everest IMS
EverestIMS Technologies

Data Sheet

Infraon NCCM

Network hyper-automation suite to effectively define, authorize, deploy & track change

Overview

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

An all-in-one OSS solution when Integrated with Infraon IMS, a unified tool for 360-degree IT Infra monitoring, and Infraon ITSM, an IT Service Management tool.

Feature Highlights

- Web-based GUI for easy access with no client installations required
- Multi Browser support spanning Chrome, Edge, Firefox, Safari, Opera,
- FCAPS-based Monitoring & Management
- Centralized NoC Operations Support as per eTOM guidelines
- Agentless deployments using standard protocols
- Easy adaptation to new devices/applications
- Centralized and remote secured access
- Open-source environment-supported deployment

Modular and Distributed Architecture

- Multi-level distribution support with local and centralized access
- Support for remote operations on local servers
- Secure data transfer between remote and central servers
- Scalable solution with multi-location expansion

Key Feature Sets

Auto Discovery

- Supports multi-mode discovery using typically required SNMP, SSH, and Telnet device credentials.
- IP Networks Scan
- CSV Bulk discovery
- Scheduled Discovery
- Manual Discovery
- API trigger Discovery via NBI

- Offers the option to add any additional topology in the network manually.
- Possesses the option to add Topology via GUI or tabular and enables downloading of topology connections. Discovery works intelligently by identifying the device in the network by the given IP range and categorizing it into network devices and servers with vendor and model details.
- It automatically learns devices that support SNMP, HTTP, Ping, SMTP, POP3, WMI, JMX, SOAP, REST API, PDC, SSH, and Telnet, and any required protocol to communicate to the devices. It discovers the Primary and Secondary lines of each branch connected to DC and monitors the connectivity with the link IP address for fault and performance.

Vulnerability Management

Manage vulnerability issues across devices and most protocols. Instantaneous detection of vulnerabilities in newly discovered target network devices. Multi-level security tagging of device vulnerabilities based on CVSS Scores and vulnerability details.

Device

- CVV
- 3rd Party
- OEM

→

Scan & Identify

CVV Score > Notify > Remediate

Devices Managed

- Routers
- Switches
- Bridges
- Firewalls
- Load
- Balancers
- Wi-Fi Access
- Controllers

Vendors

- Cisco
- HP
- Juniper
- Maipu
- Aruba
- Checkpoint
- FortiGate
- Di3
- Huawei
- Tejas

Network standard configuration protocols used

- SSHv1, SSHv2, Telnet, SNMP v2c & v3, PING, SCP, SFTP, TFTP/FTP, Netconf, HTTP REST-API etc.
- Manages devices using dual IP stacks, IPv4 and IPv6
- Scales the management of devices ranging from 5K to 25K from a single management pane.

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 manual or automatic policy-based “Kill sessions” in case of a protocol breach.
- Record and maintain an audit trail of all user activities.

Routine Task Automation

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

Inventory Tracker

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

Maintains Device critical inventories like:

- Vendor name
- Device Series
- Device Model
- Serial Number
- End of Life
- End of Support
- Serial Number
- OS Type, Version
- Running OS Image file
- Flash Size
- Memory size
- NVRAM size
- Configuration Register
- Chassis
- Ports
- Fan
- Power
- And others

Upload Process

- Configuration Templates
- Configuration Job
- Workflow

- Test & Review
- ACL
- Zero Touch
- Service Config
- Execute
- Merge
- Replace
- Roll Back
- Upgrade
- Audited
- IP Range
- Approval based
- Policy Check
- Failure Remedy

Download Process

Download Device configurations that are either Startup & Running

Download

- Startup & Running Config
- Operational data
- Inventory

Compare

- Changes
- Notify
- Rectify

Workflow

- Security Violations
- Policy Violations

Config Store

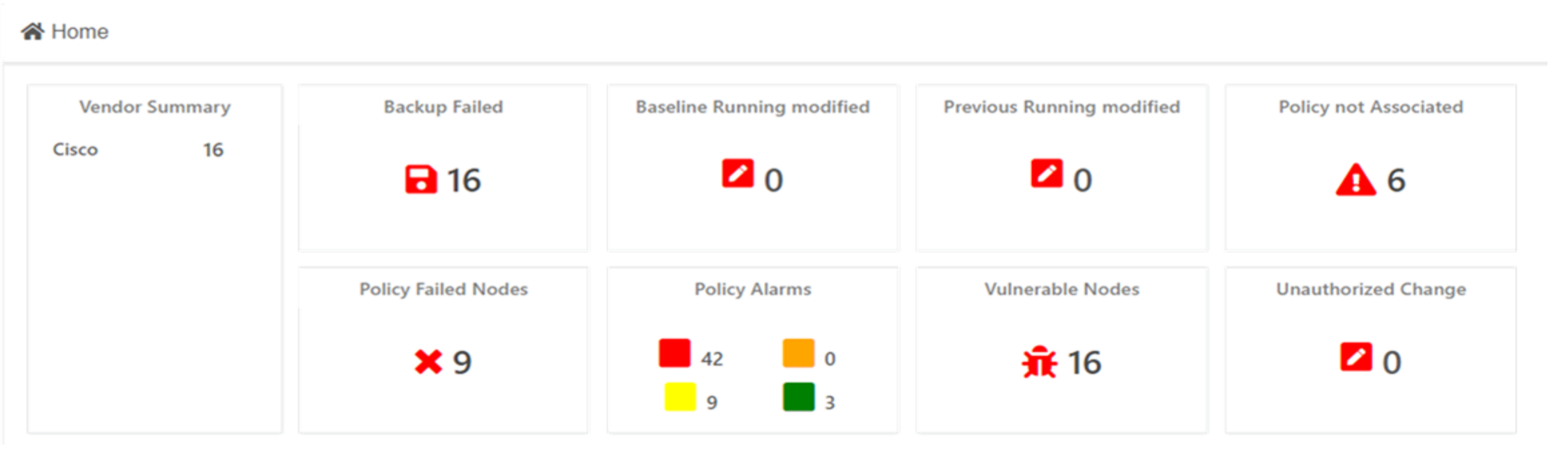
- Versions
- AES Encryption

Audit trails and Tracking

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

Workflow Automation – CLI Job & Live Session

- Perform audited ad hoc configuration changes on devices directly
- CLI Job live session view
- All CLI JOBs are audited and view available
- Auto Remediations for policy violations
- Approval-based or direct config jobs with role-based access
- Will audit and publish the commands before executing on devices and will not restrict in case commands are approved even in Policy violations.



Home

Vendor Summary
Cisco 16

Backup Failed
16

Baseline Running modified
0

Previous Running modified
0

Policy not Associated
6

Policy Failed Nodes
9

Policy Alarms
🟥 42 🟧 0
🟨 9 🟩 3

Vulnerable Nodes
16

Unauthorized Change
0

Accounts & Role-based Access Control

- Local User configurable account database
    - *Temporary Accounts*
- Two-factor authentication
- Access IP Whitelisting
- Default and custom-built Password Policy based on organization policy
- Device Group: controls based on Vendors, Series, Models, IP Address, Locations, Priority, Category, Product Type, Service Type attributes combinations
- Role-based granular access control (RBAC)
- External Account Systems like "Active Directory" or "TACACS+ System" for managing users.
- User groups for creating teams & CAB groups for approval users
- NCCM ACL feature in Policies, Upload Job, Templates, Reports, and Dashboard controls specific users or user groups to manage or view the objects of specific modules

Policy and Compliance Automation

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

- Out of the box delivers the following Policy Compliance standards. PCI DSS v3.2, ISO, NIST, CIS v7, DISA, CISP, etc.
- Policy rules can be Automated as well as user configurable
- Automatic policy check before any change in the network.
- Any network change (not via the system) is detected during the policy check on the following configuration download.
- Auto remediation of the violations based on approvals from admins.
- Policies shall have multiple rules and rule groups per compliance and/or golden template.
- Policy Execution audits are maintained at the device level

Reports

- Offers customizable reporting where users can choose from predefined widgets (40 no's) and apply filters
- Some Report types:
- Audit reports
- Failure report: Backup, non configured
- Download and Upload Job
- Policy Audit and compliance reports
- Inventory Report
- Events Reports
- Task Report
- Device Download Statistics Report
- Device Vulnerability Statistics Report

And many more

Multi-Channel Notifications

Immediate alerting of essential events like detecting configuration changes, configuration download success, policy violations, job completions, firmware upgrades, etc., using multiple channels like Email & SMS and other detailed reports. Any Event detected by the system can be notified to all users.

Different methods are prebuilt into the system:

- SMS
- Email
- Syslog
- HTTP API

3rd Party Integration

- REST API
- SOAP XML
- OEM Connectors
- HTTP

- CMDB
- ITSM
- NMS
- VA
- SIEM
- Active Directory
- TACACS+
- RADIUS

Key Functionalities

Performance Management

Device Credentials

- Stores the "Device Account information such as username, password, enable password" of specific Connection Protocol including SNMP, SSH, TELNET, FTP/HTTP/SMTP in AES 256 encryption standard
- Enable default credentials to connect to the Email server and download the Approval Confirmation Email.

Authentication Profile

- 'Device Authentication Profile' enables SSO authentication of user/user groups (verifying user identity) to access devices through CLI sessions.

Authorization Profile

- Device Authorization Profile' enables authorizing user/user groups (controlling level of access) to perform actions on devices through CLI session. Deny Commands
- Permit but Notify
- Block Commands
- Kill Session

Device Group

- Device Group groups devices under a profile based on Vendor, Configuration Profile, State, City, Location, Device Type, etc., to apply on search, Upload Jobs, Account Device Control

Discovery

Board devices into NCCM through SNMP, SSH/TELNET, and PING protocol. NCCM supports all versions of SNMP, including v1, v2c, and v3. Discover devices through Automatic Discovery, Schedule Automatic Discovery, CSV Upload Discovery, and Add Devices.

- Schedule discovery, i.e., Periodic Automatic Discovery
- Discovery report search using filters: time between changes using the calendar option and device IP address in textbox.

Devices

- The Device Grid Page displays all active devices that are monitored, including Device essential inventories (IP Address, Hostname, Vendor, Model, OS Type, OS Version, and Serial Name), configuration versions, compliance details, Device Actions (SSH, Telnet, Policy Check, Rollback, Download Status, Topology).

Archived Devices

Devices removed from NCCM are kept in archived data for auditing purposes.

- Search Archived device data with these filters: Device Audits, Device Inventories, Device Interface Details, Device Hardware Components, Device Running Configuration, and Device Startup Configuration

Device View

A simple dashboard as the landing page of NCCM for all devices.

- View information on Download Job via IP Address, Node-related information via Hostname

Download Jobs

Download Device configurations that are either Startup & Running

- Download Device Inventory Details, OS image details based on the "Configuration Profile" assigned, Device Credentials, Connection & Download protocol selection, and Schedule (daily, weekly, monthly, and Every 'N' days) period.

Supports the following management protocols:

- SSHv1
- SSHv2
- TELNET
- REST-API
- SCP
- FTP
- SFTP
- NETCONF protocol to maintain the configuration in XML Format.

Upload Jobs

Change the Device Configuration and Device OS Image after the Change Approval Process.

- View Upload Jobs with filters - Upload Job Name, Choose Time from Calendar, Job Completion Time, Job Live Status, Created By, Last Modified, Job Type, Job Frequency, Job Status, Task Status Approval Required, Approved By, Process, Change Request ID.

CLI Jobs/ Sessions

- Enable direct CLI Sessions (SSH or Telnet) between the User and Device. Users can request a CLI connection with the Device IP Address, Device account username (in case of SSH), and the reason for the connection.

Workflow Jobs

- Currently, Workflow Jobs offers Cisco Vulnerability, NIST Vulnerability, Cisco New OS Detection, Cisco New OS Download, Cisco EOX, OS Download from Devices, and Topology discovery.

Configuration Template

- Configuration changes like ‘provisioning,’ “OS Upgrade,” “Service Creation,” “Service Deactivation,” and “any change” on Networking Devices.

Service Template

- One or more configuration templates can be configured to make a service template. A service template is used to fulfill services within NCCM.

Service Job

- Initiate a Service Job from Service Template. The service Job is to select devices, define tasks, and schedule service execution

.

Configuration Trigger

- Used to get information from the devices and information on configuration. Import and export the information collected through Trigger

.

OS Images

- Search OS Image by inputting Vendor, OS Type, Series, Updated details, and Image Name in the textbox.
- Store older images in OS Versions

Configuration Profile

- Device model for Connecting devices (SSH and Telnet Connection commands)
- Model maintains OS Download, OS Upload, Operational Data, ZTP configurations, Other Configurations Download, Syslog Change Pattern

Zero Touch Provisioning (ZTP)

Set up devices to automate device configuration at initial boot up, IT and network operators to configure networking devices without manual intervention. Prerequisites include Base/ Boot image software, DHCP client, Telnet/ SSH, DHCP Options, configuration template, updated ZTP configurations, and Device credentials.

- Map the DORA process using DHCP to get the IP address.

Enables ZTP Process Flow, ZTP Job Upload, ZTP Device Credential, ZTP Notifier, ZTP Configuration System Parameters

Configuration Search

Enable searching of sensitive or policy violation configurations across vendor models at various intervals.

Manually Set the baseline configuration either for single or multiple devices at the same time or Schedule the baseline on a specific period It will be validated against the device running configuration to notify the change.

Baseline Configuration

Manually Set the baseline configuration either for single or multiple devices at the same time or Schedule the baseline on a specific period It will be validated against the device running configuration to notify the change.

Infraon NCCM Product Integrations

Infraon IMS, when integrated with other products from the Infraon Suite, forms a robust offering that can address an array of ITOps challenges in a unified approach. You get a one suite-that-caters to all products. Below, we have listed the critical integration features of three other Infraon Suite products.

Quality of Service (QoS)

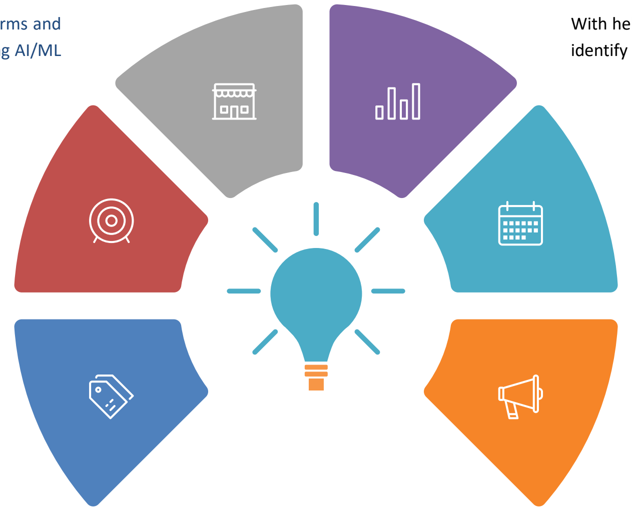
- The tool allows QoS monitoring of WAN links across multiple technologies like Cisco IPSLA, Juniper RPM, Huawei NQA, etc., across multiple protocols like HTTP, TCP, FTP, DNS, etc.
- QoS parameters include link response time, link-level latency, link-level packet loss, link-level jitter, Round Trip-Time, etc.
- It monitors Class-Based Quality of Service (CBQoS) to determine if traffic prioritization policies are effective and if business-critical applications have network traffic priority. It supports CBQoS Nested policies.

Deployment

- The tools covers geographically distributed networks through multi-level scalable distributed deployment architecture and can add new pollers at no extra cost.

INFRAON AIOPS

KEY FEATURES AND FUNCTIONALITIES



EVENT SUPPRESION

Identifies all genuine alarms and suppressing noises using AI/ML

ANOMALY DEDUCTION

With help of prediction algorithm, the system is able to identify the abnormality in business services

EVENTS PATTERN/RELATION

Identifies the unknown relations for better troubleshooting using pattern mapping algorithms

CAPACITY PLANNING

It helps in predicting hardware upgrade required for the increased capacity of CPU, Memory, Storage or bandwidth

ALARM PREDICTION

System will be able to predict the performance alarms which helps in solving the problem prior to its occurrence

INFRAON CHATBOT

Helps in ITSM/Helpdesk automation, which helps in reducing more than 50% support tickets

Licensing

Module Name	NCCM Lite	NCCM Professional	NCCM Enterprise	NCCM Telecom
Discovery Controls				
Automatic Discovery	**Y**	**Y**	**Y**	**Y**
Schedule Discovery	**Y**	**Y**	**Y**	**Y**
CSV Discovery	**Y**	**Y**	**Y**	**Y**
Device Download	**Y**	**Y**	**Y**	**Y**
Configuration Download	**N**	**Y**	**Y**	**Y**
OS Download From Device				
Vendor Device Details				
EOL/EOS Inventory	**N**	**Y**	**Y**	**Y**
New OS Detection	**N**	**N**	**Y**	**Y**
Topology Discovery	**N**	**N**	**Y**	**Y**
SSO, Command & File Control				
Device Authentication Profile	**Y**	**Y**	**Y**	**Y**
Device Authorization Profile	**Y**	**Y**	**Y**	**Y**
Configuration Template				
Configuration Template	**Y**	**Y**	**Y**	**Y**
Configuration Change				
Configuration Change (Upload Job with Single Task)	**N**	**Y**	**Y**	**Y**
Configuration Workflow(Upload Job with Multiple Tasks & Baseline Scheduler)	**N**	**N**	**Y**	**Y**
Configuration Change Only On Single Device	**N**	**Y**	**Y**	**Y**
Network Diagnosis	**Y**	**Y**	**Y**	**Y**
Configuration Trigger	**Y**	**Y**	**Y**	**Y**

Licensing

Module Name	NCCM Lite	NCCM Professional	NCCM Enterprise	NCCM Telecom
CLI Session Audit & LIVE CLI View				
CLI Session Management	**N**	**N**	**Y**	**Y**
Account Management				
Temporary Account	**N**	**N**	**Y**	**Y**
External Directory	**N**	**Y**	**Y**	**Y**
Password Policy	**N**	**Y**	**Y**	**Y**
Captcha Login	**N**	**Y**	**Y**	**Y**
Upload Job, CLI Job and Policy Remedy Approval				
Approval Management	**N**	**N**	**Y**	**Y**
Policy Management	**N**	**Y**	**Y**	**Y**
Vulnerability Management	**N**	**N**	**Y**	**Y**
Views				
Dashboard	**Y**	**Y**	**Y**	**Y**
Report	**Y**	**Y**	**Y**	**Y**
Server Performance Monitor	**Y**	**Y**	**Y**	**Y**
Offline/Schedule Report	**N**	**Y**	**Y**	**Y**
Email/SMS/Syslog/Notifications				
Notification	**Y**	**Y**	**Y**	**Y**
Security				
SecuRA Lite (only CLI command blocking)	**N**	**N**	**Y**	**Y**
ZTP	**N**	**N**	**N**	**Y**
Service Provisioning	**N**	**N**	**N**	**Y**

Minimum System Requirements (For VM as well as Physical Server)

CPU	Quad Core 2 GHz
RAM	8 GB
Hard Drive	100 GB
OS	Oracle 8.5 or above (64-bit)
Please contact our Pre-Sales team to get the exact specifications for your POC/Deployment	

About EverestIMS Technologies

EverestIMS Technologies Ltd. (Everest) is a leading software company – offering ITOM, AIOps, and Telecom OSS solutions. Backed with rich market experience in the I&O, AI, IoT, and digital transformation space, Everest has widespread global footprints through its focused product portfolio. We provide integrated IT solutions, operations, and infrastructure to empower corporations, enterprises, and telecoms to deliver future-ready services to end users. We aim to ensure they adapt and stay competitive in evolving digital landscapes.

Certifications: ISO 20000-1:2018, ISO 9001:2015, ISO/IEC 27034-1:2011, ISO/IEC 27001:2013

Navigate here for more details about us: www.everestims.com

300+	1M+	5M+	100+
Enterprise Customers	Interfaces Monitored	Assets Monitored	Vendors Supported

Reach Us

Phone
+91 80 4656 7100

email
sales@everestims.com

Web
www.everestims.com

Address

Sree Gururaya Mansion, SN 1, No 759, 8th Main Rd,
South Wing, KSRTC Layout 3rd Phase, J. P. Nagar,
Bengaluru, 560 078. Karnataka, India

ITIL® PRACTICES 9
ACCREDITED TOOL VENDOR
Infraon Infinity 7
Silver by PeopleCert

PinkVERIFY® Certified
14 PROCESSES