ASSERTION

ASSERTION v3.7 DATASHEET

+91 080 4545 3369

info@assertion.in

www.assertion.in

OSP compliance with Assertion

Contact centers, ITES companies and others providing service over telephony infrastructure in India, are required to register with the Department of Telecommunications (DoT) as an OSP (Other Service Provider) and adhere to the specified terms and conditions.
Non-compliance will lead to significant fines and disruption to operations.

Are you confident your contact center is configured to be compliant? Are you certain that frequent configuration changes or malicious users are not putting your enterprise at risk?

Companies have relied on their overworked IT departments without expert help, to configure their enterprise telephony infrastructure, and manually verify its compliance on a periodic basis. Ensuring continuous compliance through manual change control processes has also been inadequate, and exposed the enterprise to risk.

Now there is a new solution to perform automated verification of OSP compliance for the enterprise voice infrastructure and provide peace of mind to the management.

Solve it with Assertion

Assertion introduces the OSP (Other Service Provider) feature pack for contact centers in India, with controls that automate compliance verification for any OSP that is using the Avaya Aura Communication Manager for enterprise telephony.

Key Features

- Verifies logical partitions between the domestic and international OSPs on shared setups.
- Enforces proper logical partitioning of all trunk and station resources in the system.
- Zero configuration gaps arising out of group features.
- Ensure proper and effective CDR collection according to the prescribed OSP standards.
- Check system wide role based access controls.
- Perform platform checks like system time and logging configurations.
- Ensure each and every station/user is correctly partitioned.

OSP & India Toll Compliance Assurance Service

Every year DoT audits OSP enterprises and finds violations. These enterprises end up paying huge fines and face operations disruption. Even large global call centers have had to shut down operations for weeks/months since their telephony service provider cut service for failure to comply with OSP regulations.

Enterprises have mostly been forced to make design and configuration choices without understanding all the implications of the OSP regulations. They have struggled to interpret the often vague regulations into corresponding actions in the real world.

OSP consulting options available to enterprises today are mostly agencies handling the necessary paperwork, and lack the technical expertise to design and fine tune the configurations. The complete lack of automation also hinders them in ensuring continuous compliance, and effective change management.

So, how can an OSP assure compliance for the enterprise, peace of mind to the management?

Solve it with Assertion

Assertion now offers a unique OSP/India toll compliance assurance service for all enterprises in India. Assertion has created a 360 degree mechanism which takes care of all the aspects of OSP compliance like automated scanning, configuration checks, liaising with DoT, and consulting services to ensure the enterprise will always be compliant.

Key Features

- OSP compliance 'guarantees' by scanning systems, collecting reports and taking full ownership of the an enterprise's OSP and India Toll Compliance.
- Assertion offers consultation on expert interpretation of TRAI/DoT regulations.
- DoT liaising across India for OSP registrations, yearly submissions and audit handholding.
- Comprehensive historical, geographical and drill-down reports to ensure full time compliance and protection against fraud.
- Assertion performs deep automated configuration scans on the trunks, gateways, tenants, stations, special application features, mobility features, locations, class of service (COS) and much more.

ASSERTION

ITC Feature Pack

Enterprises in India that have a closed user group (CUG) setup using an enterprise PBX need to ensure they are compliant to the TRAI (Telecom Regulatory Authority of India) regulations and do not cause toll bypass.

The regulations require that complete and effective logical partitions are established between the PSTN trunks and the enterprise CUG to ensure that there is no loss of toll to the telephony service provider or the government. If a toll bypass is detected it will lead to huge fines, closure of operations and litigation.

How can an enterprise ensure that the CUG is configured to be India toll compliant? Are regular configuration changes or malicious users putting the enterprise at risk? What mechanisms are available to ensure that irrespective of what changes occur in the system, compliance violations will be flagged immediately before they turn to big trouble for the enterprise?

Solve it with Assertion

Assertion's India Toll Compliance feature pack provides automated compliance checks for enterprises with a closed user group (CUG) setup using an Avaya Aura Communication Manager or a Cisco Unified Communication Manager.

Key Features

- Checks logical partitions between trunks and detects partitioning changes.
- Ensures no toll bypass through call redirection features, Mobility and Hot Desking features, trunk-to-trunk transfer features and more.
- Scans each and every user/station configuration regularly.
- Verifies special application for toll bypass (SA9122) private/public configurations for trunks, network regions and location mappings, IP address mappings, bridge mappings etc on Avaya Aura Communication Manager
- Complex geolocation configuration and logical partitioning policy checks on device pools and phones, trunks, gateways and other resources on Cisco Unified Communication Managers.

OCL Feature Pack

Contact centers regularly encounter a need to perform checks on their operations to ensure that everything is in working order. Sometimes critical resources are down impacting the rate at which customers are serviced, while other times critical backup and/or platform processes are disrupted putting the enterprise at a serious risk of operations disruptions and compliance.

Enterprises have tackled this problem using dedicated manual resources to perform operations checklists. These resources are either employed in-house or through service contracts.

But, manual checking suffers from limitations of scale, lack of efficiency, high costs of resource and are highly error prone. Manual checks can neither handle a large number of resources (like hundreds of trunks or stations) nor can they perform it fast enough or frequently enough.

So, how can an enterprise automate their operations checklist?

Solve it with Assertion

The Assertion Operations Checklist (OCL) feature pack performs regular scans of the hundreds of resources in a contact center to verify their state of health, and provides easy to interpret reports on a customized schedule, quickly and efficiently.

Key Features

- Regular checks of state of health of all critical systems and tracking of system alarms and warnings.
- Pre-scheduled, fully-automated scans to minimize operational downtime
- Checks the status of survivability mechanisms and system links
- Verifies the availability of gateways, media resources and trunks.
- Ensures the healthy status of CDR, CTI and CMS links.
- Keeps a tab on the platform through process checks, system time checks and other interface checks
- Instant access to historical, geographical, and drill-down reports.

ASSERTION