Manage, automate, and ensure compliance for physical, virtual, and software-defined networks.

Network Operations Management (NOM) provides market-leading management for enterprise networks, integrating capabilities to monitor fault, performance, configuration, and compliance of physical, virtual, wireless, and software-defined network (SDN) infrastructure. NOM also has the broadest and deepest multi-vendor support beyond simple SNMP and ICMP monitoring, supporting more than 180 vendors and 3,400 devices including physical, virtual, Cisco, ACI, VMware, NSX, Viptela, and Cisco wireless along with enterprise scale of more than one million managed objects per global domain.

Network Operations Management is available in three editions with the following features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Express</th>
<th>Premium</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring, Troubleshooting, and Backup</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device discovery, topology, fault, and availability</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Performance and health dashboards and reporting</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Device configuration backup and change history</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Scalable architecture, virtualization, non-prod nodes, IPv6</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Router redundancy, port aggregation</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Quality &amp; Traffic Analysis and Provisioning</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network quality of service (QoS) performance monitoring</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Application and network traffic performance monitoring</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Device OS upgrades and configuration automation</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Executive dashboards and customized reporting</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Network Monitoring, Orchestration, and Compliance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orchestration engine, authoring, and workflow content</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced services monitoring (MPLS, IPT, and IP-MC)</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance policy creation and security content subscription</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-remediation and compliance audit and reporting</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monitoring, Backup, and Troubleshooting (Express)

- **Device discovery, topology, fault, and availability**
  - *Real-time, continuous, spiral discovery & monitoring* delivers an accurate topology view of even the most dynamic networks.
  - *Widest device support* of more than 180 vendors and 3,400 devices.
  - *Monitoring of bandwidth, CPU and memory utilization* proactively alerting operators to network performance issues related to interface and device resources before network performance degrades.
  - *SDN management* provides continuously updated SDN topology visualization of Cisco ACI and VMWare NSX for troubleshooting and impact analysis.
  - *Out-of-the-box, causal analysis* quickly assesses the root causes of network faults, reducing the volume of incidents up to 50%.

- **Performance & health dashboards and reporting**
  - *Out of the box performance reporting* presents users with historical data for troubleshooting and capacity management in a variety of report formats such as Top N, Heat, Headline, Peak Period, Forecast and Executive reports that can be scheduled, saved or emailed.
  - *Diagnostic Analytics* Network configuration change events are overlaid on network performance graphs to correlate and reduce MTTR via enhanced visual inspection for interfaces, memory, buffers, and other metrics – bringing the power of automation together with monitoring.
  - *Configuration data history* enables rapid troubleshooting and resolution with the same context of topology and enables quick restores to previous configurations.
  - *SDN APIC configuration* maintains configuration history of SDN APIC devices in addition to physical and virtual devices.
  - *Proxy server for single sign-on and keystroke logging* of CLI access to devices - centrally secured via permissions so users cannot override the audit trail ad-hoc or have to decide when to log. This ensures audit trail reliability and completeness.

- **Scalable architecture, multi-tenancy, virtualization, non-prod nodes, IPv6**
  - *Enterprise scale and custom polling* provides high-scale (up to 80,000 devices per global domain) and automatic and customizable polling of the managed environment to quickly detect symptoms of network faults and performance issues.
  - *Multi-tenant architecture* delivers network segregation for both external customers and internal operating groups.
  - *Virtual device support* enables monitoring and management for Virtualized Network Functions (VNF) environments.
  - *Non-production nodes* available free of charge for test environments (6-1 ratio).
  - *IPV6 support* enables support for next-generation topology.
• Router redundancy, port aggregation, BGP
  ▪ Enable high availability for enterprise environments with redundant hot backups and port
    aggregation to re-map network traffic.
  ▪ Border Gateway Protocol (BGP) support to exchange routing and reachability information.

Quality & Traffic Analysis and Provisioning (Premium)

• Network quality of service (QoS) performance monitoring
  ▪ Quality of Service monitoring alerts operators to network quality conditions that may
    impact meeting network quality SLAs such as excessive latency, packet loss, and jitter for
    particular network services.
  ▪ Enhanced performance monitoring adds traffic data or QA test data in addition to base
    performance measurement data to provide increased visibility into the performance impacts
    on the network providing faster MTTR to resolve performance-related issues.

• Application & network traffic performance monitoring
  ▪ Traffic monitoring displays traffic patterns and distribution of applications across the
    network as well as traffic volume analysis to provide insight into top applications consuming
    bandwidth.

• Device OS upgrades & configuration automation
  ▪ Network lifecycle workflow automation with a uniquely powerful process-driven
    configuration automation in a granular and flexible method—without scripting.
  ▪ Quickly deploy network infrastructure operating systems updates in mass as part of
    best practices, or in response to security issues to reduce risk.
  ▪ Automate configuration change with rollback with unique “Change Plans” automation
    process to orchestrate mass configuration deployments including automated validation of pre-
    and post-change requirements. Includes automated rollback if post-change requirements are
    not satisfied, reducing delivery errors.

• Executive dashboards and custom reporting
  ▪ Customizable and dynamic Business Value Dashboards (BVD) enable delivery of
    executive and operational dashboards with out-of-the-box or customized content.
  ▪ New BVD content for networks including Network Overview Dashboards provide real-time
    views for executives into network bandwidth, performance, and change frequency to
    understand operational performance and business impact. Network Risk Dashboards
    provide real-time views for executives of incidents, security vulnerabilities, and compliance for
    risk assessment.
  ▪ OpsBridge Reporter addresses the challenges of reporting in dynamic IT environments. In
    addition to consolidating performance data and metrics, Operations Bridge Reporter provides
    sophisticated data collection and aggregation coupled with industry-leading report definition
    and generation capabilities.
Advanced Network Monitoring, Orchestration, and Compliance (Ultimate)

- Orchestration engine, authoring & workflow content
  - **Operations Orchestration** is used to automate troubleshooting and provisioning workflows for network management use cases. These workflows automate discrete network management tasks and can be triggered by detected monitoring incidents, compliance violations, or scheduled automation tasks. Customers can author and customize their own workflows according to their operational processes and needs.

- Advanced services monitoring
  - **Multi-Protocol Label Switching (MPLS)** monitors critical MSP end-customer facing MPLS links and integrates with QoS and Multicast data to provide site-to-site connectivity.
  - **IP Telephony Monitoring** monitors the health, availability, usage, utilization, and quality of experience of the voice network components.
  - **IP Multicast** monitors multicast monitoring providing fault alerts to operators as well as a graphical representation of the multicast flows.

- Compliance policy creation and security content subscription
  - **Advanced policy creation** with granular permissions to control access and structured logic to manage change instructions.
  - **Security and compliance content** to help reduce time to detect security risks from either device vendor published vulnerabilities or network management government or industry best practices including SDN devices such as Cisco ACI and VMWare NSX.
  - **Three-Dimensional compliance auditing and remediation** to track the state of compliance and remediate in real-time relative to configurations, running state, and OS version, together with a variety of others device attributes to control risk.
  - **Proactive policy enforcement and audit and compliance reports** including: ITIL, PCI, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act.