Genesys Cloud: India Preferred Deployment Domestic & International

July 2022

Version 1.5.2

GENESYS
moments connected

Terms and Conditions

Genesys Cloud currently offers service in 10 regions globally including our newest region in India. India has some unique telecommunications laws that need to be reviewed by Customers locating Contact Centers within India. This document provides an introduction and some recommendations for review.

This document is for informational purposes only relating to Genesys Cloud use in India. It represents Genesys' knowledge and experience with India telecommunications regulations. The information is not legal advice and prior to implementing any solution, customers should consult with their legal counsel, their telephony service provider (TSP), and the India DoT in order to ensure that they are in compliance with all India laws as well as telecommunications and contact center regulations.

The regulatory environment may change, or customers specific use of services, so the document is presented as informational. There are no penalties, damages or other remedies associated with incorrect information or errors of omission that may occur in this overview.

Overview

This document provides general considerations and preferred architecture options for deploying Genesys Cloud in India. More detailed documents with additional, though less desirable, architectures are available in the Resource Center.

India is a dynamic regulatory environment and the interpretation and approval of an architecture is provided solely by the Indian government. There is no guarantee that an architecture will be approved and an architecture which is approved today may be rejected tomorrow due to legal or regulatory changes and interpretations.

Important Definitions

TSP – Telephony Service Provider – This is the customer's telephone company – Tata, Bharti, or others

OSP – Other Service Provider – This is the customer's contact center or business.

DoT – Department of Telecommunications – A division of the India government that oversees creating and enforcing telecommunications laws and regulations.

NOTE: Genesys is neither an OSP nor a TSP. We are not offering or providing telecommunications services, nor are we running centers in which people or agents make or receive calls. Genesys simply provides the platform to allow our customers to do so (as an OSP), by utilizing our platform and interconnecting it to their TSP (Telephony company).

India Challenges

The India Regulatory Environment Landscape is Evolving

- Beginning in March of 2020 the India DOT began relaxing the terms and conditions for OSP Centres in India in the wake of Covid-19 concerns

1H 2020 Regulatory Changes

- Removed the requirement for security deposits for Work From Home (WFH) agents
- Removed the requirement for obtaining VPN from TSP's for WFH Agents
- Removed the requirement for obtaining "permission" for WFH agents
- Notification, tracking, static-IP, CDR and other requirements remain
- November 2020 – Permanently Revised OSP Guidelines
- Removed OSP Registration Requirements
- Allowed VPN to interconnect OSP's
- Allowed aggregated traffic from international POP's over MPLS
- Allowed interconnection of agents to OSP Centre's via VPN in support of WFH/WFA (Work from Anywhere)
- Allowed Centralised and shared internet for multiple OSP Centres
- Removed bank guarantee requirements
- Interconnectivity between OSP companies allowed
- Reconfirmed the requirement for not mixing International and National LD (re-affirms separation of domestic and international calls)
- Allows Foreign EPABX for International, but re-affirms requirements of toll bypass prevention, privacy regulations, and locally stored CDR's with IST timestamps

June 2021 – Further simplification and clarification of DOT Regulations

- No registration is required
- No bank guarantees are required
- Allows connectivity via any WAN technology including MPLS, SD-WAN, etc.. Including voice traffic
- Allows agent connectivity to OSP's via any broadband technology (Wireless, etc..) – but still requires VPN to OSP Centre
- Internet can be obtained from any TSP and shared between OSP's (centralized)
- Non-voice entities are no longer regulated by the DOT (non-voice BPO's)
- OSP's need to self-regulate and no longer report to the DOT regularly. Routine inspections will no longer occur.
- Shared infrastructure is allowed.
- Foreign EPABX is allowed – CDR and toll-bypass requirements are still enforced
- Third-party hosting and TSP hosting is allowed
- No restrictions on interconnectivity
- No restrictions on voice interconnectivity for internal communication
- Added the requirement of MAC-ID to UDR's – maintained the requirement for tamper proof CDR copy at an OSP Centre with IST timestamps and must be maintained for 1 year

September 2021 – TSP changes

- Significant relaxation of financial requirements TSP requirements including allowing 100% FDI (Foreign Direct Investment), bank guarantees reduced by 80%, and more
- These changes are currently being reviewed but create an environment for increased competition and reduced costs for India Telecom Operators

- Telecommunications in India are regulated by the Indian government, specifically by the Department of Telecommunications (DoT). These regulations have been changing based on factors such as work from home agents but continue to evolve.
- The India telecommunications environment is highly regulated and does not allow calls to traverse the open internet or to bypass toll charges in any way. There are also established regulations for calling between the 22 specific regulatory circles within India.
- Toll Bypass (calls avoiding paying toll charges) has been a major concern of the regulations.
- Customers should consult with their legal counsel, their TSP, and the India DoT prior to implementing any solution to ensure that they comply with all India DoT laws and regulations.

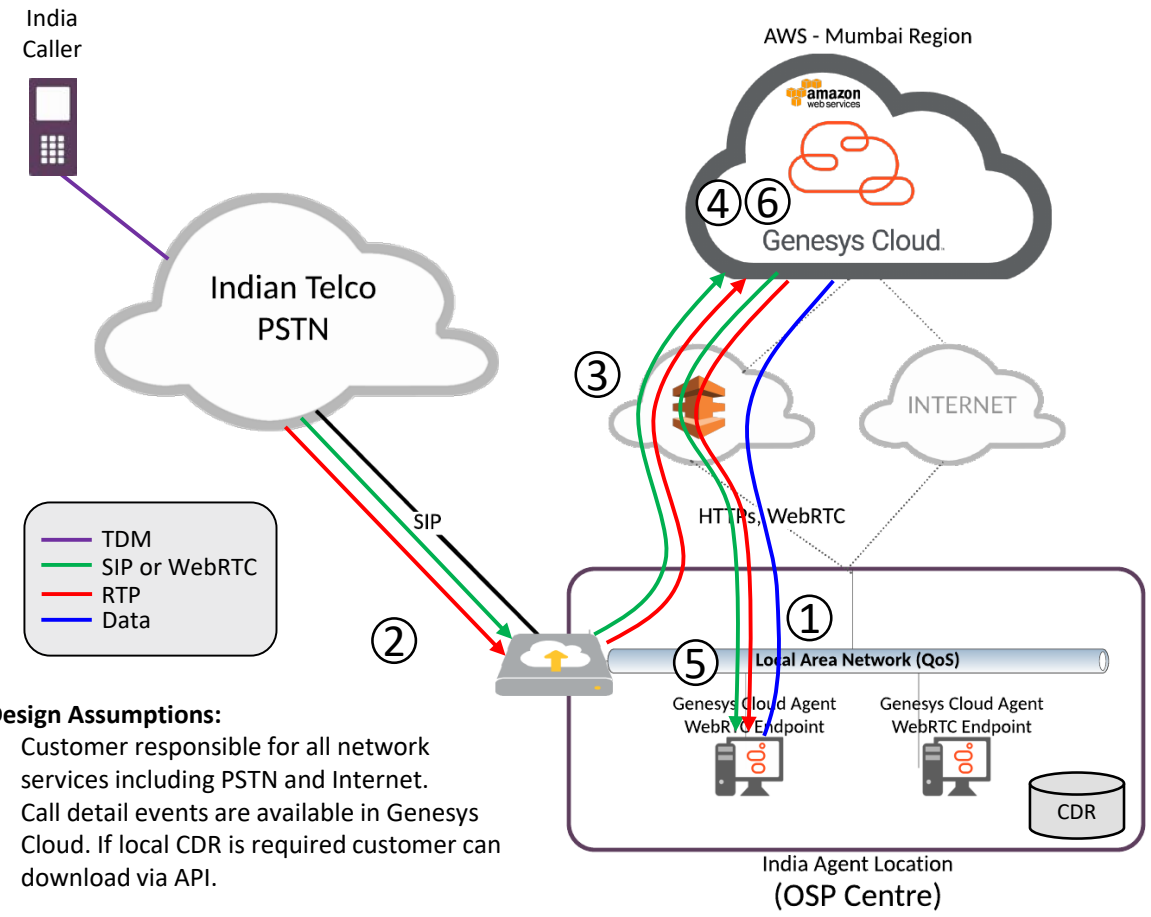
Additional India Considerations:

- Registration/Application for an "Other Service Provider" (OSP) licenses with the India Government to operate a contact centre or upon making changes to their configuration or architecture
- Interpretation can vary based upon province or Licensing Service Area (LSA). Because OSP filing and review are decentralized, and interpretation will vary.
- Under India OSP regulations, an OSP is required to purchase telecom services from an authorised Telecom Service Provider ("TSP") in India and such TSP is required to examine the network and architectural diagrams to ensure their acceptable use in conformance with India laws and regulations.
- As part of the submission of the network to the regulators, the TSP must confirm that the connectivity from the proposed OSP centre to the location outside India, is through its network.
- There exists a distinction between international, national (circles) and special economic zones/free trade zones (SEZ/FTZ) which may require special configurations and architecture to route calls in different ways between these zones.
- Infrastructure cannot connect to National and International networks. Note: With new regulatory changes a single system may be possible provided that is provides logical separation and isolation.
- India's DoT requires Call Detail Records (CDR's) that include details on the agent who handled the call for auditing and compliance. A copy of the CDR's must be maintained in India with an IST timestamp and accessible upon request of the India DoT.
- CDR's must be maintained for at least 1 year and must include the following data elements:
    - Date (IST),Time (IST),Calling Number/User(Email)ID/Extension Number/DID(Complete CLI),Called Number/User(Email)ID /Extension Number/DID(Complete CLI),Call Duration(hh:mm:ss),Call Trunk Type(PSTN/VoIP),Direction of Call - Incoming/Outgoing
- UDR's are also a requirement and include additional data fields such as MAC-ID and must be maintained by the customer on-site.
- Calls cannot cross the India border 2 times – meaning that a call originating in India cannot leave the country and be routed back to an agent in India as this should be treated as a domestic call.

Domestic Scenario: Inbound and outbound calls directly to TSP with VoIP over AWS Direct Connect (public interface)

Domestic Scenario Overview: In this model the India telco (TSP) is terminating SIP trunks to the customer's premises. Inbound calls will be delivered to the customer site and then sent from the SBC to Genesys Cloud across AWS Direct Connect. Additionally, outbound calls may originate from the customer location and follow a similar call flow between components. **As all PSTN connectivity is at a single customer location then Inbound and Outbound traffic can be supported with a single Genesys Cloud Org.** With a single site and single connection to the PSTN there are no possibilities of toll-bypass.

Domestic Scenario Diagram:



Design Assumptions:

- Customer responsible for all network services including PSTN and Internet.
- Call detail events are available in Genesys Cloud. If local CDR is required customer can download via API.

Domestic Scenario Call Flow Steps:

Step	Details
1	India Agent logs into Genesys Cloud AWS instance in Mumbai
2	Caller Dials local India number provided by Indian carrier which terminates on SBC at customer premises. Customer manages relationship with carrier.
3	Call is sent by SBC via SIP across AWS Direct Connect to Genesys Cloud in Mumbai.
4	Genesys Cloud receives call, performs IVR treatment and then selects agent to receive the call.
5	Genesys Cloud makes call to agent. Call is delivered via WebRTC. All RTP is delivered across AWS Direct Connect.
6	Once the agent answers the Genesys Cloud bridges the two parties together.

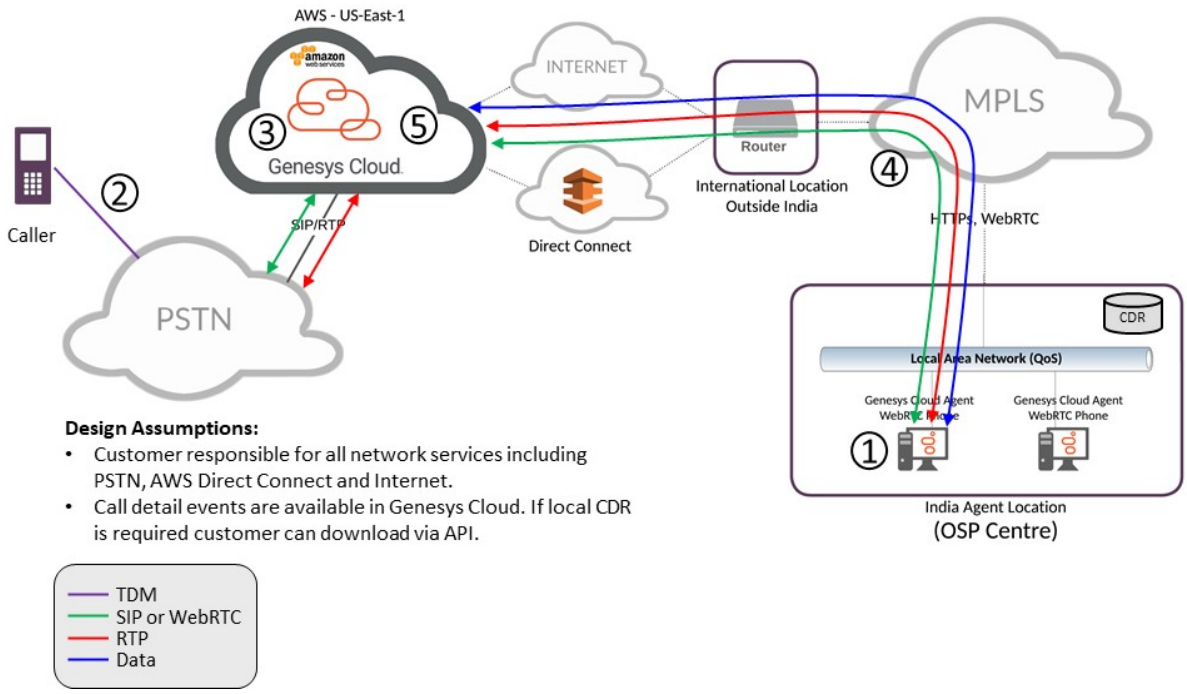
Note: WebRTC station configuration and call detail records are stored by Genesys Cloud analytics in AWS instance. The API can be used to extract appropriate analytics to create CDR.

Additional Notes:

- Genesys Cloud supports the use of AWS Direct Connect with the public virtual interface. Further details are available at https://help.mypurecloud.com/articles/aws-direct-connect-genesys-cloud-overview/. The AWS Direct Connect private virtual interface is not supported.
- If Direct Connect is used, then Internet connectivity is also required as Genesys uses AWS CloudFront services.
- To simplify network connectivity and WebRTC Force TURN may be used as detailed at https://help.mypurecloud.com/articles/use-the-force-turn-feature/

International Scenario: Inbound Call Flow from international caller using AWS Direct Connect

International Scenario Diagram:



International Scenario 1 Call Flow Steps:

Step	Details
1	India Agent logs into Genesys Cloud AWS instance outside of India (ex: US-East1) from Agent desktop. AWS Direct Connect is used for HTTPS communication from Agent to Genesys Cloud.
2	Caller Dials International (non-India) number which terminates at Genesys Cloud AWS location in US-East (for example).
3	Genesys Cloud receives call and performs IVR treatment (if required). Genesys Cloud selects agent for the call, which in this case happens to be in India.
4	Genesys Cloud delivers call to agent in India. Call travels across MPLS and is delivered to agent.
5	Once India Agent answers the Genesys Cloud bridges the two parties together.

Note: Phone configuration and call detail is stored by Genesys Cloud analytics in AWS instance. The API can be used to extract appropriate analytics to create CDR. Genesys PS has experience creating CDR for customers in India.

Additional Notes:

- Genesys Cloud supports the use of AWS Direct Connect with the public virtual interface. Further details are available at https://help.mypurecloud.com/articles/aws-direct-connect-genesys-cloud-overview/. The AWS Direct Connect private virtual interface is not supported.
- If Direct Connect is used then Internet connectivity is also required as Genesys uses AWS CloudFront services.
- To simplify network connectivity and WebRTC Force TURN may be used as detailed at https://help.mypurecloud.com/articles/use-the-force-turn-feature/