ExtremeCloud™ IQ

Highlights

Unified for Simplicity

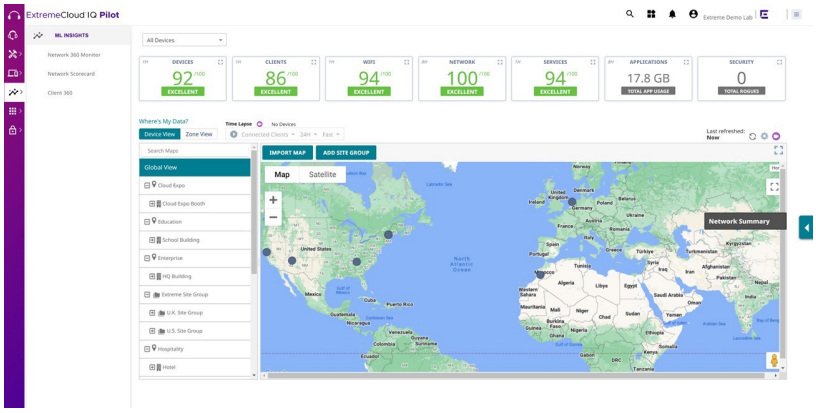
- Enable end-to-end management of wired, wireless, and SD-WAN networks.
- Manage Fabric, Extreme, third-party, and IoT devices with greater efficiency.
- Provide real-time and historical views of client and device health with built-in remediation tools.
- Expedite network planning and optimization with the Next Gen Wi-Fi Maps feature.
- Facilitate visibility and control of application usage and network access services.

Automated for Scale

- Apply configuration policies automatically and use workflows to enable near zero-touch deployment.
- Speed onboarding, provisioning, and setup with Instant operations.
- Enable integration for provisioning, management, and customization using APIs that support the OpenAPI standard.

Cloud Continuum Choice

- Deploy ExtremeCloud IQ using a consistent operational model across three cloud deployment options—public, private, or ExtremeCloud Edge.
- Choose from 21 points of presence (PoPs) worldwide across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- Connect to Extreme on-premises management applications to facilitate a migration path for current and legacy Extreme devices, as well as third-party devices, to cloud-based management.



The complexity of network operations is increasing as the demand to support remote workers and the addition of new business services at the edge continue to grow. IT organizations are under pressure with limited staff, so they need greater simplicity and automation. They are responding by transitioning to cloud-based network management applications and want the flexibility to transition to the cloud when and how they choose. Operations teams want to leverage artificial intelligence for IT operations (AIOps) that helps them to simplify complex tasks and use cases, so they can proactively manage their environment.

ExtremeCloud™ IQ provides unified management for wired, wireless, and SD-WAN to reduce risk and simplify operations. It is a core component of Extreme's One Network, One Cloud framework that is secure by design and provides cloud choice for data residency and privacy. ExtremeCloud IQ delivers unified management of Extreme devices, and it manages Cisco and HPE Aruba switches, easing the transition to cloud-based management. It also provides basic setup and monitoring of a large array of other third-party devices.

This innovative platform streamlines operations by delivering new levels of network visibility, automation, and intelligence using transparent machine learning (ML) algorithms. ExtremeCloud IQ incorporates many AIOps capabilities, such as network and client insights, that help users reduce mean time to resolution (MTTR). It also includes intuitive configuration workflows, real-time and historical monitoring, comprehensive troubleshooting, and integrated network applications.

The CoPilot add-on license brings additional practical AIOps functions that help identify problems before they impact operations. They include the Connectivity Experience feature with a quality index (QI) score and Wired and Wireless anomaly detection capabilities. Users can trust the insights and recommendations from AI because of the transparency provided by Explainable ML.

Unified for Simplicity

ExtremeCloud IQ provides the industry's most unified management of wired and wireless devices, including third-party devices. It provides a centralized view of the entire network with visibility of network and Internet of Things (IoT) devices without having to piece together multiple tools. Extreme is focused on practical AIOps.

These capabilities are available in both the Pilot license tier and the CoPilot add-on license, and they include a range of complementary attributes. They help to significantly simplify and streamline the remediation process: identify, know, and act.

The following table summarizes how the AI and ML capabilities in ExtremeCloud IQ facilitate wired and wireless network remediation:

AI capabilities/features	Identify	Know	Act
Pilot license tier			
ML Insights Network Scorecard, Network 360 Monitor, and Client 360	◆	◆	
Client Monitor with dynamic packet capture (PCAP)		◆	◆
CoPilot add-on license			
Connectivity Experience	◆	◆	
Anomaly Detection: Wi-Fi Capacity, Wi-Fi Efficiency, DFC Recurrence, Port Efficiency, PoE Stability, Adverse Traffic Patterns, Wireless, Device Health Monitoring, and Virtual Local Area Network (VLAN) Mismatch	◆	◆	◆
Explainable ML		◆	◆

Table 1: Summary of the ExtremeCloud IQ AIOps capabilities/features and the remediation process

- **ML Insights**: Analyzes device-generated telemetry data that is depicted in both real-time and historical dashboard views with the ability to drill-down to details.
- **Client Monitor**: Helps identify and troubleshoot network events that clients typically encounter when associating with an access point (AP), authenticating, and accessing the network. Intelligent automation triggers dynamic PCAP to collect salient data used for root cause analysis, and the suggested remediation is provided.
- **Connectivity Experience**: Summarizes client experience into a single QI score to easily track, identify, and troubleshoot connectivity performance issues.
- **Anomaly Detection**: Uses dynamic baselines to address the most common use cases in three relevant categories: client experiences, wireless experiences, and device CPU loading.
- **Explainable ML**: Transparent ML algorithms help explain how the analytics were derived, so users can trust the insights and recommendations.

AIOps Capabilities in CoPilot

AI provides many advantages, but these technologies are still evolving and can generate false positives. Administrators want to understand the insights and recommendations generated by AI. The ExtremeCloud IQ algorithms are built with transparency using Explainable ML. This makes it easier for administrators to understand how the insights were derived. They can see, verify, and trust the data behind every recommendation, and CoPilot provides the best options for resolution. It proactively reduces risk and provides the fastest time to the best experience.

Figure 1: CoPilot Connectivity Experience feature

The Connectivity Experience feature summarizes client experience into a single QI score to easily track, identify, and troubleshoot connectivity issues. ExtremeCloud IQ processes information from all relevant metrics to define dynamic baselines, identify outliers, and provide the necessary context to remediate issues. It calculates a QI score for each wired and wireless client that serves as an indicator of the client's connectivity experience. Any decline in the QI value indicates a degraded experience for the client. For wireless clients, the QI is a composite score comprising two main components: time to connect and performance score. For wired clients, the QI is a function of the interface errors on the connected wired port

CoPilot Anomaly Detection is focused on use cases that were derived from the most common customer service tickets. This helps identify a set of real-world networking issues and anomalies. The use cases can be grouped into three categories: client experiences, wireless experiences, and device CPU loading. Wired and wireless anomaly detection helps ensure the user experience by providing analysis per location, SSID, and client type. This capability also includes identifying anomalies in the time to connect, to associate, and to authenticate a device.

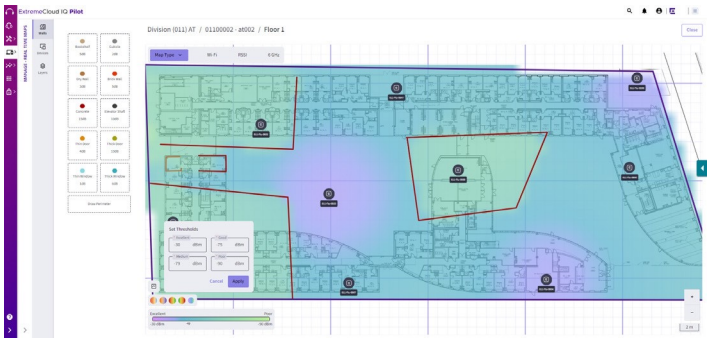


Figure 2: NextGen Maps with real-time RF views

Additional Advanced Capabilities

In addition to AIOps, ExtremeCloud IQ includes advanced capabilities to simplify and enhance daily operations. NexGen Maps display real-time radio frequency (RF) and responsive views at scale. Users can visualize active channel plans on all three bands: 2.4 gigahertz (GHz) WiFi and Bluetooth Low Energy (BLE), plus 5 and 6 GHz WiFi. It includes a scaling tool with definable wall types, custom attenuation values, an AP expandible device modal, and client information modals. One-click importation with leading design tools, such as Ekahau and Hamina, further simplifies Wi-Fi network planning.

Application performance monitoring using flow-based data provides a better understanding of user behavior in the network and identifies the level of engagement. It correlates metrics to provide context-based visibility and analytics of application and network performance. Proactive alarms and events help reduce the number of trouble tickets and escalations by looking for patterns ahead of time to identify the anomalies that matter and to recommend actions to address them quickly.

ExtremeCloud IQ provides support for Internet of Things (IoT) devices and supports Thread, a low-power, low-bandwidth IPv6-based wireless protocol that allows IoT devices to talk to one another. Using ExtremeCloud IQ to assign an IoT Thread profile to an AP5010/AP5010U wireless interface allows the device to function as a Backbone Border Router (BBR). It provides administrators with real-time insights into the health and topology of their Thread network. They can view if/when a network segmentation has occurred and interact with different roles: leader, border router, BBR, and commissioner.

Automated for Scale

ExtremeCloud IQ provides cross-domain workflow automation capabilities through an intuitive graphical approach to easily automate network tasks. The workflow tools and support for common scripting languages deliver the ability to create the sequential execution of tasks for customized orchestration. They make day-to-day tasks more efficient and consistent. The ExtremeCloud IQ API provides a full suite of cloud-optimized open APIs for developers. It conforms to the industry standard for RESTful API design, OpenAPI, and supports the Swagger UI. The API allows customers and partners to create solutions for the management, monitoring, and provisioning of any ExtremeCloud IQ environment.

Switch Automation

Instant actions speed switch provisioning, and configuration, including:

- **Instant Onboarding**: Scan using the Extreme Companion app or type in the product serial number for instant assigned cloud-based management. Administrators can choose the operating system for their Universal Devices.
- **Instant Port**: Automate device adds, moves, and changes across Series 4120, 4220, 5320, 5420, 5520, 5720, and X435 switch ports, eliminating the need for manual port reconfiguration.
- **Instant Stack**: Simplify cloud-based stack provisioning by automating setup through a single push-button operation across multiple switches.
- **Instant Port Profiles (IPP)**: Automate the configuration of switch ports based on the type of connected device, such as APs, security cameras, and voice over IP (VoIP) devices.
- **Instant Secure Port**: Link to the Universal ZTNA RADIUS service for integrated authentication and policy enforcement.

Access Point Automation

Templates for APs enable rapid deployment, with most of the port settings already applied by the associated template. Auto-provision profiles are based on device models. Users can define multiple profiles for a given model and distinguish which devices get which profile by specifying a serial number or IP address.

The Companion Mobile App, for Android and IoS, helps simplify the provisioning and configuration of devices and creates a full installation report. Companion allows users to monitor and access details about the network from any location in near real time, and it includes a comprehensive troubleshooting toolbox. The unique augmented reality (AR) feature, Visualize Wi-Fi, is another example of the practical implementation of an advanced technology to view the quality of an install. Users can view the quality of the client connection, observe the client roams, and view all the neighboring networks, augmented with the real environment. Videos or pictures taken with Companion enabled mobile phone can be included in the Wi-Fi installation or troubleshooting documentation.

Cloud Continuum Choice

ExtremeCloud IQ offers software as-a-service (SaaS) simplicity with rapid feature velocity, increased availability, and the flexibility desired for efficient network management. The application operates on Extreme's cloud services architecture that is secure by design with Infrastructure as-a-Service (IaaS) vendor agnostic security and privacy certifications. It conforms to ISO / IEC 27017 / IEC 27001 and ISO / IEC 27701 security standards. The platform can support millions of infrastructure devices and hundreds of millions of clients. The software-centric architecture is cloud-hosting agnostic. It is available on 21 points of presence (PoPs) worldwide with a choice of IaaS providers Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Extreme Networks adheres to a gold standard approach to data privacy, implementing processes and designing ExtremeCloud IQ to facilitate compliance with US and international data privacy regulations including CCPA/ CPRA, GDPR and other international regulations. The right to be forgotten is one of many data privacy requests that ExtremeCloud IQ can help customers address, including subject access requests, rectification of data requests (etc.). Administrators can search, download, and delete personal data within their network management platform with auto generation of audit logs. For detailed information see the Extreme privacy policy.

ExtremeCloud IQ offers a range of deployment options to provide greater flexibility and facilitate data privacy and residency options: public, private, or ExtremeCloud Edge.

- **Public cloud**: Extreme provides access to a hosted service which removes infrastructure management and costs, and provides data privacy and protection, unmatched reliability, and continuous delivery of innovations.
- **Private cloud**: For businesses that want increased privacy in their own dedicated IaaS environment, Extreme packages our ExtremeCloud applications into a dedicated customer instance in a public cloud. This enables the same benefits as the public cloud plus greater security and control.
- **ExtremeCloud Edge***: For customers or MSPs that want the benefit of a simplified deployment model with the benefits of data residency, privacy, and control, by hosting in a data center of their choice, Extreme provides a scalable platform delivery framework supporting all of Extreme's application portfolio for on-premises deployment.

Deployment type	Public cloud	Private cloud	ExtremeCloud Edge*
Description	SaaS-based delivery of services in a public regional data center (RDC)	Dedicated customer instance in a public cloud	Extreme or customer orchestration of applications in on-premises Universal Compute Platform (UCP)
Deployment options	AWS, Azure, or GCP	AWS, Azure, or GCP	Single or Dual UCP configurations or multi-UCP clusters on MSP or on enterprise premises
Value/differentiator	Simple SaaS delivery model	Data privacy and isolation	Data sovereignty and low latency performance

Table 2: Cloud continuum deployment options

*ExtremeCloud Edge is deployed on the Universal Compute Platform (UCP) to deploy and manage the delivery of applications to the customer premises. See the UCP documentation for details.

Key Components and Capabilities

ExtremeCloud IQ is an adaptable solution that offers a wide range of robust network management capabilities and deployment options. It provides unified, full-stack management of APs, switches, and SD-WAN. The solution provides all the benefits of a SaaS management platform while offering flexible and cost-effective options to transition legacy Extreme, third-party, and IoT devices to cloud-based network management. This flexibility enables organizations to preserve their current investments in Extreme and third-party network devices while allowing them to transition to cloud-based management in a way that works best for them.

The broad set of management capabilities has been described above. This section provides more details regarding each of the applications in the ExtremeCloud IQ suite. It includes three groups of capabilities:

1. Extensive cloud-based visibility, device management, and automation
2. Advanced cloud-based capabilities augmented with features for guest management, a wireless intrusion prevention system (WiPS), and location services with ExtremeCloud IQ Essentials
3. Support for on-premises components of the portfolio that are connected to the cloud: Extreme Tunnel Concentrator, ExtremeCloud IQ Controller, and ExtremeCloud IQ Site Engine

ExtremeCloud IQ Essentials

The Essentials component of ExtremeCloud IQ includes ExtremeGuest, ExtremeLocation, and Extreme AirDefense Essentials. ExtremeGuest is a robust and comprehensive guest engagement solution that enables managers and network operators to use analytical insights for a deeper understanding into how their guest networks are utilized.

For example, knowing how many customers use the guest network, how often they visit, and how much time they spend in the network are all metrics that can be measured through ExtremeGuest. Analytics of social networking behavior of customers can be used to increase patronage and expand brand exposure. Splash pages can be easily updated using a built-in editor and permitted email addresses can be collected for subsequent marketing campaigns.

ExtremeLocation provides enterprises with powerful multitier location services across all sites. Supporting Wi-Fi and BLE technologies, enterprises can monitor workflows and assets, in real time or historically, to improve their overall operations and efficiency. This service provides granular location accuracy resolution to support diverse industry-specific use cases. For example, retailers can track new and repeat visitors, real-world engagement times, and associates' or asset locations, to provide context-based personalized experiences to their customers. Healthcare providers may view real-time dashboards and monitor trends of users and assets, to deliver enhanced patient care.

Extreme AirDefense Essentials simplifies the protection, monitoring, and compliance of wireless LAN networks. It continuously safeguards the network from over the air threats, provides automated remediation, and notifies IT staff when attacks occur. Using existing infrastructure with AirDefense, organizations can protect their air interfaces from unwanted behavior. It is deployed as a set of APs or radios, serving as sensors to monitor the airwaves when combined with AirDefense. Sensors can be configured in radio share or dedicated sensing modes and can also be used as an overlay security network in any environment.

Extreme Tunnel Concentrator

The Extreme Tunnel Concentrator is a high-performance traffic concentrator designed to run locally on the ExtremeCloud Edge platform. Tunnel Concentrator must be linked to ExtremeCloud IQ or ExtremeCloud IQ Controller management applications. It supports Virtual Router Redundancy Protocol (VRRP) to provide redundancy and scalability. Tunnel Concentrator can aggregate network traffic through standards-based Generic Routing Encapsulation (GRE) or Internet Protocol Security (IPsec). It supports up to 5,000 managed APs per instance.

ExtremeCloud IQ Controller

The ExtremeCloud IQ Controller application provides on-premises wireless management and seamless roaming for up to 20,000 APs and high-density deployments of up to 100,000 users. It includes tightly integrated services and features for Network Access Control (NAC), Wi-Fi performance, and location management. The Controller incorporates extensive policy and control features to securely manage users and devices. ExtremeCloud IQ Controller helps to simplify deployment by providing a single point of access for trusted authentication. Flexible topology configurations ranging from a centralized data plane to local and fabric attach provide options to best match the requirements of the enterprise towards user segmentation and point of network access.

The Controller supports a range of use cases in stadiums and arenas, healthcare environments, and educational institutions. Support for management of IoT functions, such as BLE beacons, detection, or transmission is also enabled for use cases of client location or asset tracking. ExtremeCloud IQ Controller helps users understand the detailed performance of Wi-Fi by providing expert views of the RF state. It also includes an integrated location management system. This embedded capability enables location coverage, generates real-time and responsive heat maps, and understands user activities.

ExtremeCloud IQ Site Engine

The Site Engine on-premises management application provides visibility, NAC, analytics, and management for Extreme and third-party devices as well as Fabric. It also enables granular visibility into the performance of applications and the network through telemetry and deep packet inspection (DPI). There are four configurable options available for the data communicated from Site Engine:

- Share statistical data about managed devices and end-system information with ExtremeCloud IQ
- Share statistical data about managed devices with ExtremeCloud IQ
- Use ExtremeCloud IQ as a license proxy only
- Air gap mode, no internet connectivity is required

Many network environments are heterogeneous with devices from multiple vendors. In addition to Extreme devices, ExtremeCloud IQ Site Engine provides management of Cisco and HPE Aruba switches. This includes device discovery, monitoring, configuration, and archive as well as firmware upgrades. It also provides basic setup and monitoring of a large array of devices from Juniper Networks, Dell, Nokia, Allied Telesis, Zyxel, Linksys, Huawei, and more. Since it uses Simple Network Management Protocol (SNMP), it can also monitor IoT devices, such as cameras and sensors. Site Engine extends support to devices that do not have robust SNMP capabilities by utilizing scripts and Telnet/SSH.

ExtremeCloud IQ Site Engine includes three components: device management capabilities, application and end-user monitoring with ExtremeAnalytics, and NAC capabilities with ExtremeControl. The ExtremeAnalytics service uses DPI to provide granular views of applications, users, and devices with an easy-to-understand dashboard inventory and network topology for efficient management. ExtremeAnalytics automatically measures application performance and provides an alert when the Quality of Experience (QoE) of a designated application changes beyond a standard deviation, so administrators are proactively alerted before their end-users complain. The service combines flow-based technology with a rich set of application fingerprint techniques that can identify over 8,000 apps and includes more than 10,000 behavioral detection-based fingerprints. It monitors unusual traffic, so administrators can identify shadow IT, report malicious or unwanted applications, and helps with security compliance.

ExtremeControl is integrated with Site Engine and is available with a separate subscription. Administrators can use it to define granular policies to meet compliance obligations, as well as locate, authenticate, and apply targeted policies to users and devices. When access security in ExtremeControl is enabled, it provides role- based NAC for all devices, including third-party networking devices. The application securely enables guest access, bring your own device (BYOD), and IoT device control. It protects the network and corporate data against external threats by proactively preventing network access by unauthorized users and compromised endpoints.

Fabric Management

Fabric management is natively designed into ExtremeCloud IQ Site Engine to simplify fabric set up and management. Site Engine uses Fabric Topology templates so users can view and configure Shortest Path Bridging (SPB), based Level 2 (L2) and Level 3 (L3) Virtual Services Networks (VSNs), as well as IP-shortcut based VSNs. It can also extend fabric technology functionality to network devices that do not support SPB. Topology maps provide fabric-specific visualizations to help users more easily monitor fabric-related parameters, such as Intermediate System to Intermediate System (IS-IS) areas and Fabric Connect links. This helps users locate where IS-IS areas are present and determine which links are part of the fabric.

Users can visualize primary and secondary paths between any two fabric switches in the network, and where in the network a specific fabric service is present to ascertain its main attributes (such as L2VSN versus L3VSN, or virtual routing and forwarding (VRF) assignment).

The integration of Fabric over ExtremeCloud SD-WAN enables Fabric to be seamlessly extended to remote branches. Site Engine can display tunnels through SD-WAN and report tunnel failure between SD-WAN devices. Users can easily navigate from Site Engine to an SD- WAN appliance, then use the 360 view to investigate and troubleshoot. In addition to the capabilities provided by Site Engine, administrators can also access Site Engine from ExtremeCloud SD-WAN Orchestrator with SSO, as part of unified management.

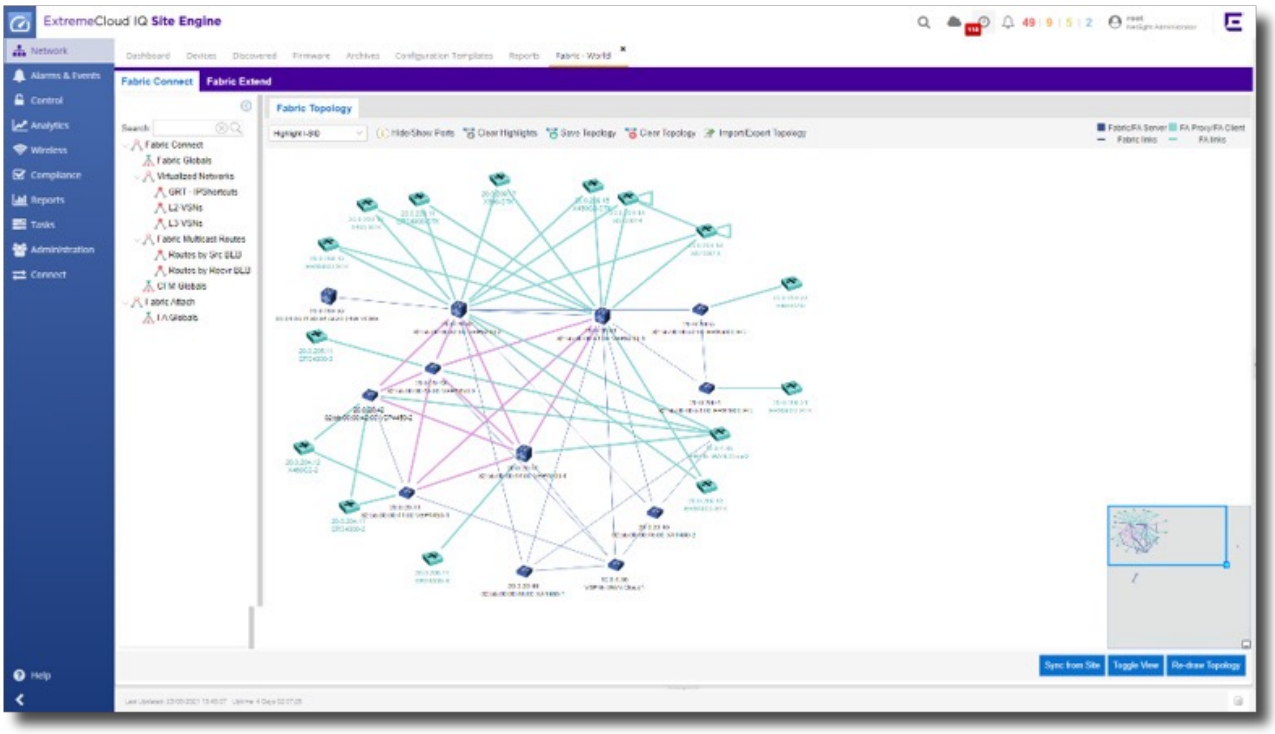


Figure 3: ExtremeCloud IQ Site Engine Topology Map

Universal Licensing

Extreme offers Universal Licensing, so customers only pay for what they need and use, which provides greater cost efficiency and flexibility. ExtremeCloud IQ value-based licensing tiers, Connect, Pilot, and CoPilot, make it easier for organizations to scale their networks and adapt to IT needs. ExtremeCloud IQ obtains access to a common license pool when it is linked to the user's Extreme Portal account. A Universal License can be used with any Extreme Networks or third-party device and upgrading license tiers is simple and seamless.

- **ExtremeCloud IQ Connect** is the base level tier. It provides subscription-free cloud management for up to 10 supported devices, enabling organizations to deploy enterprise-grade connectivity with basic network management.
- **ExtremeCloud IQ Pilot** is the primary license tier for ExtremeCloud IQ. It is designed for organizations that require enhanced policy enforcement, visibility, reporting, and advanced configurations. Pilot enables configuration and management of infrastructure devices at scale, including advanced policy, advanced segmentation, advanced troubleshooting, AI within dynamic packet capture and client monitoring, advanced guest, advanced SSH, and more.
- **ExtremeCloud IQ CoPilot** enables additional practical AI functions that help identify problems before they impact operations. It constantly scans, compares, and computes network data to alert IT administrators and recommend actions to mitigate issues or anomalies before they result in a disruption of service. This simplifies and facilitates troubleshooting and customer resolution so administrators can spend less time fixing the network and more time on essential activities. CoPilot simplifies and facilitates troubleshooting and customer resolution, allowing IT operations teams to become more data-driven and proactive. It features device simulation capabilities with networking's first Digital Twin.

	ExtremeCloud IQ Connect	ExtremeCloud IQ Pilot	ExtremeCloud IQ CoPilot*
Deployment options	**Public**	**Public, Private, and ExtremeCloud Edge**	**Public, Private, and ExtremeCloud Edge**
Feature set	Free management for APs, switches, and routers	Advanced infrastructure management, reporting and remediation tools using AI. Additional management functions for third-party and legacy Extreme devices	**Premium license on top of Pilot** Explainable ML-derived insights and intelligence, algorithmically detected anomalies
Unique features	• Onboarding • Basic configuration • Basic monitoring • Basic troubleshooting • Maximum 10 devices, 2 network policies, and 4 SSIDs	• Onboarding and configuration • Automation workflows and templates • Comprehensive monitoring, including Thread networks • ML Insights: Network 360 Monitor, Client 360, and Network Scorecard • Client Monitor with dynamic PCAP for troubleshooting • NexGen Maps for real-time RF and responsive views • Application visibility • Advanced topology views • Troubleshooting heuristics • Contextualized optimization • Additional automation and security with Site Engine • Role-based profiling • Comparative analytics • Companion mobile app • Support for OpenAPI • Pilot license includes ExtremeCloud IQ Essentials	• AIOps generates insights and recommendations for wired and wireless networks • Connectivity Experience • Anomaly Detection: RF optimization, device performance optimization, and wired/wireless interconnect optimization • Explainable ML for trust • Remediation recommendations • Digital Twin for validated design • Automated GTAC support

Table 3: Summary of ExtremeCloud IQ license tiers

* Only available for cloud-managed Universal devices

Product Specifications

Simplified Deployment

- Customer self-service sign-up
- Guided workflow for network policy deployment
- API-based integration with leading third-party RF planning applications
- Automatic connection to ExtremeCloud IQ for auto provisioning with network policy and firmware updates
- QR and bar code onboarding through the ExtremeCloud IQ Companion mobile app for IoS and Android-based devices
- Companion mobile app supports installation photography/video, augmented reality, validation, and reporting

Centralized Configuration

- Guest access functionality
- Auto-provisioning and automation for onboarding, provisioning, and setup
- Device templates for switches, routers, and APs
- APs and routers act as a RADIUS server or a RADIUS proxy, and as a DHCP server
- Centralized view of all configuration objects
- Bulk edit of device properties
- Ability to schedule firmware upgrades
- Command-line interface (CLI) access to Extreme devices
- Active directory/LDAP
- IPv6 support
- Syslog and SNMP server configuration
- Configuration audit, backup, restore, import, and export

Support for Tunnel Concentrator

- Device classification by location and time zone
- Customer application definition
- Client classification by location, OS type, and MAC address
- Multiple user profiles for each SSID
- Time-based firewall and QoS policy
- Application, network, and MAC layer firewall policy rules
- WIPS policy for rogue AP detection and mitigation

Security and Privacy

- ExtremeCloud IQ cloud platform conforms to ISO/ IEC 27017 and is certified by DQS to ISO/IEC 27001 and ISO/IEC 27701 by the International Standards Organization (ISO)
- Simple deletion tools of personal data with audit reports to facilitate data privacy compliance
- Role-based access control
- No customer data traverses the ExtremeCloud network
- Restricts traffic to enterprise data
- SSO for ExtremeCloud IQ through SAML
- Optional multifactor authentication with Google Authenticator for administrators
- Compliance with California Consumer Privacy Act (CPRA) and California Privacy Rights Act (CPRA)
- EU General Data Protection Regulation (GDPR) features including:
  - Search for, download, and delete personal data for specific users
  - Creation of reports to document the above actions

Dashboard

- Time range slider on dashboard for historical view
- 360° views of Extreme network policies, APs, client devices, users, and apps
- Global search function by network policy, MAC address, serial number, user, host name, or application name
- Enhanced data retention for monitoring and reporting usage
- Interactive Network Summary Report with easy sharing
- Savable contextual filters by location, SSID, policy, user, profile, and client OS type

Guest Access

- Onboarding and management of visitor and employee personal devices (BYOD)
- Multiple onboarding workflows though a captive web portal (CWP)
- Private PSK (PPSK), Enhanced Open (OWE), and PSK authentication
- Supports third-party and customized CWPs and cloud-based hotspot applications

Troubleshooting

- Client 360° behavioral analysis, real-time and historical network performance monitoring and optimization
- Dynamic packet capture (PCAP) triggered by live events
- Historical troubleshooting with automatic issue detection
- Anomaly detection supported with CoPilot
  - Mark issue resolved or escalate issue with email notification
  - Built-in CLI and remote SSH
  - RADIUS test
  - AP technical data download
  - VLAN probe tool for simplified troubleshooting of the wired network
  - Optional packet capture analysis with partner solution (CloudShark) or local download

Monitor

- WIPS history report
- Next Gen Maps for real-time RF and responsive views
- Real-time insights into the health and topology of Thread networks
- Drill-down capability from client list to client 360° view
- Device list with rich utilities for advanced configuration and investigation
- Real-time client list with SNR, RSSI, data usage, and connection status
- Savable and reusable filters shared across dashboard and monitor
- Alerts and event lists with historical and real-time data
- PCI DSS compliant reporting
- Rogue AP and rogue client monitoring
- Google Maps integration and navigation with floorplan upload capability

Supported Languages

- English, German, Spanish, French, Italian, Japanese, Korean, Portuguese, Chinese

Reliability

- Data centers with SOC Type 1 compliance (formally SAS 70 or SSAE 16), Type 2, and Type 3 compliance
- High availability with disaster recovery and redundancy
- Scheduled backups
- 24x7 monitoring warranty

CoPilot License Tier Specifications

Management

- Self-service trial sign-up
- Zero configuration setup
- Automatic license assignment
- Flexible license reassignment
- CoPilot license filters
- Proactive license expiration notifications
- Digital twin

Dashboard

- Streamlined user experience for reduced MTTR
- Global filters for quick data retrieval
- Summary widgets for account-level review of CoPilot status
- Table view for rapid data perusal
- Anomaly trends for historical data analysis

ML Capabilities

- Automatic anomaly detection
- ML-enabled data correlation
- Root cause analysis
- Intelligent recommendations with Explainable ML
- Dynamic baselining
- QI computation

Wireless Anomalies

- Wi-Fi capacity
- Wi-Fi efficiency
- DFS recurrence
- Port efficiency
- PoE stability
- Adverse traffic patterns
- Wireless device health monitoring
- VLAN mismatch

Wired Anomalies

- Port efficiency
- PoE stability
- Adverse traffic patterns
- VLAN mismatch

Connectivity Experience

- Wireless connectivity experience
- Wired connectivity experience

Security and Operation

- Accounts are password-protected and accessed through secure SSL
- Management traffic is encrypted and restricted using HTTPS and industry-proven CAPWAP protocol protected by Datagram Transport Layer Security (DTLS)
- Out-of-band operation ensures no customer data traverses Extreme's cloud services
- Single sign-on (SSO) to ExtremeCloud IQ
- Multifactor authentication with Google Authenticator for administrator accounts
- Centralized monitoring and management
- Integrated role-based access control (RBAC) to delegate select ExtremeCloud IQ roles and permissions to different administrators
- Value-added reseller (VAR) and partner management capabilities, including account provisioning and maintenance
- ExtremeCloud IQ connectivity does not impact network operations servicing users

Ordering Information

Category	Model number	Model description
ExtremeCloud™ IQ subscriptions		
ExtremeCloud IQ Pilot subscription	XIQ-PIL-S-C-EW	ExtremeCloud IQ Pilot SaaS subscription and ExtremeWorks (EW) SaaS support for one (1) device (1 year)
ExtremeCloud IQ Pilot subscription	XIQ-PIL-S-C-PWP	ExtremeCloud IQ Pilot SaaS subscription and PartnerWorks Plus (PWP) SaaS support for one (1) device (1 year)
ExtremeCloud IQ Navigator subscription	XIQ-NAV-S-C-EW	ExtremeCloud IQ Navigator SaaS subscription and EW SaaS support for one (1) device (1 year)
ExtremeCloud IQ Navigator subscription	XIQ-NAV-S-C-PWP	ExtremeCloud IQ Navigator SaaS subscription and PWP SaaS support for one (1) device (1 year)
ExtremeCloud IQ AIOps subscriptions		
ExtremeCloud IQ CoPilot subscription	XIQ-COPILOT-S-C-EW	ExtremeCloud IQ CoPilot SaaS subscription and EW SaaS support per device, per year (requires active XIQ Pilot SaaS subscription)
ExtremeCloud IQ CoPilot subscription	XIQ-COPILOT-S-C-PWP	ExtremeCloud IQ CoPilot SaaS subscription and PWP SaaS support per device, per year (requires active XIQ Pilot SaaS subscription)
ExtremeCloud IQ Cloud ops	XIQ-CLOUDOPS-S-EW	Subscription for on-premises cloud ops software management of distributed cloud installations is available with ExtremeCloud Edge only. 1 year, min. 3 years. For deployments with a minimum of 1,000 and up to 10,000 managed devices.

Service and Support

Extreme Networks provides comprehensive service offerings that range from professional services to design, deploy, and optimize customer networks, and customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme Networks account executive for more information about Extreme Networks service and support.

Additional Information

For additional technical information on ExtremeCloud IQ, please visit extremenetworks.com/extremecloud-IQ.

Extreme networks

http://www.extremenetworks.com/contact