FAQs on Implementation of Geolocation Across CUCM

Contents

Introduction

This document describes all the FAQs with respect to the implementation of Geolocation Across Cisco Unified Communications Manager (CUCM).

How CUCM Selects Geolocation for a Device?

This a mechanism to select a Geolocation for a device:

Step 1. Select the Geolocation from the device configuration.
Step 2. If it is not configured on the device page:

- For a phone device in roaming, read the Device Pool (DP) from the roaming configuration.
- For a phone device that is not in roaming, read the DP from the device configuration.
- For trunk, ICT, or Media Gateway Control Protocol (MGCP) port device, read the DP from the device configuration.

Step 3. From the selected DP, read the value of geolocation from DP configuration. If DP is not configured with a value for Geolocation, the device uses a blank Geolocation value.

Step 4. If the device reads blank Geolocation value, the next level is Default Geolocation Enterprise Param, which is accessed at the time of the policy checking or location conveyance.

How CUCM Selects Geolocation Filter for a Device?

This is the mechanism that is followed in order to select a Geolocation Filter for a device:

1. For phone device that is not in roaming, read the Geolocation filter value from DP in the device configuration.
2. For phone device that is in roaming, read the Geolocation filter value from DP in roaming configuration.
3. For trunk, intercluster trunk, or MGCP port device, read the Geolocation filter value from device configuration.

If no value is configured, read from DP:

1. If DP is not configured with a Geolocation filter value, the device uses a blank value.
2. If the device reads a blank Geolocation filter, the next level is Default Geolocation Filter Enterprise Param, which is accessed at the time of policy checking.

What is the Recommended Configuration to Deploy LP for Indian Customers as per TRAI Regulations?

- Enable Logical Partitioning = True
- Logical Partitioning Default Policy = Deny

The system default policy shall be **Deny** for an enterprise, so calls or features are blocked between VoIP device participants' i.e A Phone and a Gateway, a Gateway and another Gateway, an ICT and a Phone, an ICT and a Gateway.

In order to allow VoIP communication, based on VoIP network topology, the Allow policies must be configured by navigating to **System > Logical Partitioning Configuration**.

For example, typically a Gateway in one site will be allowed communication with Phones or another Gateway in that site so accordingly, there shall be allowed policies /per site.

How Much Robust is LP and What an Administrator Needs to Configure to Ensure that no Scenario Occurs against the Regulations?

The Administrator will need to ensure that this configuration is there in Enterprise Parameters configuration:

- Enable Logical Partitioning = True
- Default Geolocation = BlankGeolocation
- Logical Partitioning Default Policy = Deny
- Logical Partitioning Default Filter = None

BlankGeolocation - This needs to be configured from the **System > Geolocation Configuration** and not populating any data.

Other than that, the Administrator will need to configure Allow policies from **Call Routing > Logical Partitioning Policy Configuration** screen.

This prevents any Public Switched Telephone Network (PSTN) to VoIP or PSTN traffic unless an Allow policy is configured in the configuration for that device.

The reason the BlankGeolocation is configured is to cover those devices in a cluster which do not get associated with any Geolocation through Device or DP configuration.

And by default, unspecified Geolocation means that the device will not participate in any LP checking.

The BlankGeolocation ensures that no scenario occurs against regulation.

At the time of policy search, a policy such as this would be searched without any Geolocation fields and there won't be any such configured in the system:

- Border Interior Allow
- Border Border Allow

What is Location Conveyance?

The conveyance of GeoLocation from one SIP user agent to another entity with the use of SIP is called Location Conveyance.

Here **GeoLocation** is a description of the physical geographical area where something currently exists.

The IETF RFC 3693 (Geopriv Requirements) describes the Geographic location in Presence Information Data Format (PIDF-LO) and draft-ietf-sip-location-conveyance-10 describes the location conveyance.

In order to support LP requirements, the UCM's implementation additionally communicates **Device type** information in PIDF-LO.

This is based on **User Agent Capability Presence Status**, as per specification in SIP extension draft-ietf-simple-prescaps-ext-08.

The UCM's SIP Trunk supports location conveyance as per these specifications.

In order to allow ICT to be feature compatible with SIP Trunk and allow the same capabilities, the ICT/H225 Trunk also supports location conveyance across the cluster with the use of PIDF-LO.

The UCM supports the conveyance of location information both at call establishment as well as location changes due to change in the connected party in participation to midcall joins and redirects.

How Location Conveyance is turned on in UCM?

- The devices for which location needs to be conveyed across cluster must associate with a Geolocation.

- **Send Geolocation Information** checkbox checked on SIP Trunk or ICT.

If such a device makes or receives a call, the associated Geolocation is conveyed across the Trunk or ICT.

Supporting what Requirement, the Location Conveyance needs to be Turned on?

The Logical Partitioning feature is based on a framework of Geolocations. As long as participant devices in a feature are within the cluster, the UCM receives the associated Geolocation information from local configurations.

If participant devices are across clusters then for the purpose of policy checking Geolocation information with devices across the cluster would be required.

There are two possible options:

1. Use Geolocation which is associated with a SIP Trunk or ICT on Trunk device configuration- Use this information for policy checking. All the devices across the cluster will be represented with a common Geolocation as specified on Trunk device configuration. If location conveyance is not turned on in a remote cluster then also LP policy checking will be able to work.

2. Use Geolocation which is received in location conveyance from across the cluster. The actual Geolocation and Device type for a device across the cluster will be received and can be used for LP policy checking.

Incoming calls - The remote cluster if sends PIDF-LO in call signaling, the **actual** Geolocation is available for policy checking and would be used even before placing/ringing the call to UCM device.

Outgoing calls- The UCM device placing a call to SIP Trunk or ICT would need an LP policy, so that call can be extended to a remote cluster. This policy will be the same as 1. The "actual" geolocation for a device (VoIP phone or gateway) across the cluster shall be received during Alerting phase. The UCM "must" have an "Allow" policy correspondingly (Interior to Interior will not need any policy. Yes, if one or both of involved devices is Border)

The location conveyance provides an opportunity for doing scenarios based on **actual** Geolocation and device types.

Basically, Geolocation information is carried end to end across an enterprise.

This kind of implementation is important for deployments, where calls are redirected back & forth across the clusters and **real** Geolocation, needs to be carried along with the call, which would assist in correct LP checking.

In what Methods, Location Conveyance (PIDF-LO) is Communicated for SIP Trunk and ICT?

SIP: INVITE, UPDATE.

ICT/H225 Trunk: Setup, Alert, Progress, Notify, Connect.

When Location Conveyance is Enabled and Geolocation PIDF-LO Associated with a Device in a Remote Cluster is Received, How Does Local Cluster Match the Policies?

The administrator needs to follow these steps:

1. Configure Geolocations based on a set of fields which may be received from the remote cluster. This is manual exercise by an Administrator, which would normally need access to Geolocation configurations in the remote cluster and copying the data to the **local cluster. System > Geolocation Configuration**.
2. Configure GeolocationPolicy Records and policies based on deployment requirements.

Call Routing > Logical Partitioning Configuration.

How it is Determined whether a Device across the Cluster is a Gateway or a VoIP Endpoint?

This information is carried in a device cap element of PIDF-LO.

Currently, the information is communicated in the proprietary tag:

```
<caps:devcaps>
<cisco:gateway>false</cisco:gateway>
</caps:devcaps>
```

When this information is received, UCM maps it to internal UCM enumeration in order to represent it to the CallManager device type.

What is the Purpose of Assigning Geolocation and Filter with Intercluster Trunk (ICT or SIP Trunk)?

This requirement is mainly relevant for an LP Enabled cluster, where it is required to allow/deny traffic from VoIP phones to ICT or PSTN Gateway to ICT.

The Geolocation and Filter ensure that the identifier is made for participation in LP checking. In correspondence, an LP policy (policies) must be configured.

The relevance of SIP Trunk Device's Geolocation on location conveyance (the one which is configured on SIP trunk):

The Geolocation which is associated with a caller or called device is the one which is used for location conveyance. Say a Phone A (geoloc1) makes a call across SIPTrunk/ICT (configured with geoloc2). The Geolocation which is sent in location conveyance is geoloc1.

Assume a SIP Trunk, trunk1 (geoloc3) that points to a SIP Gateway receive a PSTN call. Say the call is forwarded by UCM to SIPTrunk/ICT (geoloc2). The Geolocation which is sent in location conveyance is geoloc3 (which is configured on trunk1).

Are LP Policies Communicated across the Cluster?

No. The LP policies are specific to the local cluster only. There is no inter-cluster communication of LP policies.

Can Location Conveyance be Enabled without Configuring LP?

Yes. The LP is not a prerequisite for Location Conveyance. In fact, LP is one of the features that uses Location conveyance functionality.

Is there Performance Degradation when UCM's Logical Partitioning Feature is Used?

The policy checking is implemented as a Tree search mechanism, which is a string comparison for each field of Geolocation. If filters are used short, say 4-5 fields, then it will be faster as compared to the usage of all 17 fields in the filter and policy configurations.

There are two ways LP can be used:

- Without Location Conveyance: The Geolocations are not communicated between clusters and there is no processing involved in that.
- With Location conveyance: The Geolocations are communicated between clusters and there is processing involved in that.

Both these implementations are noted reasonable in performance.

The Geolocation fields might be configured as Unicode and with upper limits on size. This might not be recommended for LP policy checking.

Recommended Points to Teams That Deploy LP in Deployments That Exist

Select 2-3 Phones with the use of Single Line, in each site to do pilot testing:

1. Configure Geolocations: associate with Devices from device configuration.
2. Configure Filters: associate with devices from DP or Device (for Trunks. Gateways) configuration.
3. Reset the devices.
4. Configure LP policies.
5. Enable Logical Partitioning from Enterprise Param.

As you have not associated Geolocations with all the devices so it would not participate in LP policy checking.

Test the supplementary scenarios with pilot phones as well as other production phones in order to make sure that things work as expected.

- The pilot phones should be able to observe LP restrictions in the scenarios.
- The other production phones should not be impacted.