Configuration and Troubleshoot of Logical Partitioning and Geolocation

Contents

[Introduction](#)
[Prerequisites](#)
[Components Used](#)
[Background Information](#)
[Elements of Logical Partitioning](#)
[Geolocation](#)
[Geolocation filter](#)
[Logical Partition Policy](#)
[Configuration](#)
[Troubleshoot](#)
[Points to ponder](#)
[References](#)
[Known bugs](#)

Introduction

This document describes how to configure Logical Partitioning and Geolocation in Cisco Unified Communications Manager (CUCM).

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communication Manager

Components Used

- Cisco Unified Communications Manager 8.6 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The logical partitioning feature ensures that a single system can be used to support both types of calls as long as calls that pass through a Public Switched Telephone Network (PSTN) gateway don't connect directly to a Voice over IP (VoIP) phone or VoIP PSTN gateway in another

geographic location (geolocation) even when a mid call feature is invoked.

In some countries such as India, there are Telecom regulations that have to be met at the enterprise level. Because of which the companies are liable to set up a voice infrastructure. They are setup such that the local PSTN is used exclusively when connecting calls outside the enterprise. According to the Telecom Regulatory Authority (TRAI), PSTN telephony network in India must never be interconnected with VoIP Telephony network for the purpose of Toll ByPass.

This requires that the voice system be partitioned logically into two systems: one VoIP within the enterprise and a second one to access the local PSTN.

It was quite difficult to maintain this sort of voice system with the Calling Search Space (CSS) and Partition feature in CUCM. CSS and Partition can restrict the basic calls, but it fails to restrict mid call features like redirect and join.

Elements of Logical Partitioning

Geolocation

CUCM requires provisioning of identifiers for assigning to the devices like phones, gateways, trunks, etc. Geolocation is a standard that can be used as an idenfitier in Logical Partitioning.

Geolocation is used to specify the physical location based on up to 17 parameters: Country 2 letter abbreviation, State (A1), County (A2), City (A3), District (A4), Neighborhood (A5), Street (A6), Direction (PRD), Street Suffix (POD), House Number (HNO) and House Number Suffix (HNS) among others.

Geolocation filter

A typical Logical Partition policy configuration uses only subset of fields in Geolocation policy record. This selection is narrowed down by Geolocation filter. The fields that are selected in Geolocation Filter are used by the Logical Partitioning feature.

Logical Partition Policy

In CUCM, Logical Partitioning is defined as a call control feature that can be used to restrict the communication between these VoIP entities with the help of Logical partitioning policies.

- IP phone to/from Gateway
- Gateway to Gateway
- IP phone to/from Trunk (ICT/SIP trunk)
- Gateway to/from Trunk (ICT/SIP trunk)

The devices in Logical Partition are categorized as interior and border. These are the devices classified as interior:

1. Phones (SCCP, SIP, third party)
2. VG224 analog phones
3. MGCP port (FXS)
4. Cisco Unity Voice Mail (SCCP)

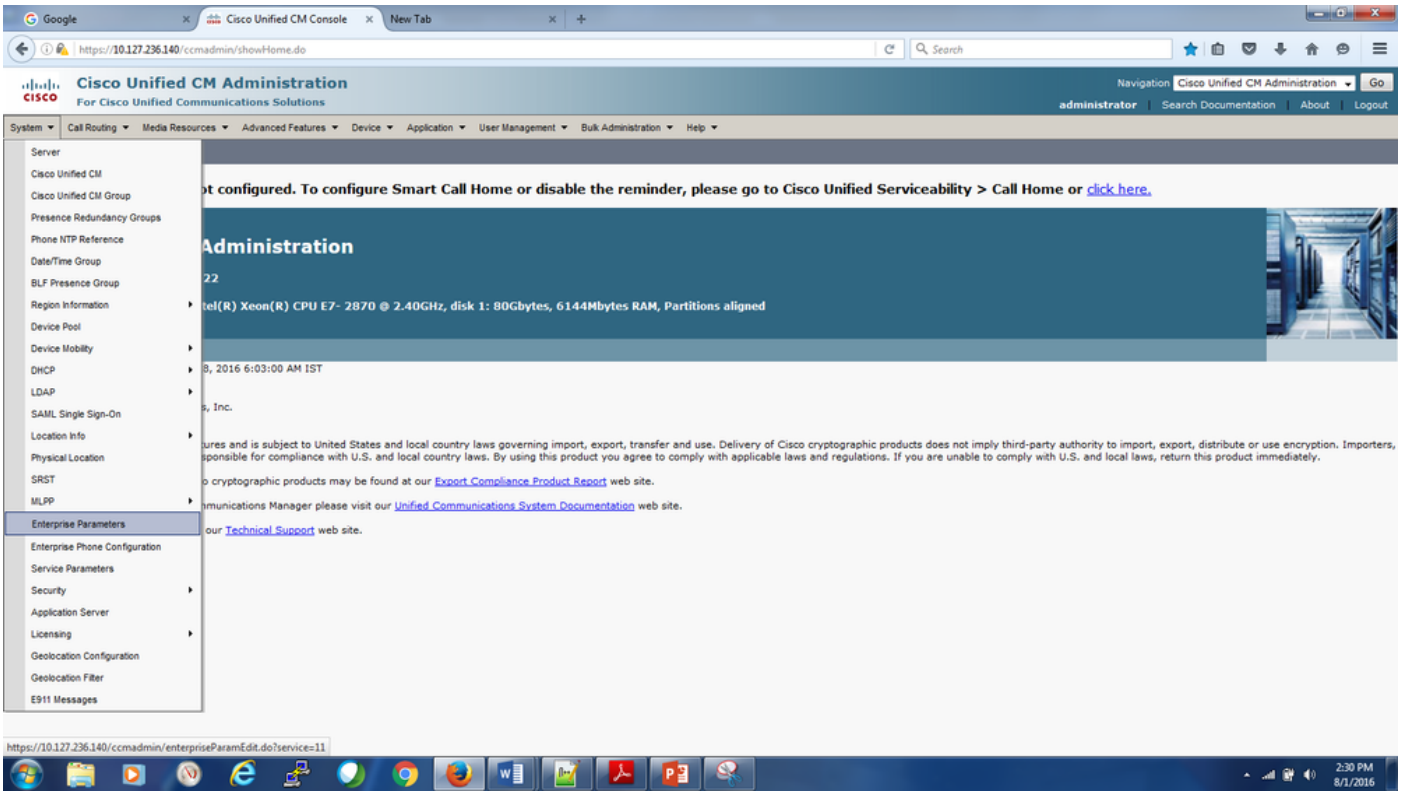
5. CTI Route Point, CTI Port
6. QSIG Gateway or ICT

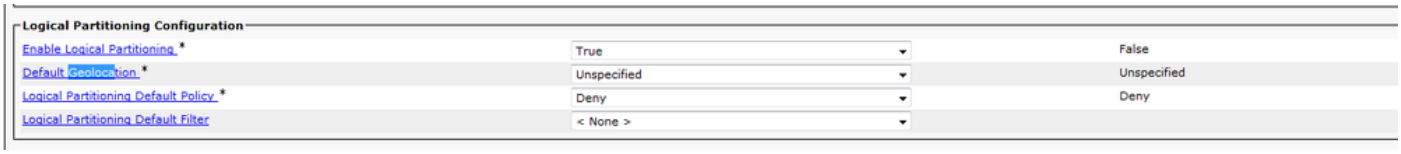
These devices are categorized as the border:

1. Gateway
2. Intercluster trunk (ICT)
3. H.225 trunk
4. SIP trunk
5. MGCP port (E1, T1, PRI, BRI, FXO)

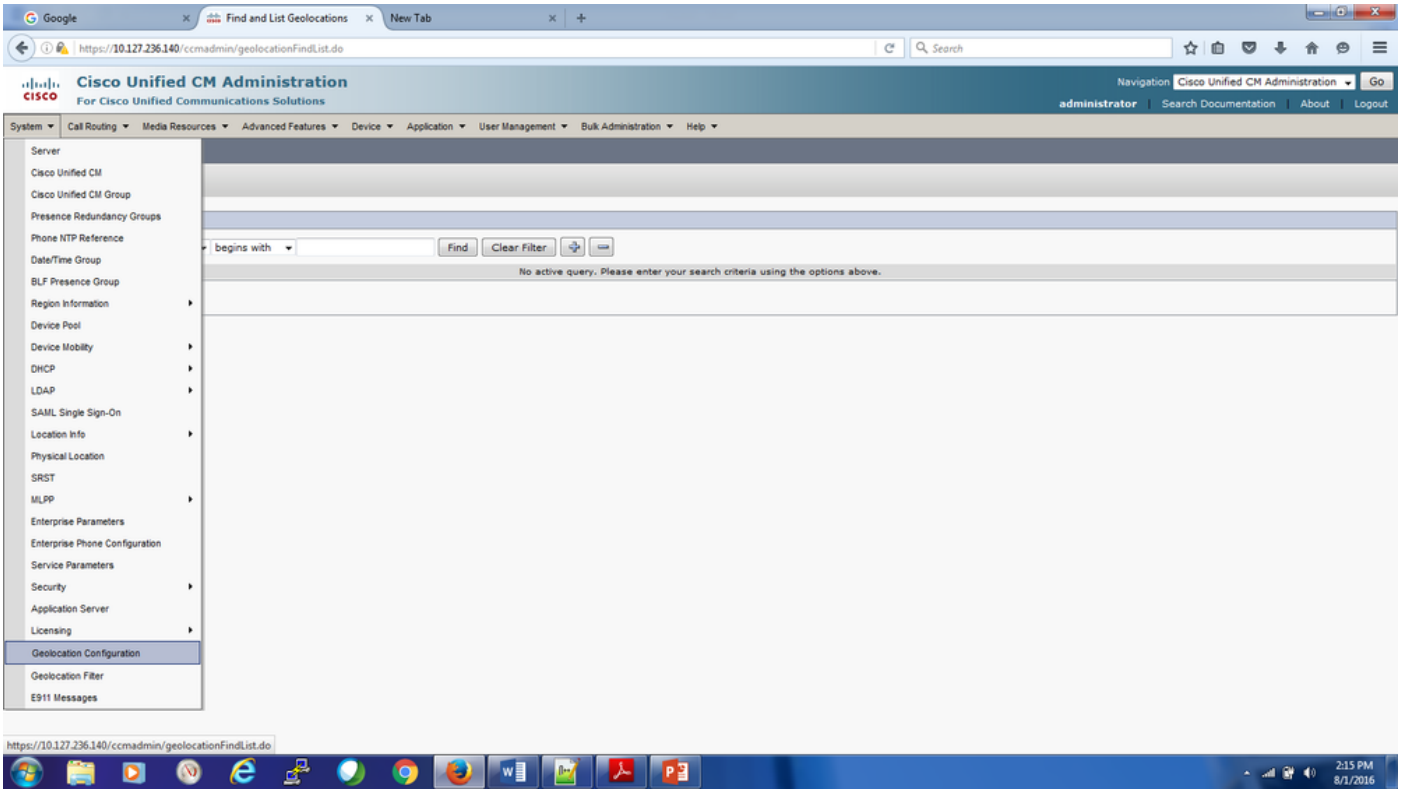
Configuration

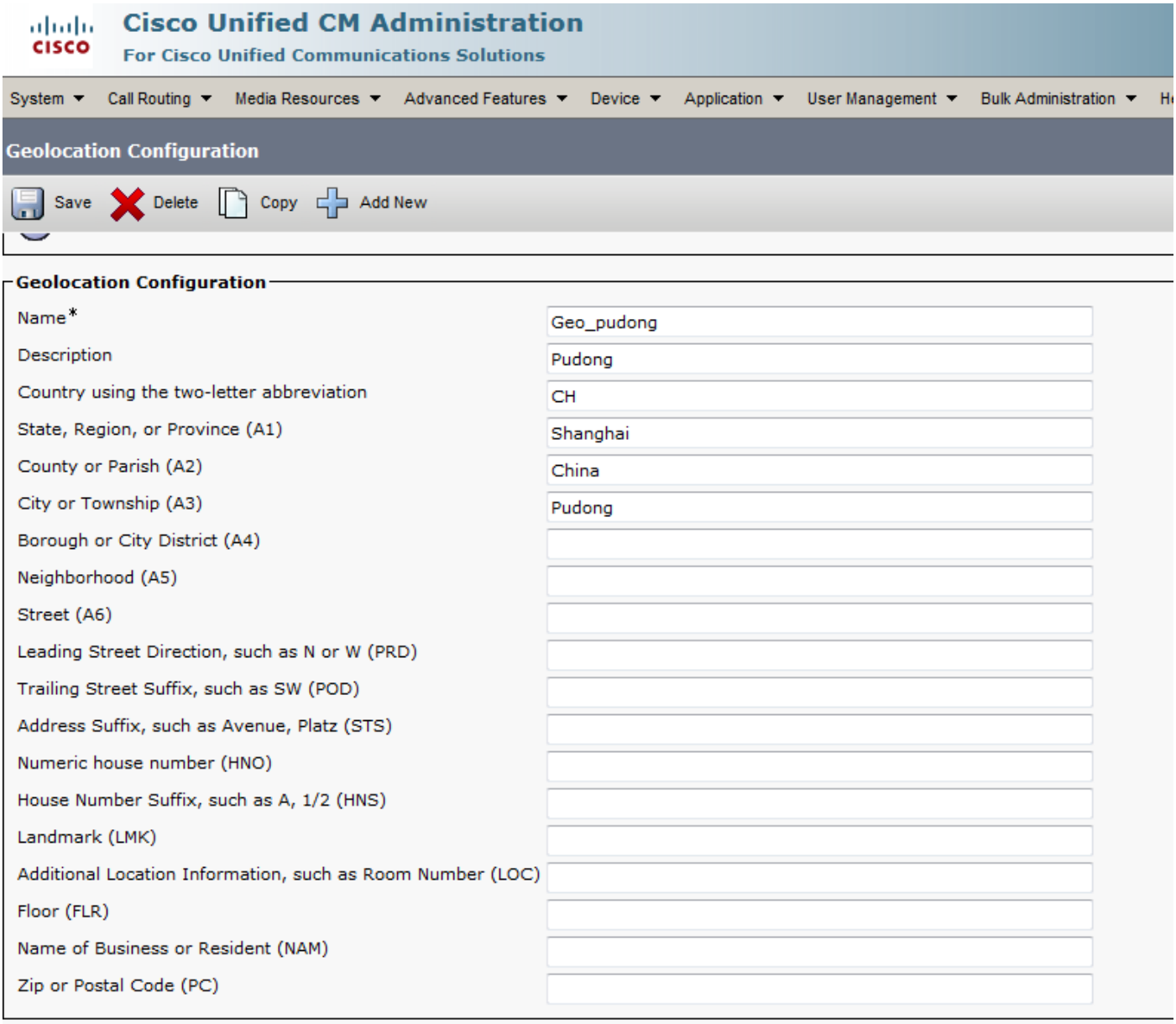
Step 1. Default Geolocation is applicable for the devices in which no Geolocation is configured and do not participate in the Logical Partitioning. To set the default Geolocation policy plays a major role, if it is set to allow then it is necessary to appropriate Logical Partition policies with deny functionality and vice-versa.



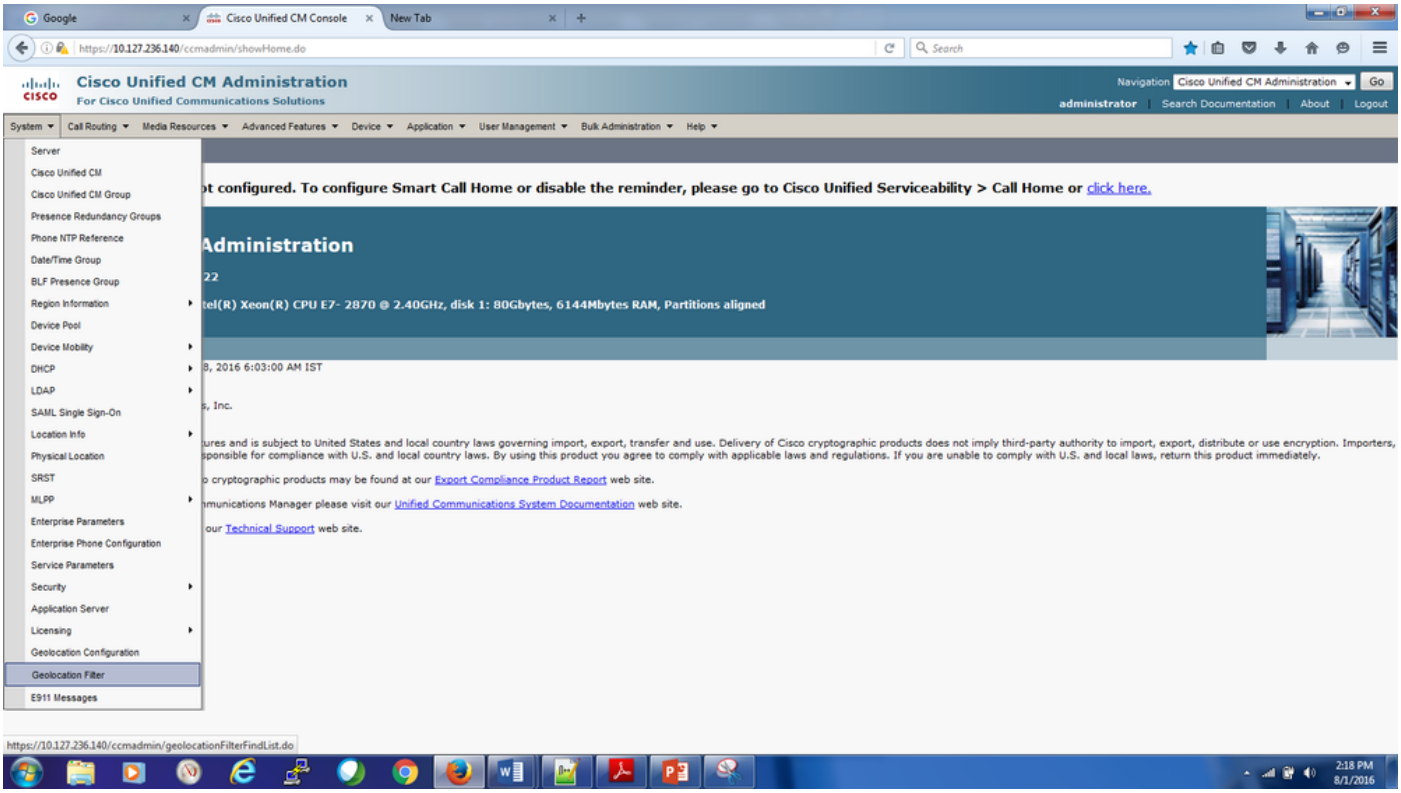


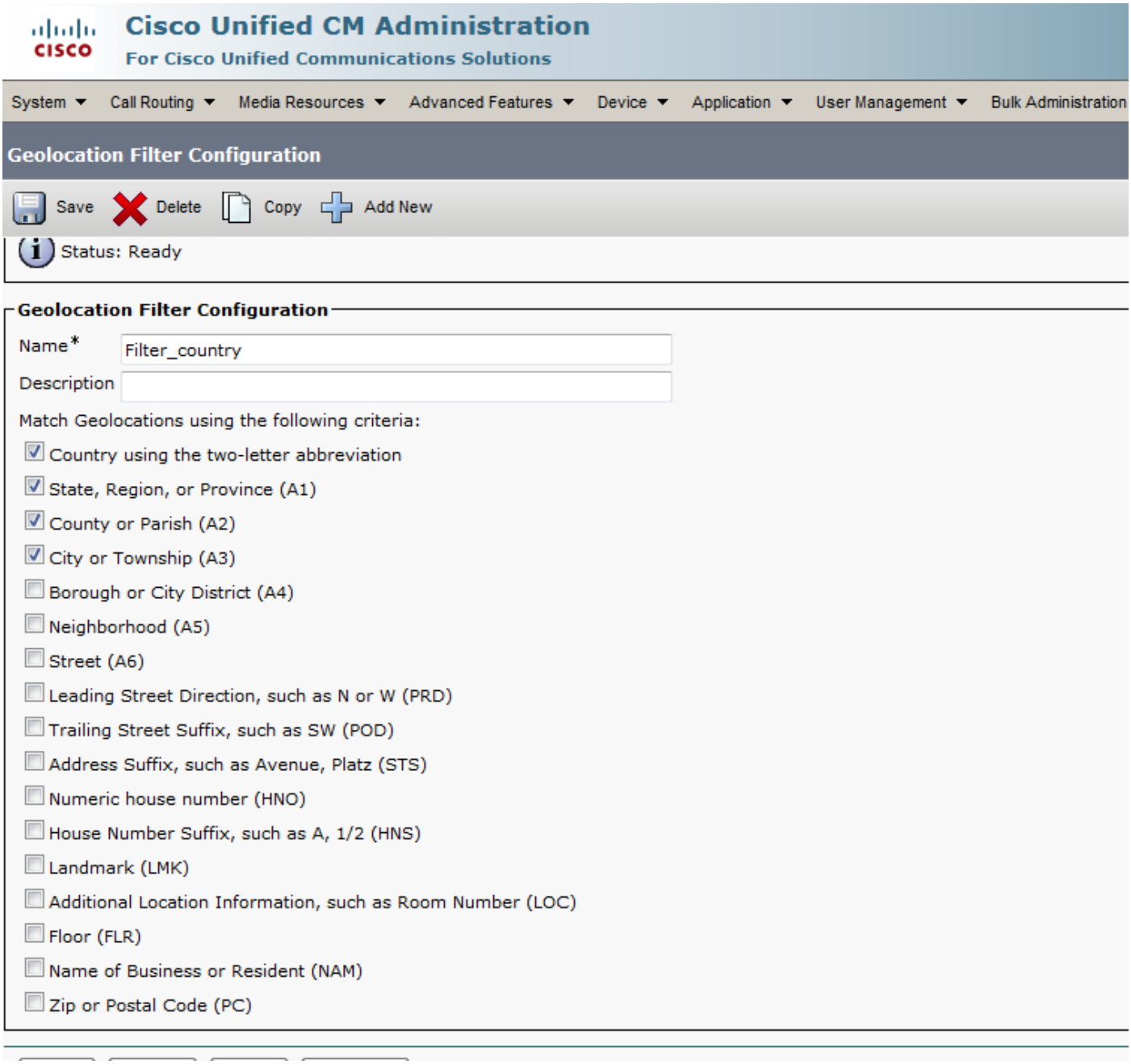
Step 2. Go to System-> Geolocation Configuration and add the information related to the location. This acts as an identifier for the devices that are associated with this particular Geolocation.


Google
Find and List Geolocations
New Tab
https://10.127.236.140/ccmadmin/geolocationFindList.do
Search
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
administrator | Search Documentation | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Server
Cisco Unified CM
Cisco Unified CM Group
Presence Redundancy Groups
Phone NTP Reference
Date/Time Group
BLF Presence Group
Region Information
Device Pool
Device Mobility
DHCP
LDAP
SAML Single Sign-On
Location Info
Physical Location
SRST
MLPP
Enterprise Parameters
Enterprise Phone Configuration
Service Parameters
Security
Application Server
Licensing
Geolocation Configuration
Geolocation Filter
E911 Messages
begins with
Find
Clear Filter
No active query. Please enter your search criteria using the options above.
https://10.127.236.140/ccmadmin/geolocationFindList.do
2:15 PM
8/1/2016

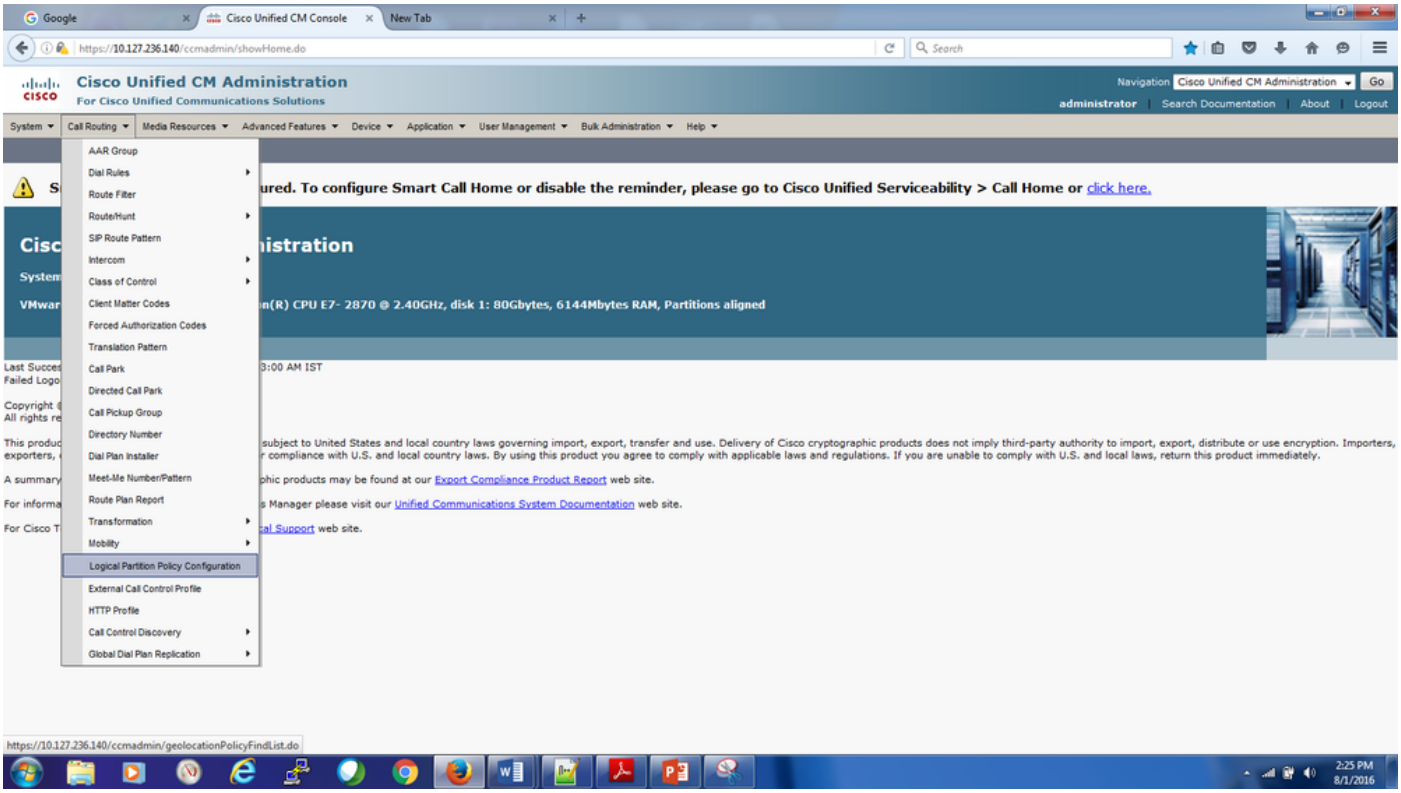


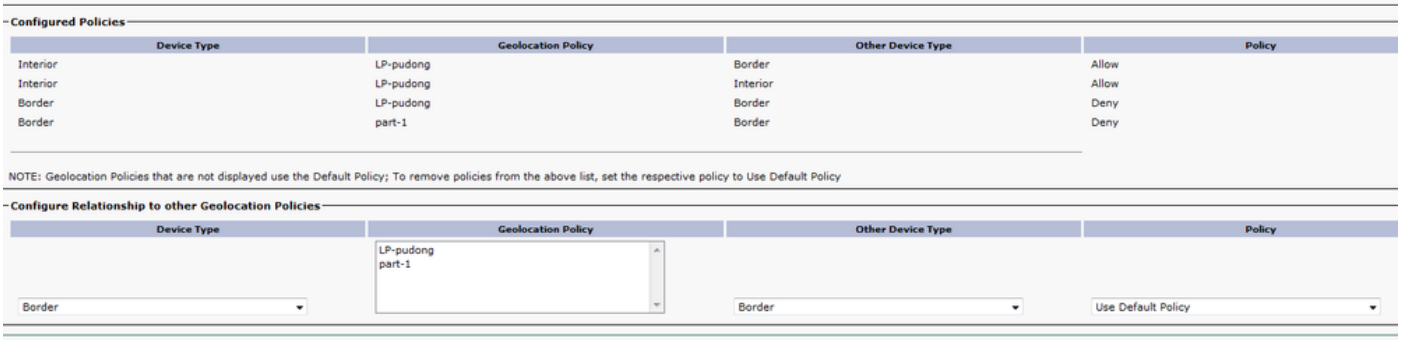
Step 3. Go to System-> Geolocation Filter and check the fields in the Geolocation Filter configuration based on what the logical policy is required to filter against.


Google
Cisco Unified CM Console
New Tab
https://10.127.236.140/ccmadmin/showHome.do
Search
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
administrator | Search Documentation | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Server
Cisco Unified CM
Cisco Unified CM Group
Presence Redundancy Groups
Phone NTP Reference
Date/Time Group
BLF Presence Group
Region Information
Device Pool
Device Mobility
DHCP
LDAP
SAML Single Sign-On
Location Info
Physical Location
SRST
MLPP
Enterprise Parameters
Enterprise Phone Configuration
Service Parameters
Security
Application Server
Licensing
Geolocation Configuration
Geolocation Filter
E911 Messages
ot configured. To configure Smart Call Home or disable the reminder, please go to Cisco Unified Serviceability > Call Home or click here.
Administration
22
tel(R) Xeon(R) CPU E7- 2870 @ 2.40GHz, disk 1: 80Gbytes, 6144Mbytes RAM, Partitions aligned
8, 2016 6:03:00 AM IST
s, Inc.
ures and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, sponsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
o cryptographic products may be found at our Export Compliance Product Report web site.
mmunications Manager please visit our Unified Communications System Documentation web site.
our Technical Support web site.
https://10.127.236.140/ccmadmin/geolocationFilterFindList.do
2:18 PM
8/1/2016



Step 4. Configure the logical partition policy. This is most important part of the configuration as all the decisions to allow or deny the calls depend on its configuration.





Step 5. Go to the device configuration page of the phone and apply the geolocation depending on where the phone is located.

Similarly go to the device pool and add the geolocation configuration.

Step 6. Next go to the configuration page for the Gateway/Trunk/MGCP port that acts as an interface to the PSTN and apply the geolocation configuration and the geolocation filter.

Troubleshoot

Step 1.Check in Enterprise Parameters that **Enable Logical Partitioning** option is set to **True**.

Step 2. Make sure that the devices are associated with a valid geolocation at device or device pool level.

Step 3. Check in the configuration page that the device is associated with a valid geolocation filter, having selection of some of the geolocation fields at device or device pool level.

Step 4. Make sure case sensitivity is correct for fields of the LP GeolocationPolicy records and match with the geolocation records configuration.

Step 5. The geolocation configuration, the filters and the policies can also be verified from the CLI with the help of these SQL commands.

```
run sql select * from geolocationfilter
run sql select * from geolocationpolicy
run sql select * from geolocationpolicymatrix
run sql select * from typelogicalpartitionpolicy
```

Step 6. After the basic configuration is checked, verify the relationship set between geolocation policies. When Enterprise Parameter **Logical Partitioning Default Policy** is set to **Deny**, check if **Allow** logical partition policies between Geolocation Policy of a Gateway & VoIP site are configured. To the contrary, if default policy is **Allow**, check if **Deny** logical partition policies are configured.

Step 7. Make sure there are no overlapping or conflicting policies configured.

Example.

GeoLocation Logical Partitioning Policy Matrix Summary

Lists records from the GeoLocation Logical Partitioning Policy Matrix for LP-India.

Device Type A	GeoLocation Policy Name A	Device Type B	GeoLocation Policy Name B	Logical Partitioning Policy
Interior	LP-India	Border	LP-pudong	Allow
Border	LP-pudong	Interior	LP-India	Deny

LP-India->Interior LP-Pudong->Border Allow

LP-Pudong->Border LP-India->Interior Deny

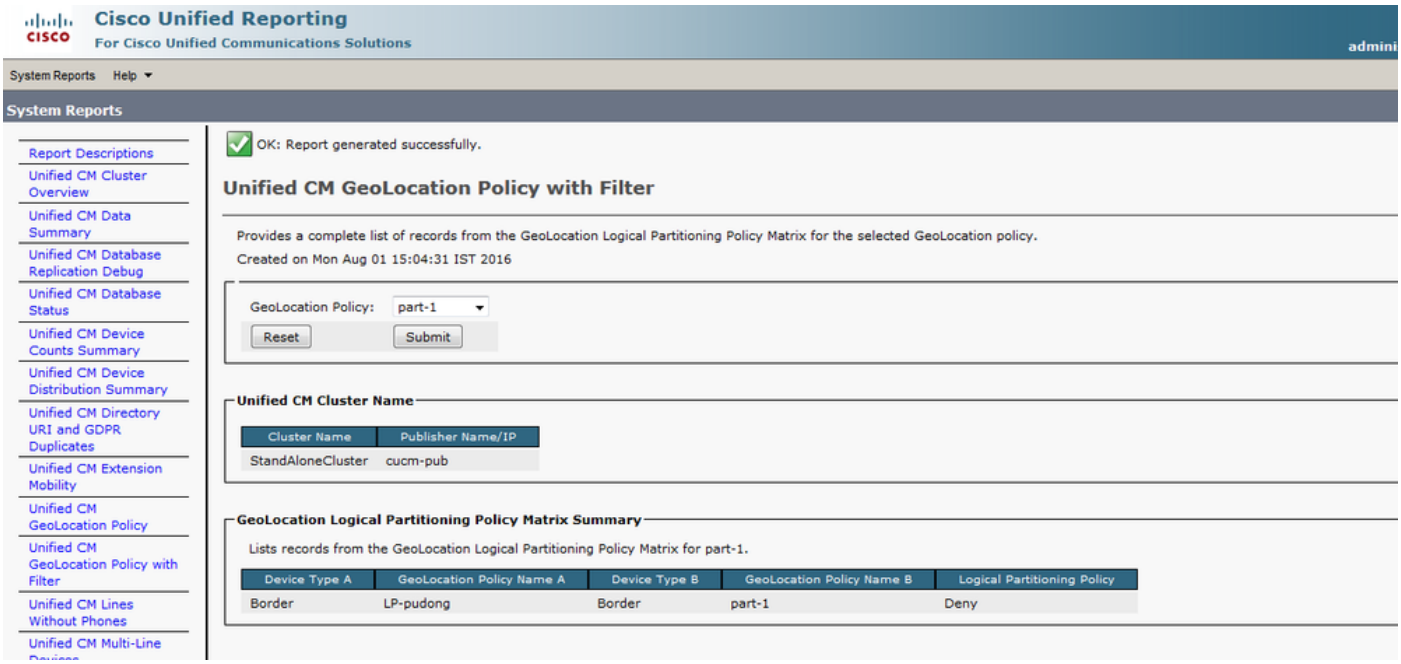
Here the logical relationship between policies have a conflict. If a logical policy interior LP-India to Border LP-pudong is configured, it implies that this relation holds true for Border-LP pudong to LP-India. These policies are bi-directional in nature.

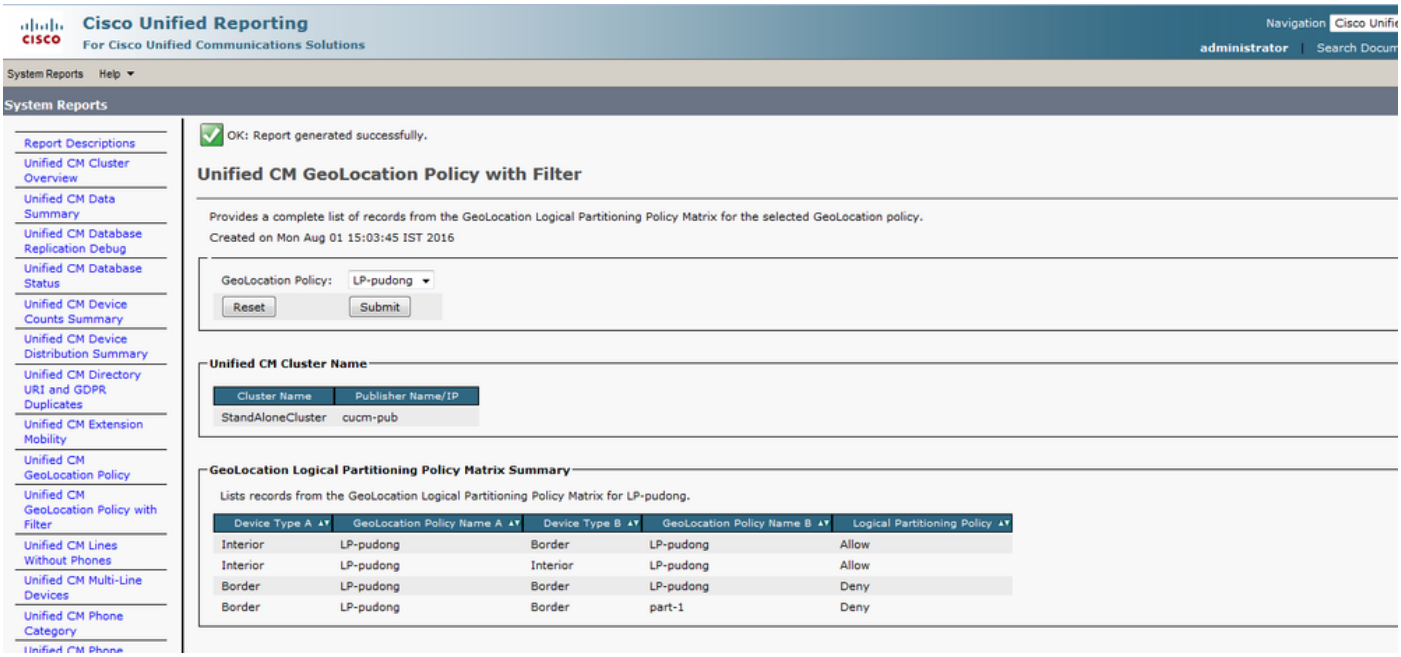
So in this example, according to first policy, internal IP phones in Pudong location are allowed to call out via PRI-India. At the same time, PSTN calls from the PRI-India to the IP phones in Pudong Geolocation are allowed.

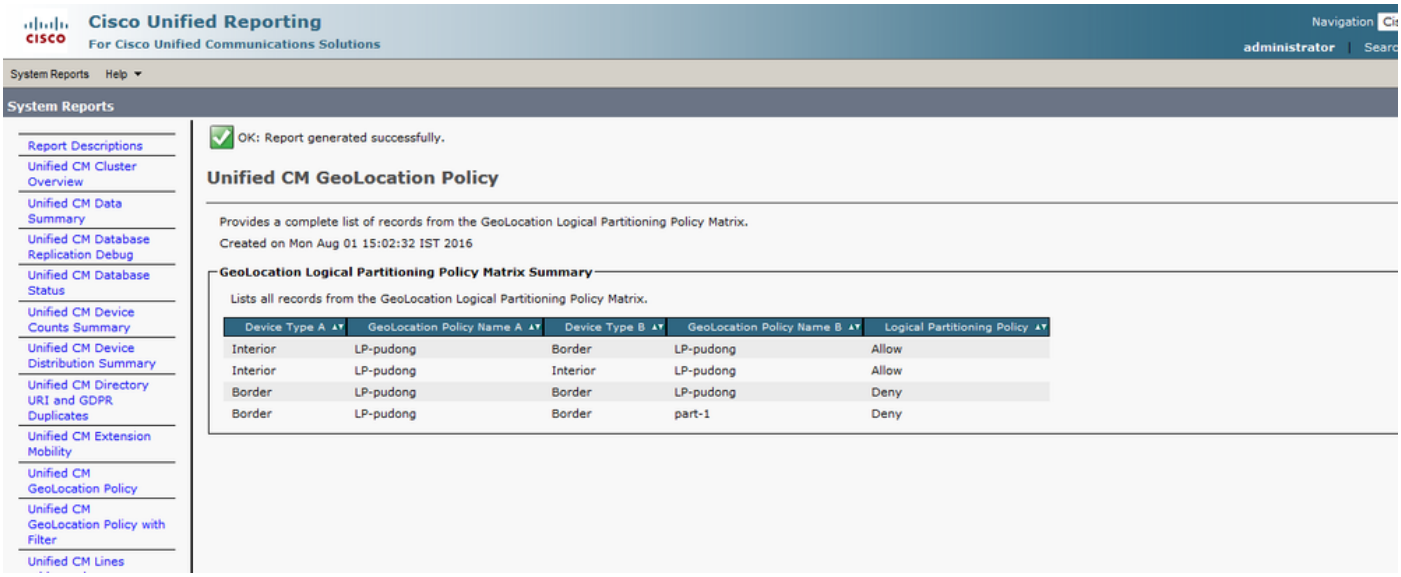
But as per the second policy, the calls from the India-PRI to IP Phones in Pudong location and vice-versa are denied but this conflicts the first policy.

In such cases, do remember that the policy that was added last will take precedence.

Step 8. Track the overlapping policies with Unified Reporting feature to obtain the Logical Partition Policy matrix. It is very helpful to troubleshoot as you can get to know all the logical partition policies configured in CUCM from a single screen. The Unified CM Geolocation Policy with Filter Report provides a complete list of records from Geolocation Logical Partitioning Policy matrix for selected Geolocation Policies, while the Unified CM Geolocation Policy report provides a complete list of records of all the Logical Partitioning Policies.


Cisco Unified Reporting
For Cisco Unified Communications Solutions
admini
System Reports
Help
System Reports
Report Descriptions
Unified CM Cluster Overview
Unified CM Data Summary
Unified CM Database Replication Debug
Unified CM Database Status
Unified CM Device Counts Summary
Unified CM Device Distribution Summary
Unified CM Directory URI and GDPR Duplicates
Unified CM Extension Mobility
Unified CM GeoLocation Policy
Unified CM GeoLocation Policy with Filter
Unified CM Lines Without Phones
Unified CM Multi-Line
OK: Report generated successfully.
Unified CM GeoLocation Policy with Filter
Provides a complete list of records from the GeoLocation Logical Partitioning Policy Matrix for the selected GeoLocation policy.
Created on Mon Aug 01 15:04:31 IST 2016
GeoLocation Policy: part-1
Reset
Submit
Unified CM Cluster Name
Cluster Name
Publisher Name/IP
StandAloneCluster
cucm-pub
GeoLocation Logical Partitioning Policy Matrix Summary
Lists records from the GeoLocation Logical Partitioning Policy Matrix for part-1.
Device Type A
GeoLocation Policy Name A
Device Type B
GeoLocation Policy Name B
Logical Partitioning Policy
Border
LP-pudong
Border
part-1
Deny


Cisco Unified Reporting
For Cisco Unified Communications Solutions
Navigation
Cisco Unifi
administrator
Search Docum
System Reports
Help
System Reports
Report Descriptions
Unified CM Cluster Overview
Unified CM Data Summary
Unified CM Database Replication Debug
Unified CM Database Status
Unified CM Device Counts Summary
Unified CM Device Distribution Summary
Unified CM Directory URI and GDPR Duplicates
Unified CM Extension Mobility
Unified CM GeoLocation Policy
Unified CM GeoLocation Policy with Filter
Unified CM Lines Without Phones
Unified CM Multi-Line Devices
Unified CM Phone Category
OK: Report generated successfully.
Unified CM GeoLocation Policy with Filter
Provides a complete list of records from the GeoLocation Logical Partitioning Policy Matrix for the selected GeoLocation policy.
Created on Mon Aug 01 15:03:45 IST 2016
GeoLocation Policy: LP-pudong
Reset
Submit
Unified CM Cluster Name
Cluster Name
Publisher Name/IP
StandAloneCluster
cucm-pub
GeoLocation Logical Partitioning Policy Matrix Summary
Lists records from the GeoLocation Logical Partitioning Policy Matrix for LP-pudong.
Device Type A
GeoLocation Policy Name A
Device Type B
GeoLocation Policy Name B
Logical Partitioning Policy
Interior
LP-pudong
Border
LP-pudong
Allow
Interior
LP-pudong
Interior
LP-pudong
Allow
Border
LP-pudong
Border
LP-pudong
Deny
Border
LP-pudong
Border
part-1
Deny



Step 9. Make a few test calls and check if it works. The Real Time Monitoring Tool (RTMT) is enhanced to track the number of failures due to logical partitioning policy restrictions in new Perfmon counters. Perfmon counters have a new group called **Cisco Call Restriction**. From there we can track a number of call failures in different scenarios as Tansfer Failures, Adhoc Conference Failures, Meet-Me Conference Failures, Forwarding Failures, Basic Call Failures, Mid-Call Failures, Total Call Restriction Failures, etc.

Step 10. Collect the CUCM traces from RTMT for the duration of the call. In the Signaling Distribution Layer (SDL) traces you can see the policy being selected and the policies that are configured between the Geolocation Policy pair.

Communication of Geolocation Info in CC signals.

```
| SdlSig    | CcRegisterPartyA                    | restart0                    |
LineControl(1,100,139,3)        | SIPCdpc(1,100,55,17)            | (1,100,45,1).3035-
(SEP0019555CBAE3:10.76.253.14)| [R:NP - HP: 0, NP: 2, LP: 0, VLP: 0, LZP: 0 DBP: 0]CI=23624774
CI.branch=0  CSS= cssIns=0 aarCSS= aarDev=T doNotAppendLineCSS=F lrg= ccBearCap.itc=0
ccBearCap.l=3 ccBearCap.itr=1 protected=1 flushCapIns=0 geolocInfo={geolocPkid=9dc76052-3a37-
78c2-639a-1c02e8f5d3a2, filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal=, devType=4}
locPkid= locName=
```

Communication of Geolocation Info in PolicyAndRSVP signals.

```
| SdlSig    | PolicyAndRSVPRegisterReq            | wait                        |
RSVPSessionMgr(1,100,76,1)      | SIPCdpc(1,100,55,17)            | (1,100,45,1).3035-
(SEP0019555CBAE3:10.76.253.14)| [R:NP - HP: 0, NP: 0, LP: 0, VLP: 0, LZP: 0 DBP: 0]CI= 23624774
Branch= 0  reg=Default cap=5 loc=0 MRGLPkid= PrecLev=5 VCall=F VCapa=F regiState=0 medReq=0
dataCapFl=2 ipAddrMode=0 status=0 geolocInfo={geolocPkid=9dc76052-3a37-78c2-639a-1c02e8f5d3a2,
filterPkid=d5bdda76-6a86-56c5-b5fd-6dff82b37493, geolocVal=, devType=4}
| SdlSig    | PolicyRegisterReq                   | await_init                  |
LPSession(1,100,26,21)          | RSVPSessionMgr(1,100,76,1)      | (1,100,45,1).3035-
(SEP0019555CBAE3:10.76.253.14)| [R:NP - HP: 0, NP: 0, LP: 0, VLP: 0, LZP: 0 DBP: 0]CI= 23624774
Branch= 0  geolocInfo={geolocPkid=9dc76052-3a37-78c2-639a-1c02e8f5d3a2, filterPkid=d5bdda76-
```

```
6a86-56c5-b5fd-6dff82b37493, geolocVal=, devType=4}
```

Points to ponder

- Media Devices i.e (Media Termination Point) MTP, (Conference Bridge) CFB, Annunciator, (Music on Hold) MoH are not required to be associated with geolocation values.
- There is no LP Policy check for VoIP to VoIP device call or feature with only VoIP participants. In other words, Interior to Interior policy is always allowed.
- LPPolicyManager is a singleton process which interfaces with InMemDB and maintains policies in call processing as LP Policy Tree. During CUCM service startup, the LPPolicyManager reads the policies from InMemDB tables and constructs the LP Policy Tree. The Add/Delete/Update of a Policy in DB results in Change Notification to LPPolicyManager and change is affected in LP Policy Tree.

Logical Partitioning Policy Checking.

```
001853112| 2008/09/26 11:50:39.687| 001| AppInfo   |                                        |
|                                 |                                 |
| LPPolicyManager -getLogicalPartitionPolicy, GeolocInfoA[pkid=31396408-3d83-74a9-1655-
d2f0a05dd0a4, filter=d5bdda76-6a86-56c5-b5fd-6dff82b37493, val=, devType=4]
001853113| 2008/09/26 11:50:39.687| 001| AppInfo   |                                        |
|                                 |                                 |
| LPPolicyManager -getLogicalPartitionPolicy, GeolocInfoB[pkid=9dc76052-3a37-78c2-639a-
1c02e8f5d3a2, filter=d5bdda76-6a86-56c5-b5fd-6dff82b37493, val=, devType=8]
```

- The DevType that appears in the traces describes the types of the devices.

The **devType =4** (UserDevice) is for these devices.

- Phones (SCCP, SIP, third party)
- VG224 analog phones
- CTI Route Points and CTI Ports
- Cisco Unity Voice Mail (SCCP)
- MGCP port (FXS)

The **devType =3** (AccessDevice) if for these devices.

- Intercluster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlledH.225 trunk
- MGCP port (E1, T1, PRI, BRI, FXO)
- Gateway (for example, H.323 Gateway)

The **devType =8** (SIPAccessDevice) for this device.

- SIP trunk

References

- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmfeat/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100_chapter_011100.html?bookSearch=true

- http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/116038-logical-partition-geolocation-00.html

Known bugs

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsz91044

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuo85770

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsq79192

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsr91423

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsy73509

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCtb33479

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCtb05434

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsv65724

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsq73894

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCsr38397