911 Manager. Additionally, supplemental information may be placed in the Room or Floor fields.

Figure 12: TDM – Site Data

IP Phone Registration

1. E911 Manager needs to be able to determine when an IP phone registers or unregisters.
2. In the Logging Level settings, “Log IP Registrations and events” must be set to Y in order for E911 Manager to discover phones.

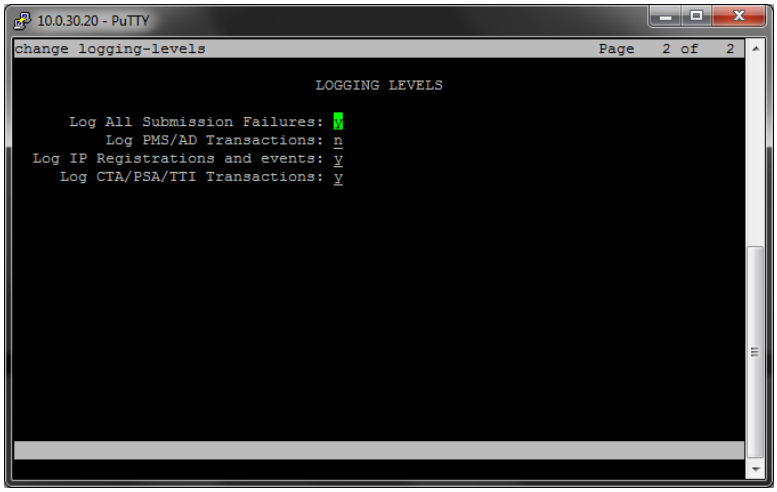

Figure 13: IP Phone Registration – Logging Levels

Call Back - Emergency Location Extension Forwarding

If an emergency call was placed from a trunk acting as an extension, the return incoming trunk call from the PSAP will ring at the extension that placed the emergency call. This is made possible by the ACM Emergency Location Extension Forwarding capability. This becomes important in the event that an emergency call gets disconnected. For this to work, each Emergency Location Extension (ELE) must exist as a station in the ACM. Additionally, an Emergency Location Extension should not be one of the following extensions, because call forwarding from these types of extensions is not possible:

- A multimedia set
- Virtual Station
- An EAS agent ID
- A hunt group extension
- A data extension
- A terminating extension group extension
- An attendant
- An extension with "Call Coverage: All" administered for it. Call Coverage Criteria: “all” is administered on the "call coverage" form. It is typically used if someone goes on a leave of absence, for example. It prevents any calls from terminating at an extension. Call Forwarding is set up at the station calls are being forwarded from. If a call never reaches the station, the call cannot be forwarded on. If the Emergency Location Extension has call coverage All enabled, a return call from the PSAP would never have a chance to be forwarded to the station that dialed 911.