RedSky

Interface Control Document

for

Cisco CUCM

E911MANAGER

Revision History

Date	Version	Revision	Made By
8/14/2012	1.5	• Updated port requirements	Steve Madlock
8/14/2012	1.5	• Formatting • Network Configuration	Steve Madlock
8/20/2012	1.6	• Updated port requirements	Steve Madlock
5/8/2014	1.7	• Updated Port requirements • Updated Directory Number requirements	Ryan Olsen
7/28/2014	1.8	• Added Sample configuration Diagram	James Rusch
4/25/2016	1.9	• Updated screenshots and added call flow diagram	Warren Hunter
5/16/2016	2.0	• Added Failover Route Point configuration	Ryan Olsen
8/24/2017	2.1	• Added Voice Gateway Requirements	Warren Hunter
7/25/2018	2.2	• E911 Manager Interface Configuration	Sam Schlicher
12/30/2020	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 Cisco Unified Communication Manager (CUCM) Call Servers. E911 Manager provides a fully automated approach to enhanced 911 for CUCM. E911 Manager maintains the location information for the entire enterprise and allows CUCM to out pulse the appropriate Emergency Line Identification Number (ELIN) during a 911 call. E911 Manager also provides additional value added services which will be outlined in further detail later in this document.

Audience

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

Requirements

E911 Manager directly interfaces with CUCM leveraging the available IP network. There are a variety of management protocols used by E911 Manager and E911 Manager must have IP connectivity to all Publishers and Subscribers that exist on the enterprise network.

AXL API	The AXL API is made available through the use of web services and exists on the same ports used for web administration of a CUCM, the default port being TCP 8443 for later versions of CUCM. The AXL interface is used to obtain information about the different endpoints that exist on the call server.
JTAPI Interface	During a 911 call E911 Manager provides CUCM the appropriate ELIN to out pulse. Along with the AXL interface, JTAPI is available on the same ports as the web management interface, the default port being TCP 2748 in later versions of CUCM. JTAPI is used to control the Calling Party Number (CPN) and replace it with an ELIN.
SNMP	SNMP allows for near real-time data updates from the call server. SNMP runs on the default port UDP 161. The below table includes all of the connectivity methods for a successful integration with E911 Manager.

Port Requirements

SSH/SFTP	TCP	22	• E911 Manager Linux Server Admin
HTTPS	TCP	443	• E911 Manager Web Interface • Web/Real time updates to ALI providers
SNMP	UDP	161	• Used to query the Cisco call manager for new end point registrations.
SOAP/AXL	TCP	8443	• Used to communicate with the Cisco call manager for end instrument registration data.
SFTP	TCP	10022	• Used to transmit ALI data to the Intrado SFTP provider.
JTAPI	TCP	2748	• Used to register a CTI port on the Cisco call manager to monitor for 911 calls.

Voice Gateway Requirements

Cisco Analog Voice gateways such as VG224, 350, etc must be configured to use the SCCP protocol. Redsky E911 Manager does not support MGCP Voice Gateways due to the way CUCM reports the device name.

Emergency Call Routing

The diagram below demonstrates how the Call Manger using E911 Manager routes an emergency call.

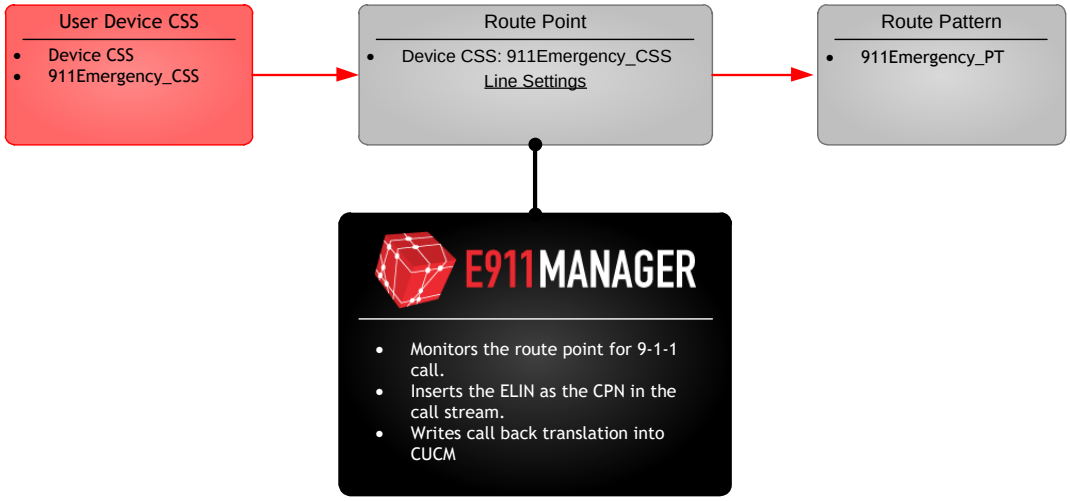


Figure 1: Emergency Call Routing

CTI Route Point

1. From the Device drop down menu, select CTI Route Point.
2. Click Add New.
3. Add a Device Name and Calling Search Space. Use the appropriate CSS for emergency calls.
4. Click Save.

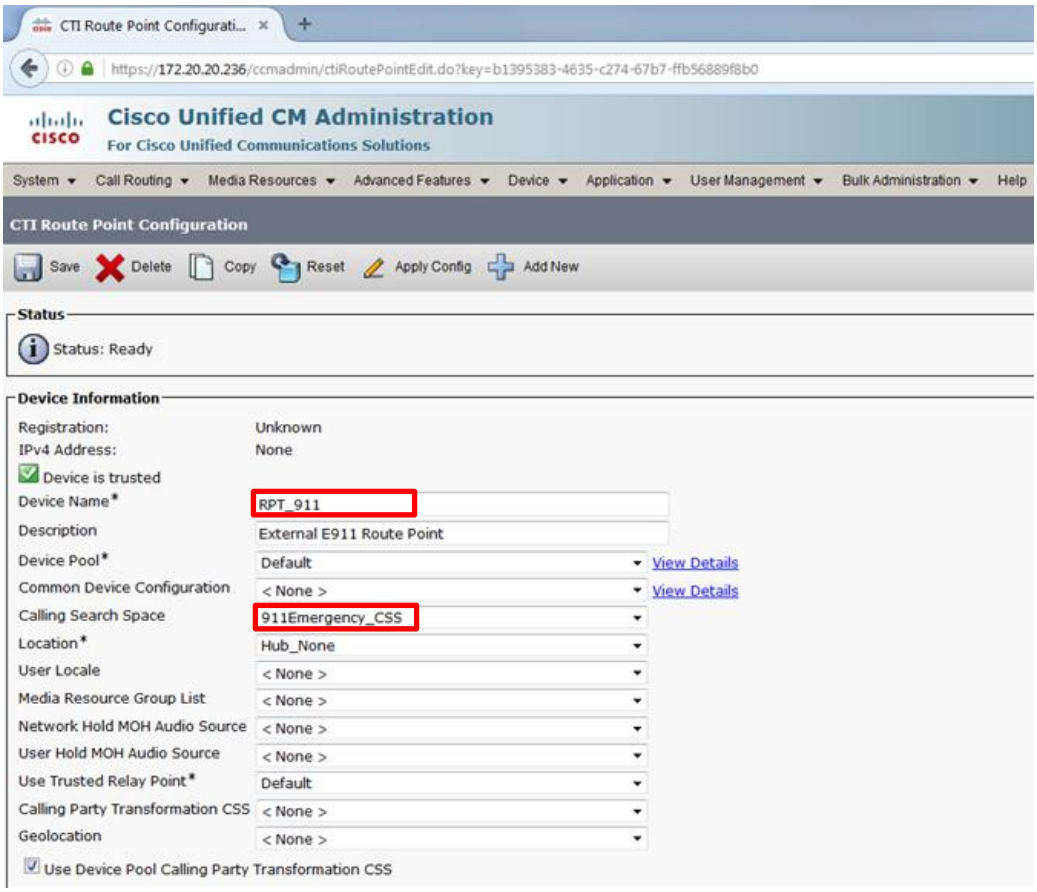


Figure 2: CTI Route Point Configuration

5. Under Association Information, click on “Line [1] – Add a new DN”.

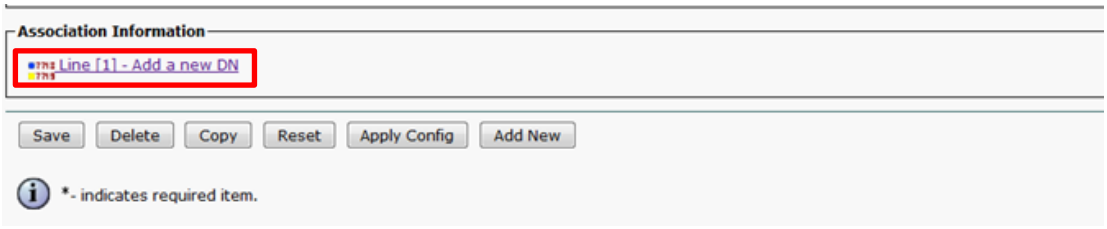


Figure 3: CTI Route Point Configuration – Add DN

6. Add the Directory Number associated with emergency calls, i.e “911”, and select the appropriate partition for e911.

   Note: Any number may be used; however RedSky advises to include 911 as well as 9911.

7. Click Save.

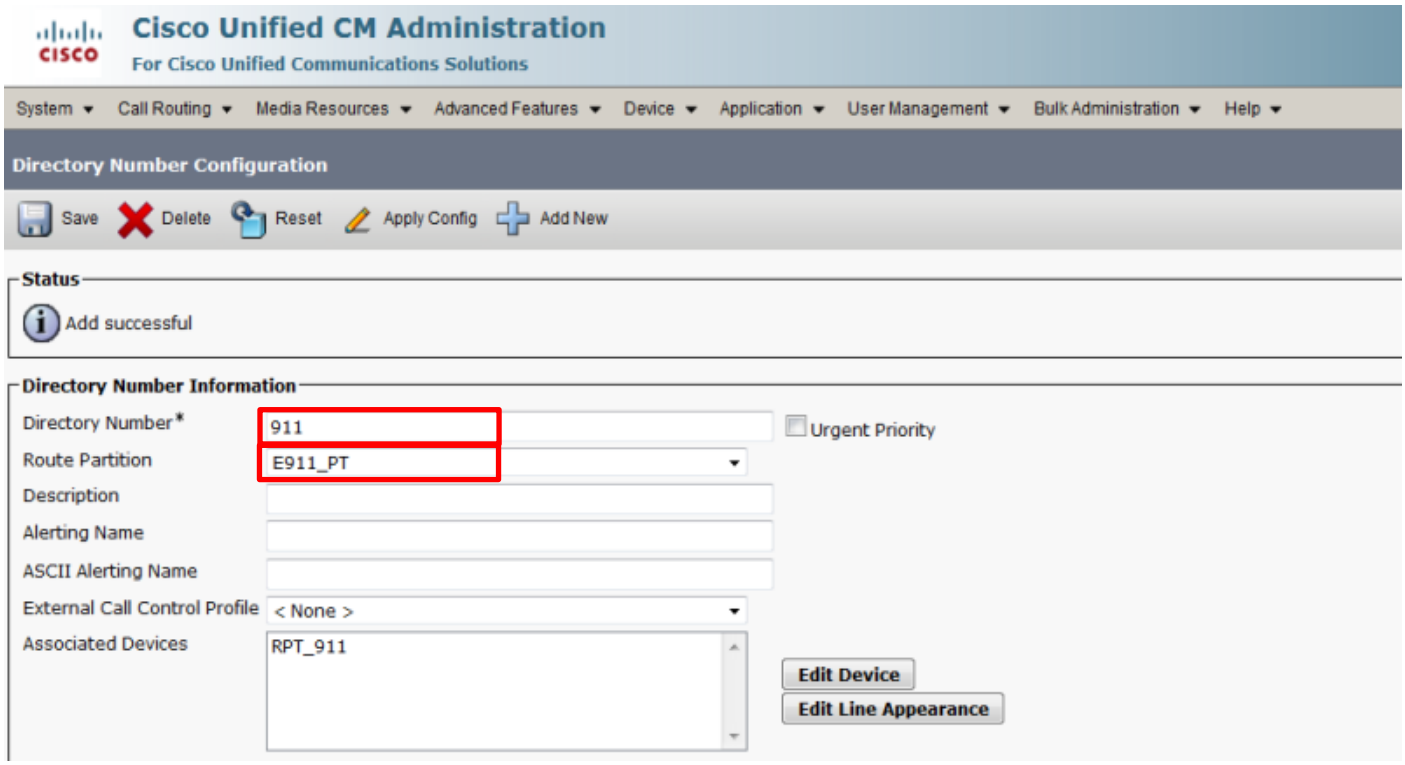


Figure 4: CTI Route Point Configuration – Add DN cont.

Optional – Failover CTI Route Point

The Failover route point will be used in the event that the primary route point is not available.

1. From the Device drop down menu, select CTI Route Point.
2. Click Add New.
3. Add a Device Name that identifies this as a failover route point, and a Calling Search Space. Use the same CSS as the primary route point.
4. Click Save.
5. Under Association Information, click on “Line [1] – Add a new DN”.
6. Add an alternate Directory Number, not one that is typically associated with emergency calls, i.e “912”, and select the appropriate partition for e911.
7. Click Save.
8. Go back to the primary route point and configure the Forward options for the Directory Number to point to the new Failover pattern (912 in this example). This will forward the call to the new failover Route Point in the event the primary Route Point is not available. The CSS used should be able to reach the partition that the failover Route Point is associated with.

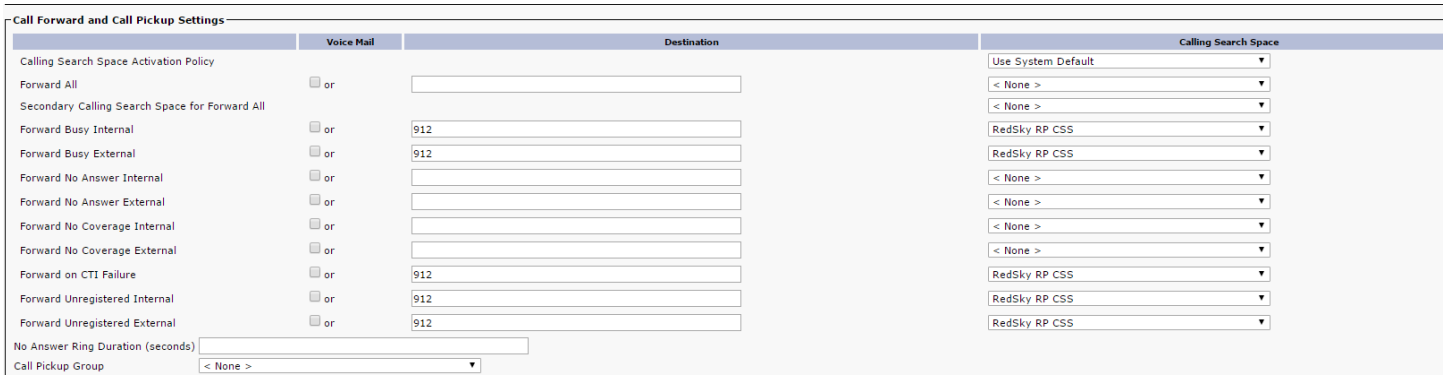


Figure 5: Route Point Forwarding

9. Finally, create a translation pattern in the out the door partition to translate 912 back to 911. The CSS used should also point to the out the door partition. This will insure that the call follows the regular route for 911 calls out of CUCM.

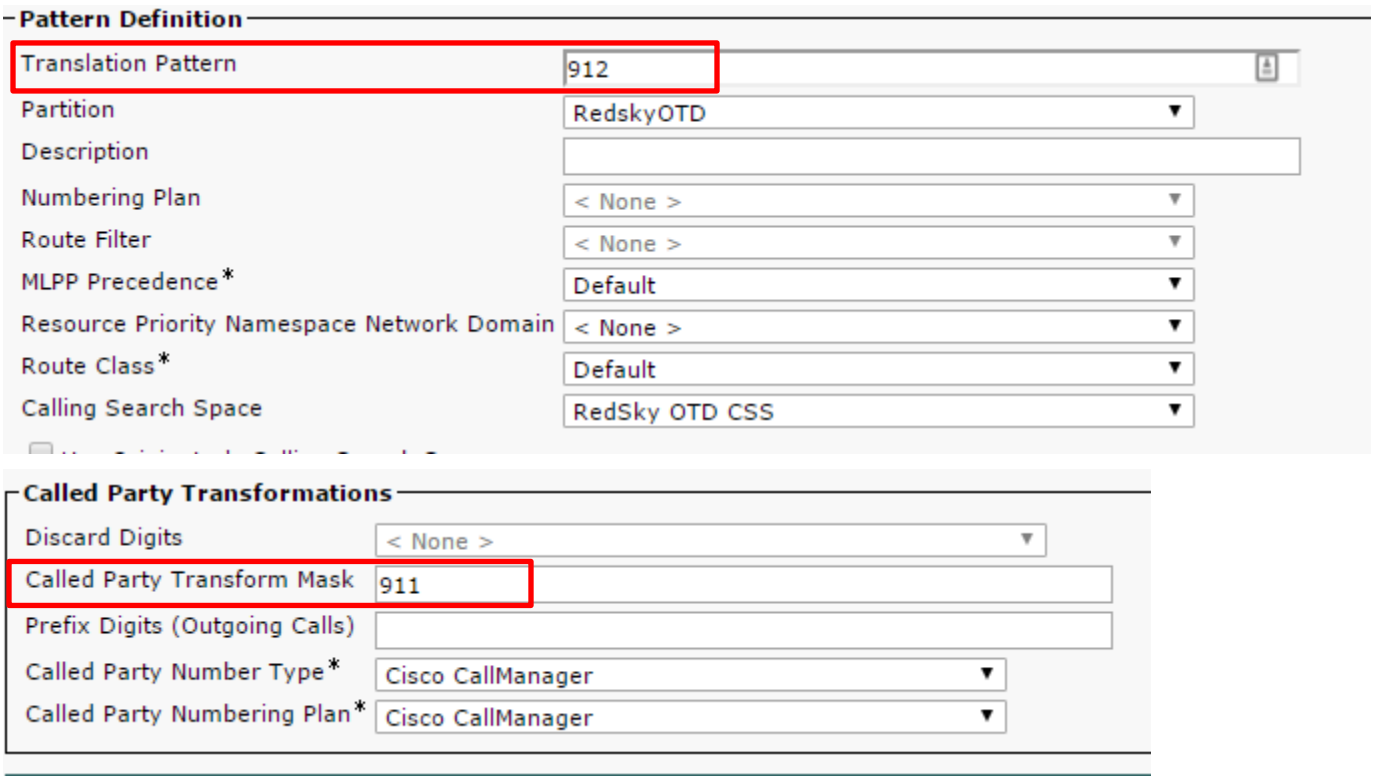


Figure 6: Failover Translation Pattern

Application User

1. From the User Management menu select Application User.
2. Click **Add New**
3. Enter the User ID name and Password.
4. Select the primary route point(s), and failover route point(s), you created in the Device Information Section. Click on Device Association. Select the configured Route Point by adding check to the box and Save Selected/Changes. In the Related Links Box (Top Right) **Back to User** click on Go. The Route Point is added to the Controlled Devices.
5. Click Save.

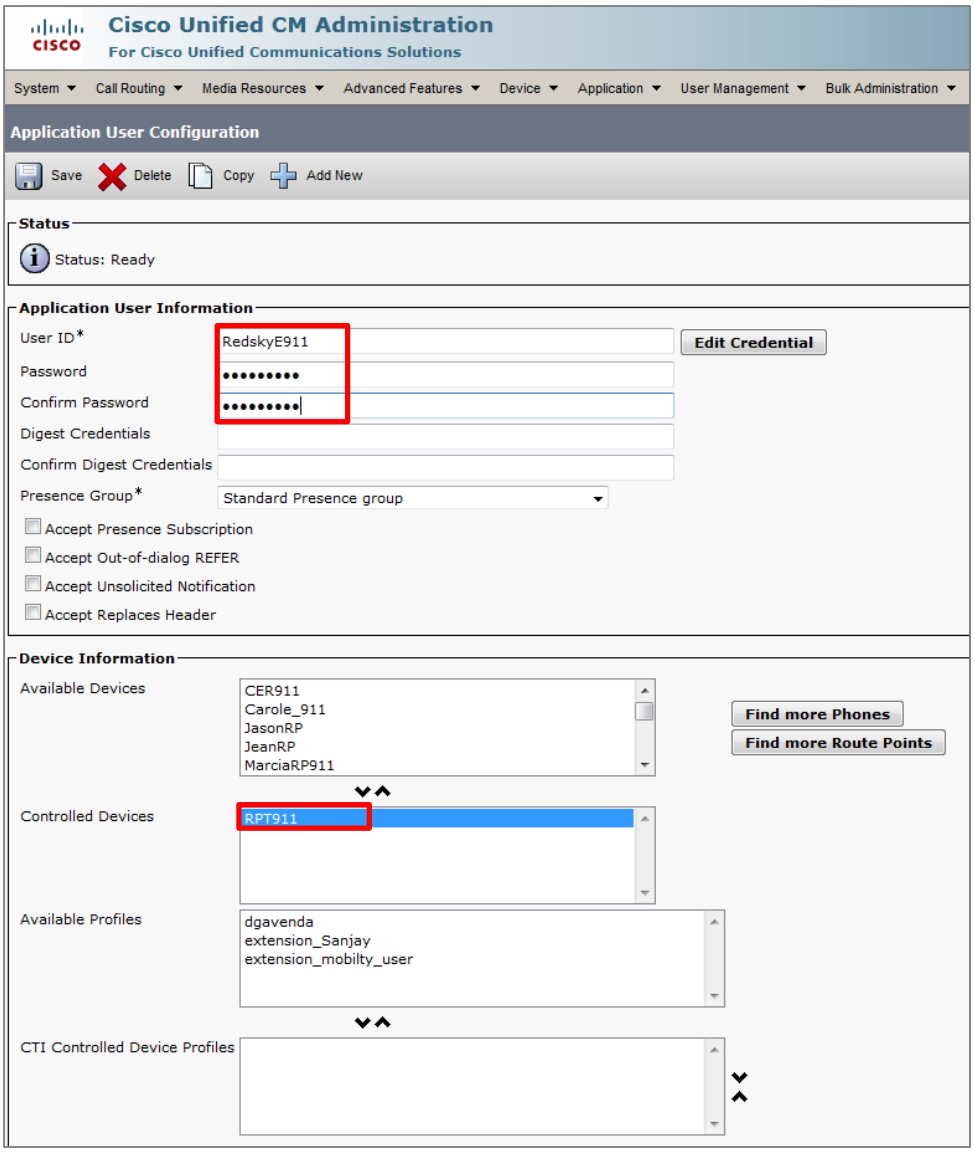


Figure 7: Application User Configuration

User Group Permissions

1. From the User Management Menu > User Setting > Access Control Group.
2. Click Add New and enter the name of the group.
3. Click Save.
4. From the Related Links dropdown menu on the top right, select **Assign Role to Access Control Group**. Click Go.

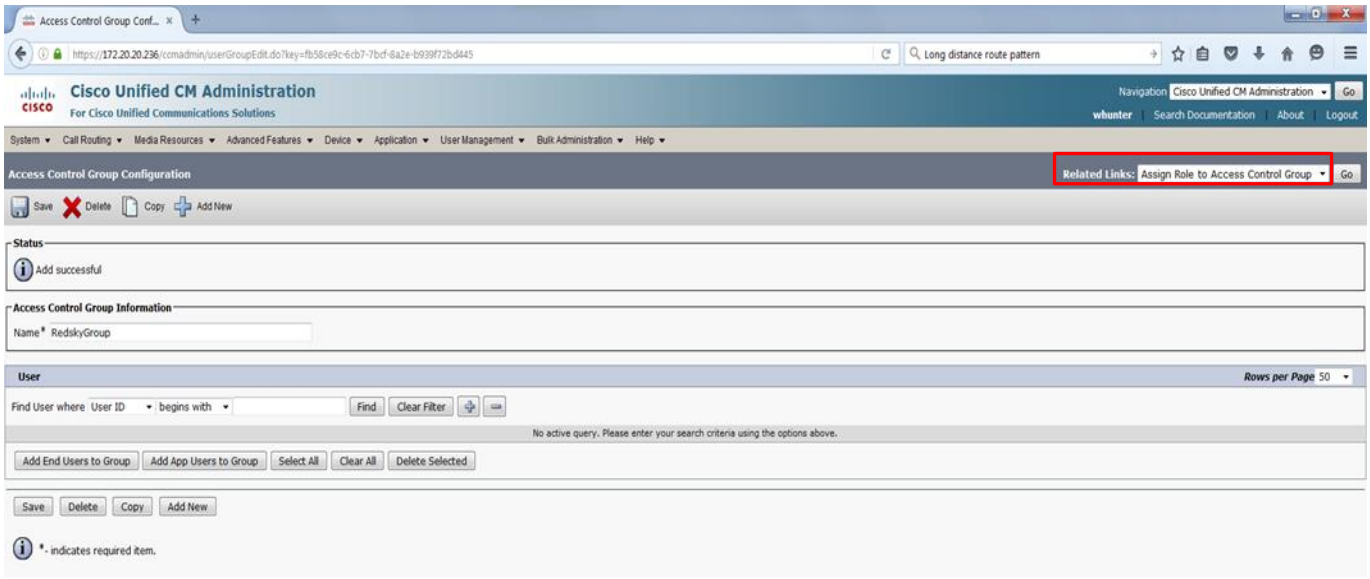


Figure 8: User Group – Related Link Menu

5. Click Assign Role to Group.

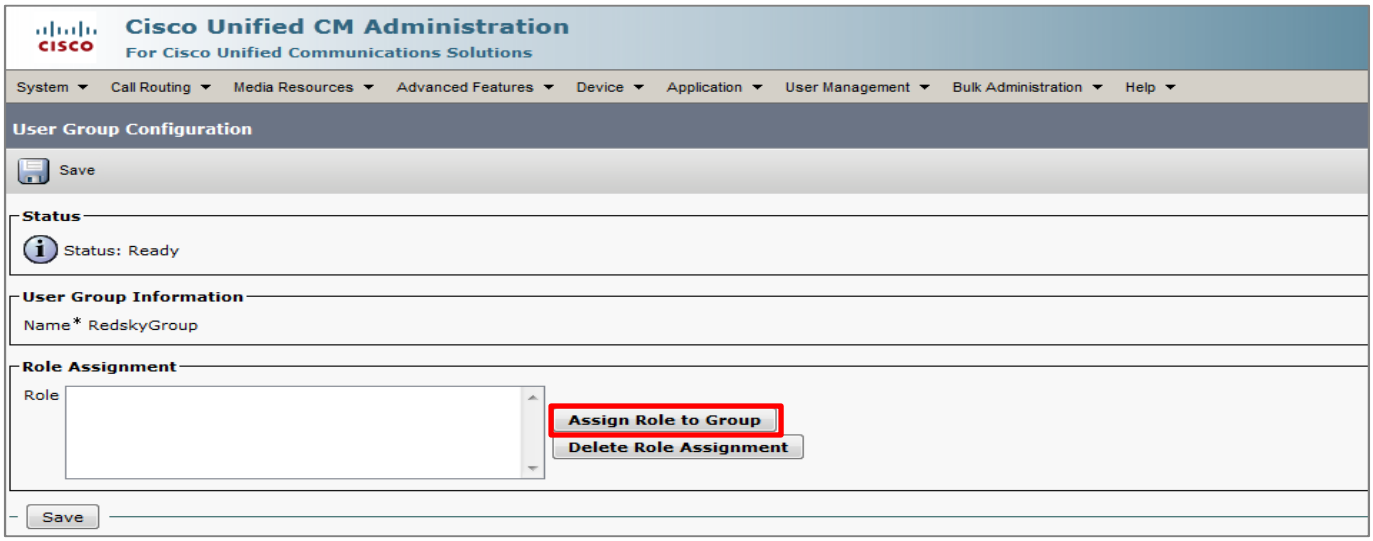


Figure 9: User Group – Assign Roles

6. The Find and List Roles Menu will appear.

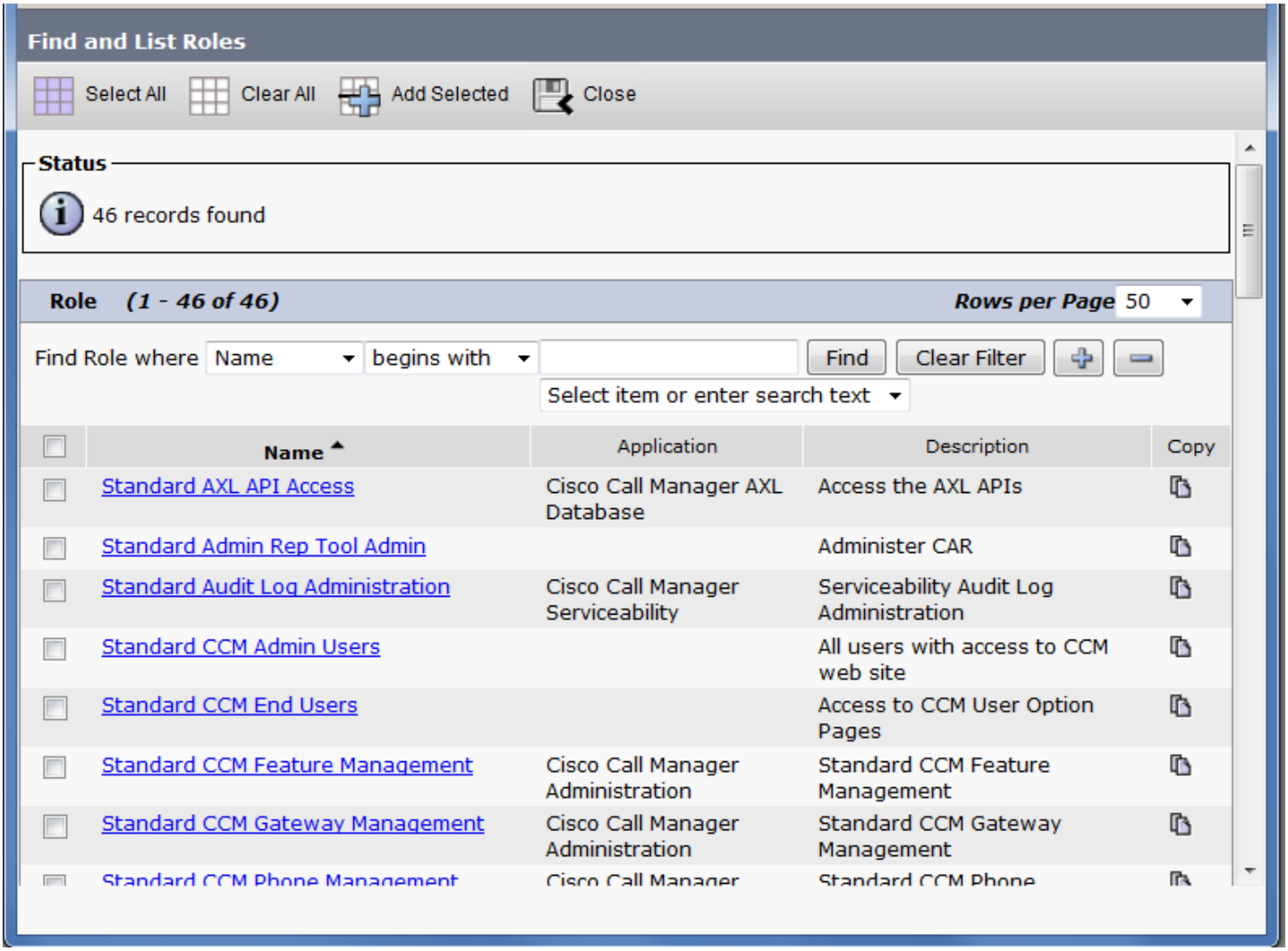


Figure 10: User Group – Find and List Roles Menu

The E911 user should contain the following list of roles:

Standard AXL API Access	Access to the AXL APIs
Standard CCM Admin Users	All users with access to CCM website - Standard CCM Admin Users role can access Cisco Call Manager Administration but cannot make any changes.
Standard CCMADMIN Read Only	Read access to all CCMAdmin resources
Standard CTI Allow Call Monitoring	Allow monitoring of calls
Standard CTI Allow Calling Number Modification	allow calling number modification
Standard CTI Enabled	Enable CTI application control
Standard RealtimeAndTraceCollection	Real-time and Trace Collection
Standard SERVICEABILITY Read Only	Read access to all serviceability

7. Once all the roles have been selected, click Add Selected.

8. Click Save.
9. From the Related Link dropdown menu select **Access Control Group** and click Go.

Figure 11: User Group – Add Application User

10. From the Access Control Group Information, click on the **Add App Users to Group** button

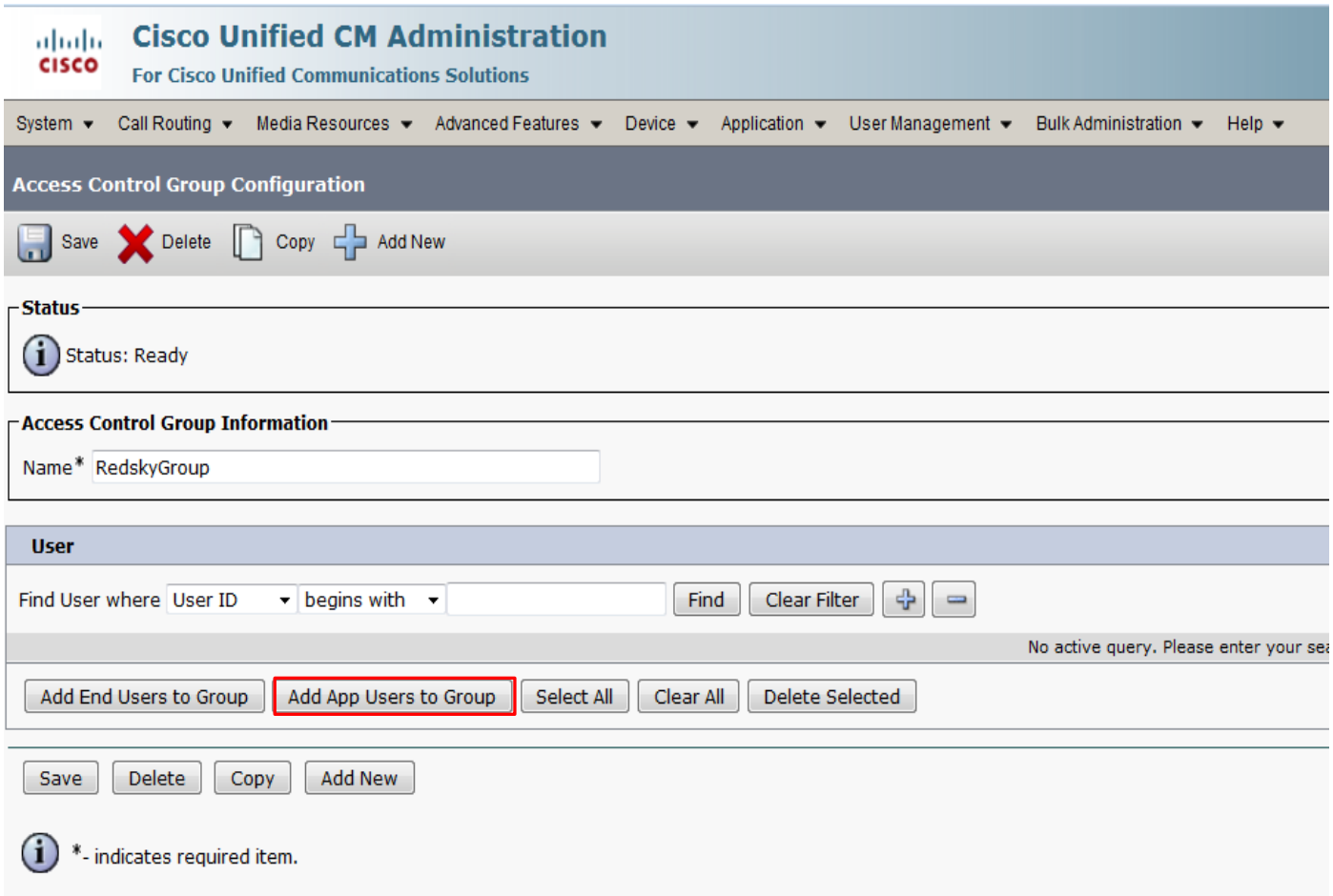


Figure 12: User Group – Add Application User Cont.

11. The Find and List Application Users menu will appear.
12. Select the Application User that was created.
13. Click Add Selected.
14. Click Save.

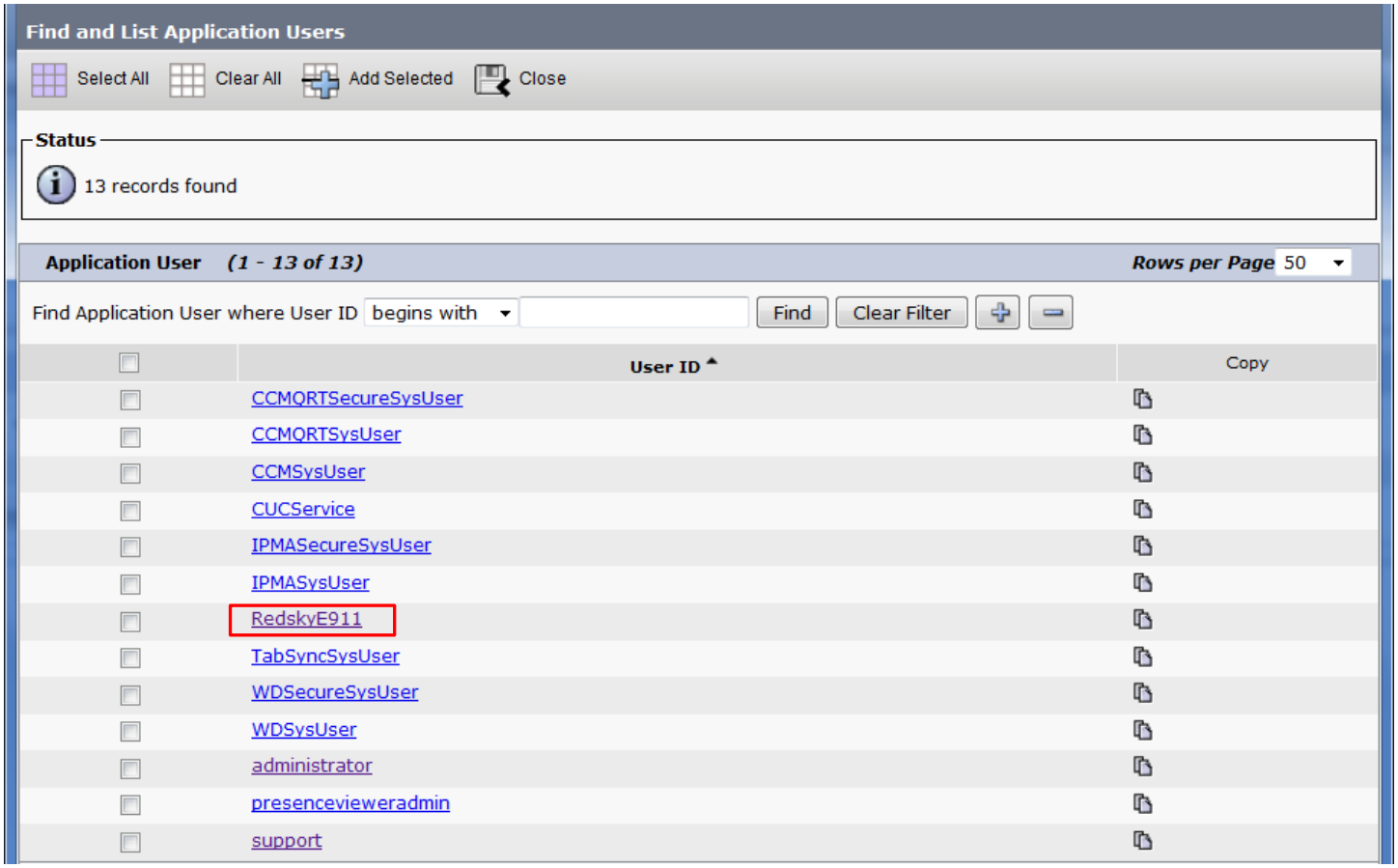


Figure 13: User Group – Find and List Application Users Menu

Services

1. Select Cisco Unified Serviceability from the Navigation drop down menu.
2. Go to Tools > Service Activation and select the appropriate server.

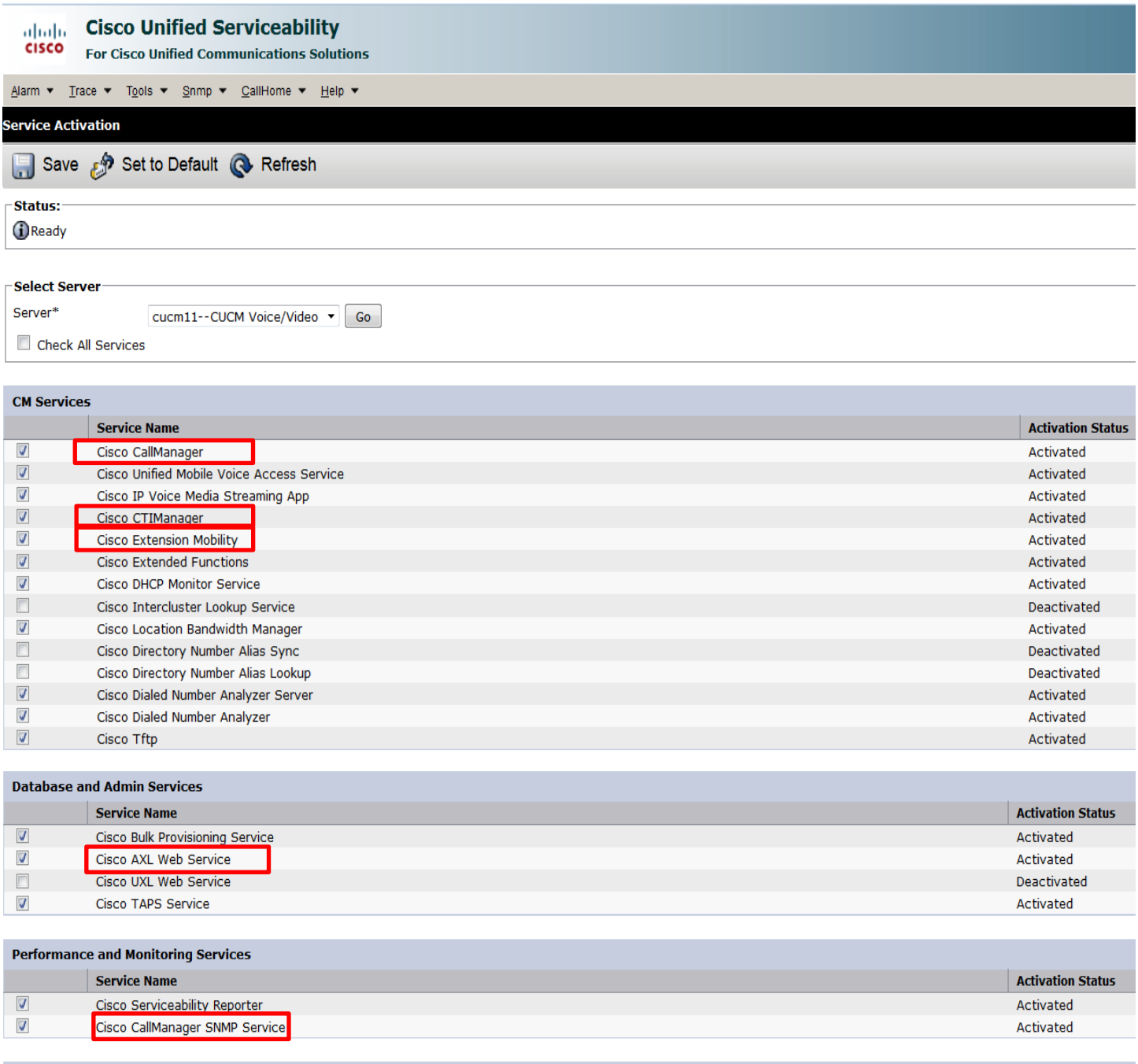


Figure 14: Services

The following Services should be running (minimum):

Cisco CallManager	
Cisco CTIManager	911 call monitoring (EON/JTAPI connectivity)
Cisco Extension Mobility	
Cisco AXL Web Service	Administrative connectivity (downloading from the PBX)
Cisco CallManager SNMP Service	Phone registration monitoring

Sample Configuration Diagram

The diagram below demonstrates how the Call Manager using E911 Manager routes an emergency call. In this example the device with extension 1000 initiates the emergency 911 call. The Call Manager matches the 911 to the E911 partition in the LinePhone_CSS to the E911 partition in the Route Point. The call then goes through the Route Point where the E911 Manager inserts the ELIN into the call stream. The Route Point RPT_911 matches 911 to the route pattern in the 911Emergency_PT contained within the 911Emergency_CSS. The 911 call with the ELIN is routed through one of the interfaces whether PRI, FXO, SIP assigned to route group Redsky_RG. The Redsky_RG is added to the Redsky_RL route list.

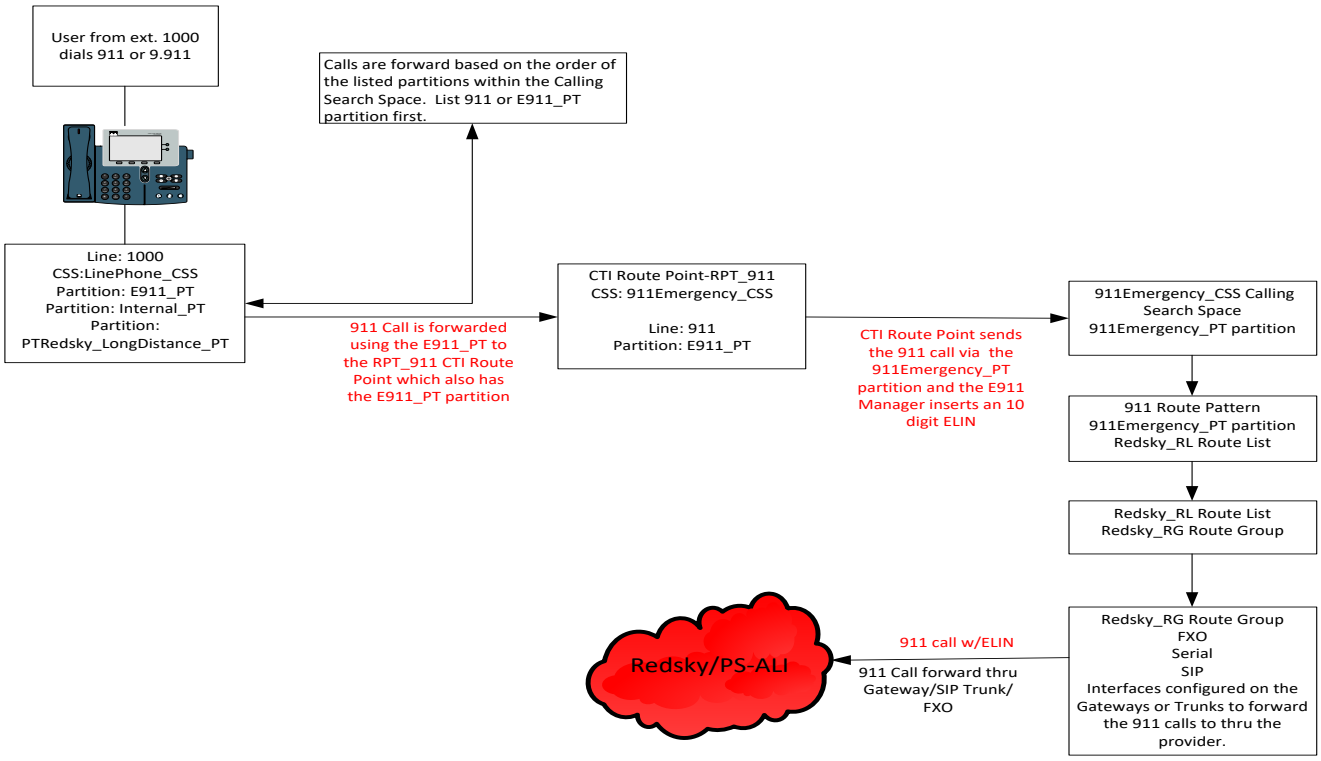
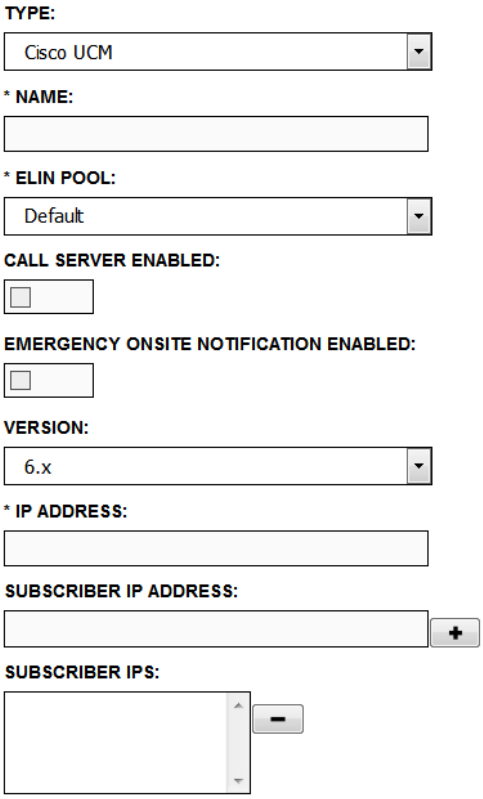


Figure 15: Call Flow Diagram

E911 Manager Configuration

Below is a brief description of the fields available in E911 Manager for a CUCM call server.



Type: Cisco UCM

Name: Only used to uniquely identify in E911 Manager

ELIN Pool: ELINs matching call server dial plan

Call Server Enabled: Activates E911Manager connection to CUCM

EON Enabled: Adds ability for alerts on emergency calls

Version: Current CUCM version

IP Address: IP of the publisher

Subscriber IP Address: IPs of subscribers in that cluster

Figure 16: E911 Manager config 1

SNMP Port: standard port is 161 but can be changed

SNMP Version: V2 requires a community string V3: Username, auth string, auth type, privacy string, & priv type

Add Route Point: CTI route point device name

Failover Route Point: Optional route point configured above for Use in the instance the primary is no longer available

Route Point Polling Interval: Time between E911 Manager Checking for Route Point registration.

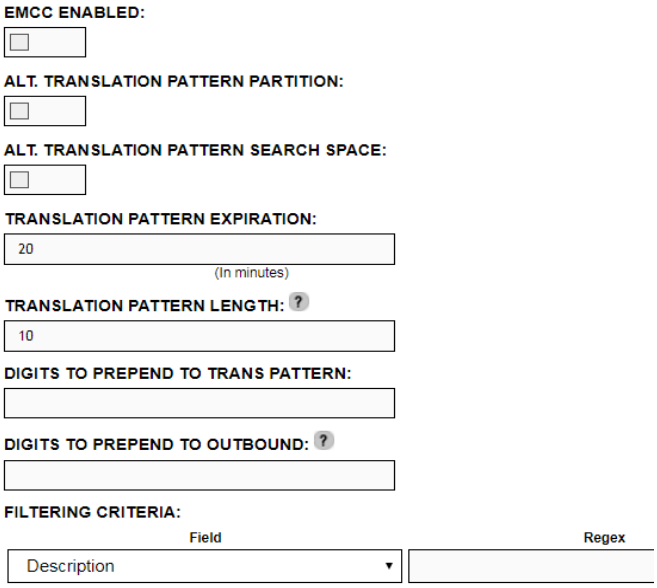
SOAP Login: Application User also used for JTAPI

SOAP Port: Used for SOAP and AXL queries

SOAP Retry Attempts: Amount of retries before timeout

Figure 16: E911 Manager config 1

Figure 17: E911 Manager config 2



EMCC Enabled: Devices that do not show up on the current PBX, are treated as potential EMCC devices, and E911 Manager sends requests to all other Cisco PBXes to try to get the proper device information. If it is not enabled, E911 Manager will not make those requests at all. E911 Manager will send requests only to other clusters where EMCC is also enabled.

Alt. Translation Pattern Partition: gives users the flexibility to have E911 Manager write the translation pattern to different partition in the CUCM.

Alt Translation Pattern Search Space: gives users the flexibility to have E911 Manager use a different search space when writing the translation pattern CUCM.

Translation Pattern Expiration: Defines how long the translation pattern E911 Manager creates will be active. This allows a PSAP to call the person who dialed 911 back. The default is 20 minutes

Translation Pattern Length: Defines how many digits the translation pattern should be. The default is 10 digits.

Digits to Prepend to Trans Pattern: Defines what digits to add onto the right side of the translation pattern. For example, it can give an alternative area code to the translation pattern.

Digits to Prepend to Outbound: Defines what digits to add to the left of the outbound ELIN. This can be used to add a +1 to the front of the ELINs.

Filtering Criteria: E911 Manager allows devices to be excluded from E911 Manager based on filtering criteria defined through Regular Expressions. Such fields include Description, Name, IP, CSS, Device Pool, pattern, UUID, and other attributes.