DATASHEET

io Canvas

Experience the power of Practical AI for 360° Observability and Actionable Insights

AI-Powered Unified Network Platform

Unified management and control across Access Points, switches, and clients through a single pane of glass, powered by AI-based analytics to detect problems and performance bottlenecks, identify anomalies, and faster RCA for reducing the Mean-Time-to-Resolution (MTTR).

Deployment-Ready at Any Scale

From small offices to large, distributed campuses, io Canvas scales flexibly with multiple deployment models, to match your growth and control needs.

Zero-Touch Provisioning

Onboard hundreds of devices in minutes with bulk provisioning, apply network and device-level policies automatically using hierarchy-based configurations, and reusable templates.

Secure & Standards-based Integrations

Enable third-party integrations—including Captive Portals, AAA servers, NAC systems, Syslog server. Seamlessly integrate with external applications via northbound REST APIs supporting secure data exchange.

QoE-based Performance Monitoring

Move beyond static QoS metrics and translate real-world user experience into a single QoE (Quality of Experience) score, trained to adapt to app behaviour, network dynamics, and user satisfaction instead of a multitude of network KPIs.

Always-on Analytics at Entry Level

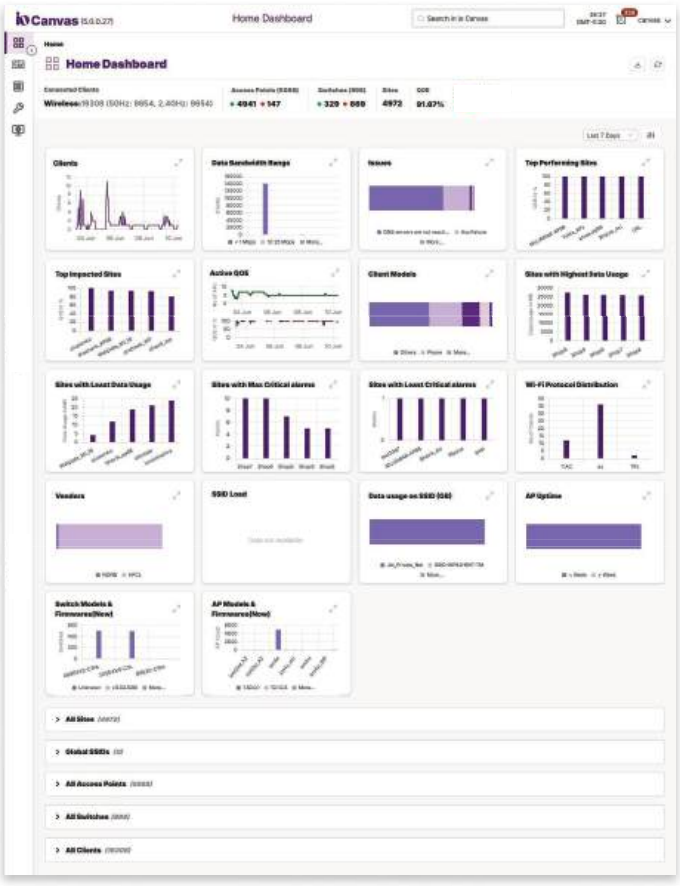
AI-driven analytics engine runs 24x7x365 across sites, devices, & clients and is available to deliver insights across all license tiers, ensuring no blind spots in network performance.

Client-Centric Issue Intelligence

Go beyond basic KPIs with deep visibility into client-specific issues encompassing connectivity failures, network-layer anomalies, application experience disruptions.

Issue Detection & Recommendations

Let the system proactively identify issues in the client experience journey and guide you with actionable AI recommendations to reduce Mean Time to Resolution (MTTR), ensuring consistent satisfaction for end-users across all applications and devices.



io Canvas

Automated Network Assurance with QoE Monitoring

Navigating Modern Network Complexity

Enterprise networks have evolved rapidly, driven by the rapid proliferation of devices, surge in cloud-first strategies, and widespread IoT adoption, increasing both the complexity and the criticality. Network environments are now highly dynamic, hosting a diverse mix of wired and wireless devices, hybrid architectures, and multiple layers of security. Just as complexity peaks, end-user demand for flawless connectivity turns it from a challenge into a daily stress test for network teams.

Rising Pressure on Network Management

For administrators, this complexity translates into unmanageable events flooding network logs daily, blurred priorities, and reactive. Manual configurations across distributed sites introduce risk and delay, while repetitive tasks drain time from strategic initiatives. As a result, performance gaps linger, and user experience suffers.

Beyond the Buzz: Embracing Practical AI

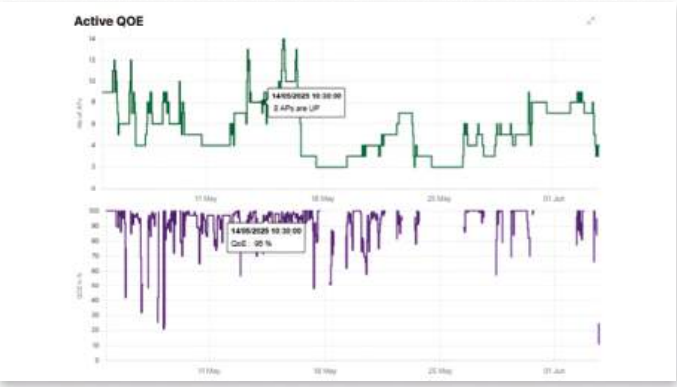
As networks grow more complex, IT teams no longer need AI for novelty, they need it for clarity and action. While many platforms claim AI, few deliver meaningful assistance to those managing real-world networks. What network teams truly need is Practical AI, an intelligent assistant that doesn't just report symptoms, but helps resolve the underlying problems. It guides administrators through root cause, scopes the blast radius, recommends precise actions, and learns from each incident to improve future responses.

Practical AI with io Canvas

io Canvas is a unified, AI-powered network management platform designed to provide practical AI which cuts the clutter to bring much-needed clarity in the face of increasing complexity. Engineered to offer comprehensive visibility and control across network entities, io Canvas pinpoints root causes, highlights what matters, and guides resolution in real time.

Elevating User Experience with QoE-Driven Intelligence

Traditional Quality of Service (QoS) metrics—bandwidth, latency, jitter, packet loss—often fall short of reflecting the true user experience. Users can face poor video conferencing quality or lagging applications even when basic network parameters appear healthy. io Canvas transforms conventional performance monitoring with its Quality of Experience (QoE) based network intelligence, emphasizing the actual user-perceived performance rather than technical thresholds alone. Powered by advanced ML algorithms and AI, the QoE feature translates real-time application behaviours, network dynamics, and end-user feedback into a single, dynamic Quality Index (QI) score. This QoE indicator is continuously recomputed based on end-user device behaviour and user interactions, offering administrators meaningful insights into the true quality of service delivered.



With io Canvas's QoE capabilities, administrators gain an unprecedented level of clarity and actionable intelligence, enabling them to proactively optimize network experiences,

io Canvas

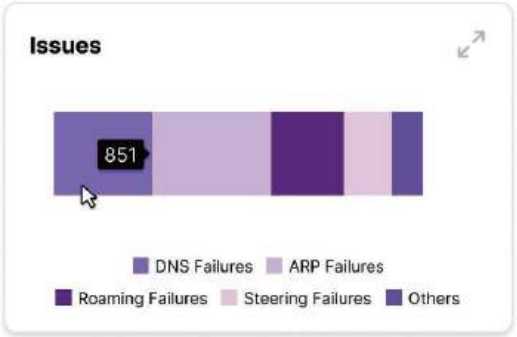
Practical AI with Multi-Layer Framework

Purpose-Built AI

io Canvas brings AI not as a monolithic block, but as a multi-layered, purpose-driven engine. Each layer builds on the underlying layer(s), offering, escalating intelligence from visibility to insight to autonomous action. Network teams can gain the right level of assistance, tailored to their operational maturity and scale.

- **Foundational AI: Real-Time Visibility**

  At the base layer, Foundational AI offers instant awareness of what's happening in the network. It constantly **tracks QoE**, **connectivity failures** like DHCP timeouts or authentication issues, and **real-time usage**, **performance** and **anomalies** across sites, devices and clients. With historical performance baselines at both AP and client levels, administrators no longer operate in the dark—they gain full visibility into how the network is behaving right now.



- **Analytical AI: In-Depth Insight and Prioritization**

  Analytical AI brings context to the surface. It diagnoses where bottlenecks are forming, prioritizes incidents based on their user impact, and surfaces application-level experience data. It goes further with **client journey analytics**—tracking roaming behaviour, latch times, and connectivity patterns—giving admins clarity on **user pain points**. This layer empowers teams to stop guessing and start solving with confidence.

- **Predictive & Autonomous AI: Proactive Optimization**

  The most advanced layer turns insights into action. io Canvas continuously **optimizes performance** with intelligent channel selection, dynamic bandwidth allocation, and smart client steering. It detects roaming inefficiencies and fine-tunes cell boundaries in real time. Best of all, it performs **QoE-driven auto-corrections**, ensuring performance never lags behind user expectations.

AI Capabilities	Real-time Visibility	In-depth Analysis	Predictive Automation*
Foundation AI			
Real-time QoE degradation insights	★		
Wireless connectivity insights (e.g., DHCP, Auth failures)	★		
Usage insights (Traffic patterns, Client density)	★		
Historical performance insights (AP, Client)	★		
Analytical AI			
Network performance optimization (Spectral, Airtime)	★	★	
Incident detection & prioritization	★	★	
Application experience insights	★	★	
Client connectivity analytics (Roaming, latch times)	★	★	
Advanced diagnostic & troubleshooting support	★	★	
Predictive & Autonomous AI			
Dynamic channel & bandwidth optimization	★	★	★
Intelligent client steering	★	★	★
Intelligent cell adjustment	★	★	★
Roaming pattern insights & proactive adjustments	★	★	★
Advanced QoE-driven auto-corrections	★	★	★

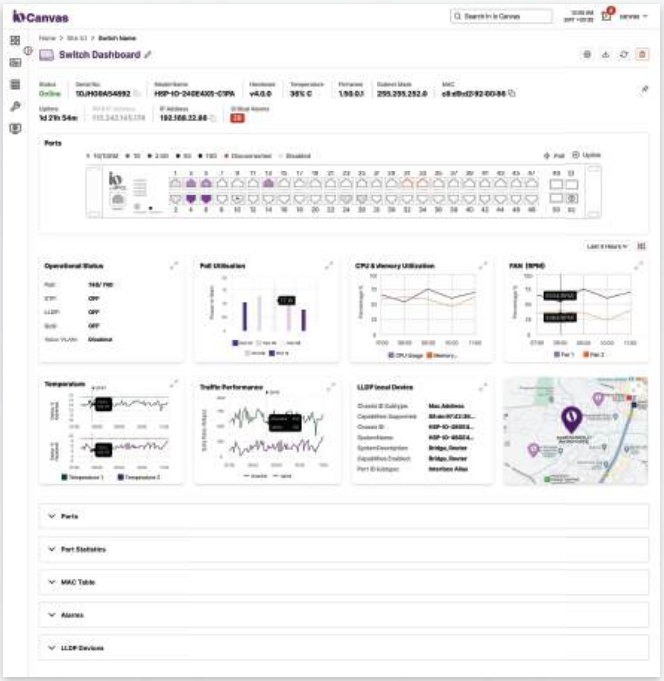
**Predictive Automation features will be available in future releases of io Canvas*

io Canvas

Single Pane of Glass: Unified Platform for Wired and Wireless Network Elements

End-to-End Visibility

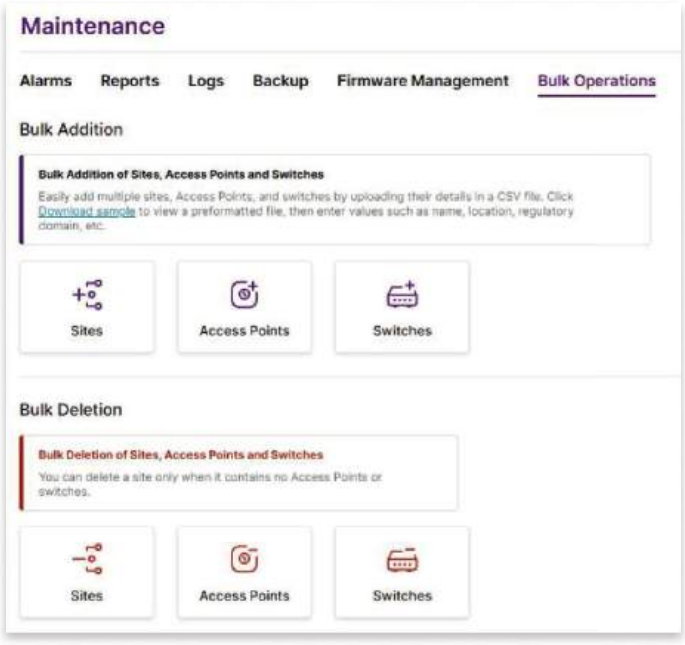
io Canvas provides full visibility across the network, from switches to access points to clients and user applications. With detailed dashboards, user is able to view the network performance across the network hierarchy, with user friendly navigation across and within the dashboards.



Operational Agility

Repetitive configuration work often slows down network rollouts. io Canvas removes that grind with **Global Profiles** (reusable configuration objects), and one-click **site cloning** that replicates entire network across locations. **Bulk onboarding** of APs, switches, and sites is supported, with **zero-touch provisioning** automatically applying the appropriate settings as soon as devices connect.

Beyond initial configurations, io Canvas streamlines ongoing operations with **scheduled firmware upgrades** and **site backups**. Admins can stage updates by sites, minimize downtime with maintenance windows. Combined, these tools turn time-consuming rollouts and updates into a reliable, scalable workflow.



io Canvas

Secure Your Network at Every Layer

Layered Security Right from Login

Security in io Canvas begins with protecting access to the platform itself. **Two-Factor Authentication** (2FA) ensures that only authorized administrators can log in, adding a vital layer of control. From there, io Canvas delivers a layered, end-to-end security.

Administrators can also manage user access through built-in **User** and **Role Management**, enabling them to create user accounts with specific role-based permissions. These roles ensures users access only what they are authorized to. All user actions are captured via **audit logs**, offering full traceability and compliance.

Access Control Layer

Access to the network starts with intelligent access control. io Canvas enables centralized and granular access management through user-based authentication methods (such as **Multi PSK**) and device-level access controls (**MAC-based ACLs**). These are enforces at network elements, i.e., Access Points and Switches.

Policies can be centrally defined, reused, and consistently applied across both wireless (SSID-level) and wired (port-level) infrastructure, ensuring comprehensive, uniform security at every network entry point. **Integrated NAT profiles** and captive portal-based access (via **io Pass**) ensure that guest and external traffic stays contained and auditable. **Role-based VLAN assignment**, **session tracking**, and **custom access controls** further elevate security and regulatory compliance.

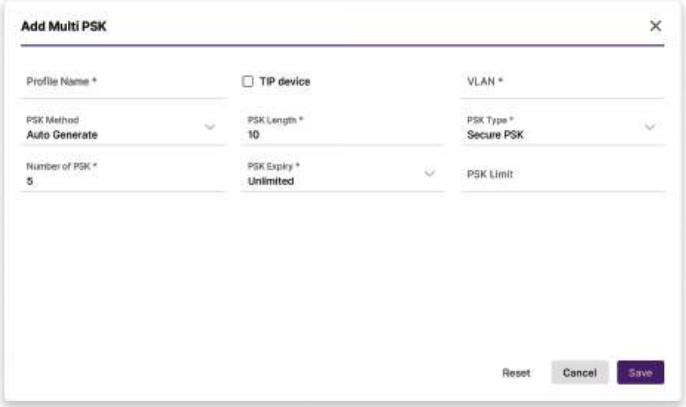
Policy Enforcement Layer

From **Layer 2 to Layer 7**, administrators can implement precise control over user traffic by leveraging ACLs, per user/SSID bandwidth limits and URL/IP filtering.

RF & Wireless Protection Layer

At the radio layer, io Canvas features **built-in WIDS/WIPS** capabilities. Access Points actively monitor the RF environment for threats like **rogue APs**, **spoofing**, **beacon floods**, **de-authentication attacks**. Admins can configure detection thresholds and toggle real-time mitigation ensuring the airspace stays secured.

io Canvas enables users to choose the appropriate user authentication mechanisms for different business requirements, for ensuring secure access and data encryption. **Client isolation** helps network administrators to prevent peer-to-peer communication.



Seamless Ecosystem Integrations

io Canvas is built for interoperability, enabling easy integrations into diverse enterprise IT environments. It supports standards-based interfaces to connect with **external AAA servers** (RADIUS, LDAP, TACACS+), **NAC solutions**, and **third-party captive portals** for centralized access control and authentication workflows.

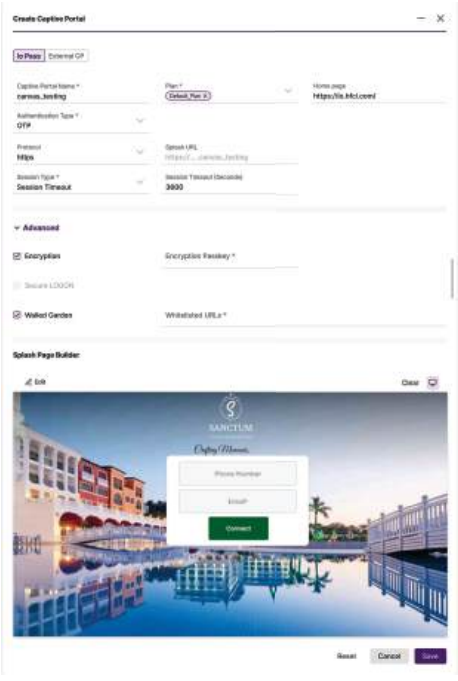
Administrators can integrate io Canvas into broader monitoring and automation platforms using **Northbound APIs (NBI)**. These secure, token-authenticated APIs support real-time access to performance KPIs and alarm data, making it easy to feed network intelligence into ITSM tools, NOC dashboards, or reporting systems.

Syslog integration ensures that logs from controllers and APs can be forwarded to centralized logging systems for compliance, auditing, or forensic analysis.

io Canvas ensures that key network operations such as **user onboarding, alarm notifications, troubleshooting** and **reporting** can be integrated directly into your existing IT systems. Whether it's feeding KPIs into a monitoring dashboard or sending alarms to your incident management tool, the platform keeps your network data in sync with the broader enterprise environment.

Frictionless Guest Access with io Pass

io Pass, the platform's **built-in captive portal and AAA** engine, delivers a fully customized guest Wi-Fi experience. Whether offering **click-through** access in a shopping mall, **OTP-based** onboarding in a corporate campus or **voucher-based** access at airports, io Pass adapts to the scenario. It gives admins full control over session lifecycles, usage quotas, and access plans. io Pass also supports 3rd-party captive portal integrations.



io Canvas

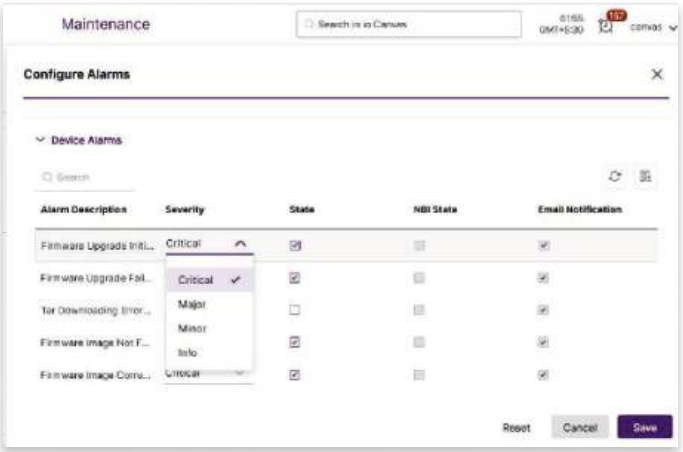
Experience the power of Practical AI for Unmatched Efficiency and Smart Insights

Enhancing Operational Efficiency

Modern IT teams need fewer tickets, faster MTTR and confidence that every maintenance window actually improves the network. io Canvas bakes those outcomes into day-to-day operations with three operator centric pillars:

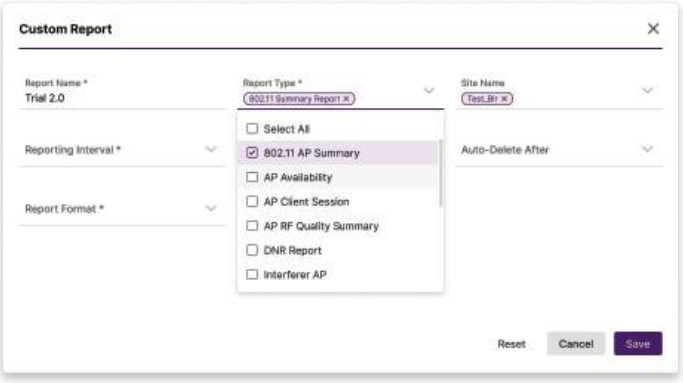
Proactive Alarms and Events

io Canvas equips administrators with a centralized view of **system health** through the alarms engine. Alarms can be classified by severity - **Critical**, **Major**, or **Minor** and presented with clear timestamps and impacted elements. Alarms can be delivered as **email notifications** or streamed to **external systems** via REST APIs, ensuring seamless integration into enterprise workflows and reducing reliance on manual monitoring.



Device and KPI Reporting

io Canvas provides rich, **customizable reporting** availability on device health, usage, connectivity trends, and service quality. Administrators can generate **on-demand** or **scheduled** custom or pre-defined reports, covering KPIs like signal quality, throughput, client density, and session behaviour, filtered by site, AP, or client. Reports can be exported in formats like CSV or Excel, aiding audits and long-term performance analysis



Monitoring & Troubleshooting Toolkit

io Canvas includes a robust toolkit that covers both proactive monitoring and troubleshooting. Administrators can initiate **AP snapshots**, capture **live packets** remotely, or trigger **LED blink** for device identification, all from the dashboard. With full role-based access control and **audit logging**, every action is tracked, ensuring accountability while empowering network teams to respond quickly and precisely to issues as they arise.

io Canvas

Deploy with Confidence: A Platform for Every Enterprise Scale

Flexible Deployment for Every Network Scale

io Canvas is architected with versatility in mind, offering distinct deployment models tailored to the unique requirements of your network, scale, and administrative preferences.

Shared Enterprise (SE)

The Shared Enterprise variant provides a **fully managed**, **cloud-hosted** environment, ideal for businesses aiming to minimize infrastructure overhead and rapidly **scale network management**. SE significantly reduces operational complexity, freeing your teams from managing infrastructure, updates, and maintenance tasks, allowing more focus on strategic network operations and end-user experience.

Private Enterprise (PE)

Designed for enterprises requiring stringent control and data sovereignty, the Private Enterprise model offers **on-premise** or **private cloud-based** deployment. PE gives you complete visibility, management, and data ownership within your own infrastructure, complying effortlessly with your security, compliance, and regulatory mandates. It is built to scale up to **100,000 network devices** and supports **1+1 high availability** and **full DC/DR** readiness to ensure maximum resilience and uptime.

Light Enterprise (LE)

The Light Enterprise edition serves smaller enterprises and branch-office environments, combining simplicity with robust capabilities. Deployed **on-premise**, LE offers a streamlined management solution for environments with up to **5000 network devices**, without compromising on core management, security, or analytics capabilities.

Licensing Flexibility Tailored to Your Needs

io Canvas licensing tiers ensure that you gain access precisely to the capabilities your network demands, with each license incrementally unlocking powerful AI-driven functionalities designed to scale with your organization's evolving needs.

Essentials License – Foundation for Network Visibility

Essentials tier provides fundamental **AI-powered insights** that help network teams quickly identify and track performance issues. It includes **real-time QoE** metrics, basic **network health monitoring**, and **historical analytics**, making it suitable for organizations starting their journey toward intelligent network management.

Premium License – Enhanced Analytical Intelligence

The Premium tier builds upon Essentials by adding **advanced analytics** for deeper insights and proactive issue diagnosis. Administrators gain access to comprehensive **root-cause analysis**, **performance optimization tools**, detailed **application experience** analytics, and **prioritized incident** detection—significantly boosting network reliability and operational responsiveness.

Premium Pro License – Predictive and Autonomous Management

Premium Pro represents the pinnacle of io Canvas intelligence, incorporating **predictive analytics** and **autonomous optimization** features. The platform intelligently predicts network conditions, **dynamically adjusts** resources like channels and bandwidth, steers clients intelligently, and **proactively corrects** potential QoE issues, ideal for businesses requiring sophisticated, hands-off management of large scale, high-density environments.

Deployment Variant	Shared Enterprise (SE)	Private Enterprise (PE)	Light Enterprise (LE)
Description	Fully Managed, Scalable Public Cloud Instance	Dedicated Self Managed, Private Cloud or On-premise Instance	Lightweight On-premises Instance deployable on Laptop, Desktop, or VM
Scalability	Unlimited Network Devices	Up to 100,000 Network Devices	Up to 5000 Network Devices
Management	Centralized Multi-tenant Management	Centralized, Single & Multi-tenant Management	Centralized Management with Easy Self-administration

iQ Canvas

Experience the power of Practical AI for Unmatched Efficiency and Smart Insights

Product Specifications

Network Management

- Zero Touch Provisioning of Access Points and Switches
- Hierarchical organization of network elements for inheritance-based configuration and policy management
- Ability to customize configuration at AP/radio and switch/port level
- Profile-based approach to simplify repetitive configurations
- Single console for account and inventory management

Network Monitoring

- Global/Site dashboards with summary of APs, Switches and Clients
- Drill down to individual AP, switch and client dashboards
- Live and Historical Alarms
- Inventory management
- Device and System Health monitoring
- AP, Switch and System Logs

Performance Management

Global Dashboard

- Total count of connected clients, access points, switches, and active sites
- Current and historical QoE views
- Categorization of sites based on performance, usage and alarms
- Switch, AP and client summary statistics
- Summary of active critical alarms requiring immediate attention

Site Dashboard

- Site-level details for client density, QoE scores, and network traffic
- Insights into connection times and roaming statistics
- Real-time visibility into wireless connectivity issues including DHCP and authentication failures
- Time-series view of site-specific KPIs
- Categorization of APs based on performance
- Summary views of switches, APs and clients associated with the site

AP Dashboard

- Connected client count and real-time network/device health per access point
- Time-based performance views including RF, application and health metrics
- Channel occupancy, utilization and interference per radio
- Rogue AP listing
- Device-specific alarms list

Switch Dashboard

- Port utilization, VLAN insights, and PoE usage per switch.
- Switch-level throughput, traffic flow details, and historical performance metrics
- Health indicators including CPU and memory usage
- Real-time operational status for each port and VLAN configuration accuracy

Client Dashboard

- Detailed session history and connectivity insights per client
- Real-time visibility into connection and roaming latencies, and application experience
- Analysis of client-specific QoE scores and signal strength
- Identification of individual client issues such as DHCP/DNS/ARP failures and poor link quality and their underlying cause

Fault Management

Real-time Alarms

- Instant visibility into critical, major, minor, and informational alarms related to devices, network, and system health

Alarm Customization & Notifications

- Administrators can configure alarm severity levels, enable or disable specific alarms, and set up email notifications for timely responses

Alarm Suppression & Correlation

- Set damp periods and thresholds to minimize alarm fatigue by avoiding redundant alerts; correlated alarms group related events for easier diagnosis

Historical Alarms

- Store and access historical alarms to analyze patterns, recurring issues, and improve long-term network performance and stability
- Secure NBI integration using REST API along with Alarm dampening to control network flood alarms

Performance Reports

- Generate both on-demand and scheduled reports covering APs, clients, RF metrics, alarms, and network usage trends
- Choose from a wide variety of report types: client sessions, AP performance, RF quality, interference detection, and availability reports
- Automated KPI Reports for NBI integration
- Customize reporting intervals (15 mins, 1 hour, 6 hours, 1 day) and durations (e.g., last hour, yesterday, last week)
- Export reports in CSV or Excel format

OpenWiFi (OWF)

- Support for OpenWiFi Controller to manage APs running Open Wi-Fi firmware
- Works with HFCL Access Points only

Hotspot 2.0 Support

- Enables secure, automated onboarding of mobile devices to public and carrier Wi-Fi networks
- Facilitates mobile data offload and enhanced roaming experiences through Passpoint/HS2.0 standards

Security and Access Control

- SSID-level security management
- MAC-based and RADIUS-based access control
- Multi-PSK support
- Dynamic & Static VLAN assignment and client isolation
- WIDS and WIPS
- Client Isolation

Security Gateway Integration (SE, PE only)

- Configure and monitor Unified Security Gateway appliances with built-in firewall, IDS/IPS, content filtering, and advanced networking features.

Content Filtering

- Ability to block content as per network policy
- List of URLs /IP Addresses / Categories with allow/deny rule

io Pass Captive Portal

- Built-in captive portal with splash page builder
- Onboarding methods: Click-through, Voucher, OTP (SMS), along with Sponsor Approval and integrated AAA
- RADIUS integration and customizable access plans

External Captive Portal Integration

- Integration with third-party captive portal providers for guest and employee onboarding
- Enables redirection to external onboarding workflows while maintaining secure access control

AAA Integration

- RADIUS-based integration with external AAA servers for 802.1X and captive portal SSIDs
- Option to proxy RADIUS requests via io Canvas
- Supports AAA server redundancy to ensure high availability during authentication

Northbound API

- RESTful APIs for seamless integration with external IT systems including NMS, ticketing, and reporting platforms
- Provides access to alarms, KPIs, and device data for centralized monitoring and automation

Logs

- Centralized log management for system, audit, security, and event logs
- Real-time and historical log views with customizable retention periods
- Export logs to external Syslog servers for compliance and analytics

Troubleshooting

- Instant client-level diagnostics for DHCP, DNS, and connectivity issues
- Integrated troubleshooting toolkit including remote packet capture, AP snapshots,
- Live RF environment details for proactive radio interference analysis and optimization

Maintenance

- Scheduled firmware upgrades with backup capabilities
- Backups and quick restoration of configurations
- Bulk device and site provisioning and deletion
- Site-wide configuration cloning for efficient, error-free network operations

User and Role Management

- Add, modify, or delete users and assign roles with site- or function-specific permissions
- Granular role-based access control (RBAC) ensures secure multi-user administration
- All user actions are captured via audit logs for traceability and compliance

Last Updated June 10, 2025

io by HFCL

Email: iosupport@hfcl.com
Website: hfcl.com | io.hfcl.com
Office: 8, Commercial Complex, Masjid Moth, Greater Kailash II, New Delhi 110048