**infraonNCCM**
Powered by EverestIMS

# Define, Authorize, Deploy and Track Change

## On any Network Infrastructure

**70% of all outages are perpetrated by authorised users**

## Automate your Configuration & Change Management

Infraon Network Configuration and Change Manager (NCCM) automates the Configurations and Compliance of network devices. Infraon NCCM (which is a part of the Infraon Suite), places a stringent focus on compliance for regulatory standards, complemented by real-time alerts on important events and comprehensive reports for managing overall network devices & their daily operations.

Infraon NCCM is vendor-agnostic and manages various devices covering Routers, Switches, Bridges, Firewalls, Load balancers and Wi-Fi access controllers.

Infraon NCCM enables change to occur in a controlled, innocuous and measured manner by ensuring impacts and risks are sufficiently assessed.

It provides insight into making informed decisions about what changes can be allowed for deployment, and what changes need additional analysis or risk mitigation.

## Infraon NCCM helps you manage change in all its forms, complexity and challenges

Infraon NCCM helps you find out 'who' made 'what' changes, 'when' and 'why'. Further, it alerts you in real-time on your mobile phone (or through other immediate channels) when changes or events occur. Infraon NCCM helps support the processing of changes and enables their traceability. It can automate the Configuration and Compliance of network devices across any scale of magnitude and numbers.

Currently being used by one of India's top banks for change management, network automation, disaster recovery, and configuration auditing.
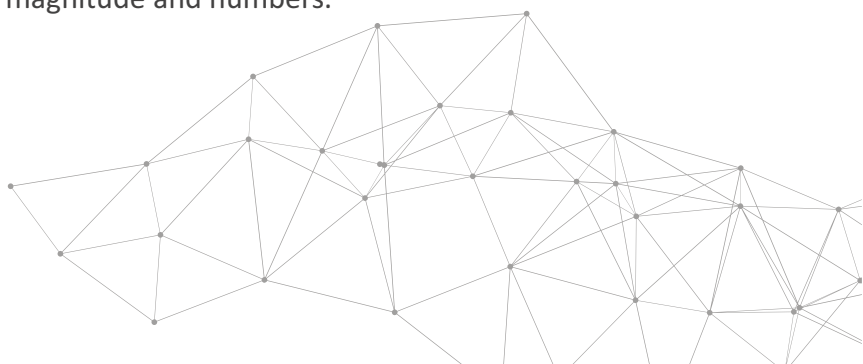
## Network Discovery

Supports multi-modes of discovery using typically required SNMP and device credentials.

## Configuration Management

Comprehensive Network Configuration Backup & Recovery across all network devices. Instant detection and alerting on configuration changes with the option to automatically roll back to a previous configuration.

## Network Security Auditing

Monitor via "Live Tracking" all authorized user actions on target network devices displaying CLI commands executed and results with audit archiving for historical analysis. Initiate "kill sessions" in the event of any protocol breach.

## Multi-Channel Notification & Reports

Immediate alerting of important events like detecting configuration changes, configuration download success, policy violations, job completions, firmware upgrade etc., using multiple channels like Email & SMS along with other detailed reports.

## Inventory Tracking

Capture complete inventory details of multi-vendor Network Devices including Host name, Serial Number, Vendor, Model, OS, Firmware Version, End-Of-Life, End-Of-Support details etc.

## Routine Task Automation

Automate common & repetitive tasks with respect to Network Operations with pre-configured templates allowing execution of tasks at multiple locations at the same instant.

## Vulnerability Detection

Instantaneous detection of vulnerabilities in newly-discovered target network devices. Multi-level security tagging of device vulnerabilities based on CVSS Scores along with vulnerability details.

## Audit Trails & Tracking

Complete audit trail of device configurations, tool operations, job executions for end-to-end tracking of network operations and tool activities.

## Policy Compliance

Flexible Rules & Policy Configuration Templates ensuring complete Security, Operational & Regulatory Policy Definition & Enforcement.

## Key Highlights

- Network Administrative Operations support for NoC
- Network Service Provisioning Automation
- Network Asset Inventory
- Configuration Download, Back-up and Upload Operations
- Network Device Firmware image upload
- Configuration File Version Control
- Manage Devices of IP/MPLS and Optical DWDM Networks
- Radius / TACACS Integration support for User Authentication

## Capability Snapshot

- Scheduled and Bulk Discovery
- Multitenancy & Role-Based Access
- In-Built Diagnostic Tools
- Scheduled Backup Operations
- Comprehensive Auditing
- Reusable Templates for Bulk Changes
- Detect Policy Violations
- Email & SMS Notification
- API-based 3rd Party Tool Integration
- PDF, Excel, CSV Export options

## NCCM for Banks

NCCM helps banks adhere to norms set out in the RBI circular (RBI/2015-16/418 | DBS.CO/CSITE/BC.11/33.01.001/2015-16) on guidelines addressing Cyber Security Framework in Banks. NCCM specifically fulfills points pertaining to Annex 1: No. 4) Network Management and Security spanning inventory of authorized devices, appropriate configuration, and maintenance of network activity logs.

www.everest-ims.com

sales@everest-ims.com

+91 80 46567100

**everest IMS**
EverestIMSTechnologies