At-a-Glance

Unify Management with Multivendor Device Support

ExtremeCloud™ IQ Site Engine Makes the Transition to Cloud-Based Management Easy

Most networks are heterogeneous, and devices from different vendors need to be managed in a consistent manner. A unified solution is required to reduce the complexity involved when depending on multiple management tools. The solutions should also allow a variety of deployment options to facilitate the transition to cloud-based network management as well as compliance and data privacy requirements.

ExtremeCloud™ IQ is designed to streamline lifecycle management of third-party and Extreme Networks devices from deployment to maintenance. In addition to Extreme devices, ExtremeCloud IQ Site Engine manages Cisco and HPE Aruba switches, easing the transition to cloud-based management, and it provides basic set up and monitoring of a large array of devices from Juniper Networks, Dell, Nokia, Allied Telesys, Zyxel, Linksys, Huawei devices, and more. ExtremeCloud IQ Site Engine delivers the following benefits:

Efficient Management

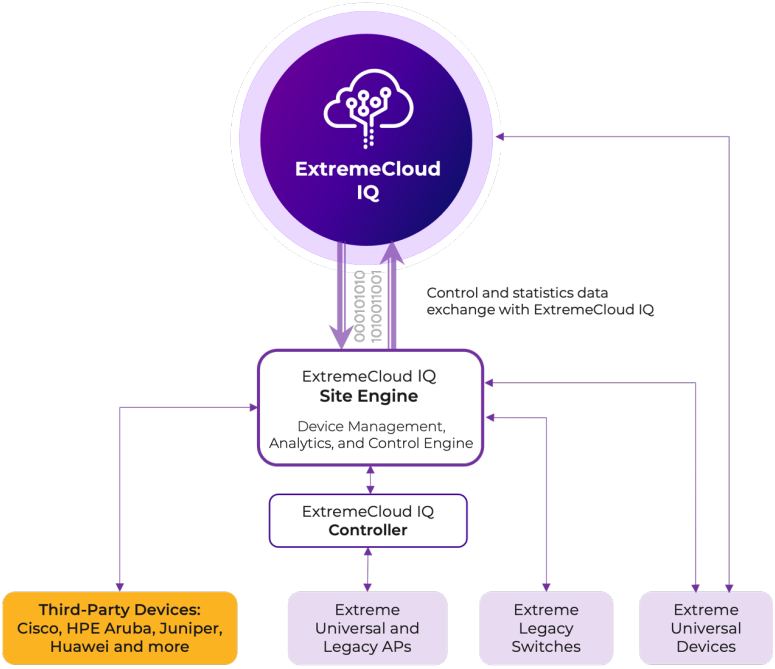
- Unifies management of Universal, legacy, and multivendor devices
- Expedites root cause analysis and troubleshooting
- Enables a transition path to cloud-based network management

Enhanced Security and Flexibility

- Role-based access security
- Flexible deployment options to address security and compliance requirements: on-premises, air gap, and hybrid modes

Automated Daily Activities

- Intuitive task automation and built-in workflow tools
- Scripting language support



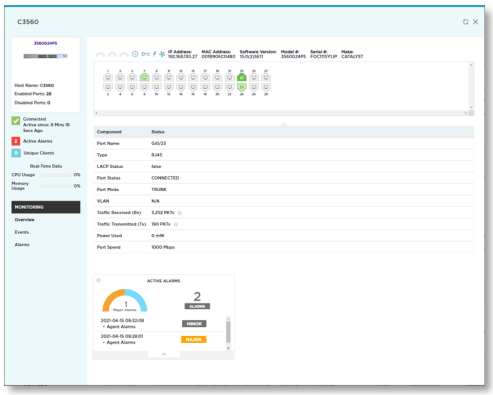
How Benefits Are Delivered

The ExtremeCloud IQ network management solution includes cloud-based and cloud-linked on-premises deployment options. The ExtremeCloud IQ Site Engine component uses SNMP and CLI to provide management of third-party devices and it extends support to devices that do not have robust SNMP capabilities by utilizing scripts and Telnet/SSH. Site Engine also enables a migration path for third-party and legacy networking devices by allowing deployment in a local, cloud-linked, on-premises mode with the ability to transition to cloud-based network management when and how an IT organization chooses.

ExtremeCloud IQ Controller is another component of the ExtremeCloud IQ solution that works in conjunction with Site Engine. It delivers simplified management and tightly integrated services for on-premises deployments of legacy access points (APs). The ExtremeCloud IQ solution allows administrators to control the data forwarded from Site Engine to ExtremeCloud IQ to support compliance, security, and data privacy requirements. (Details regarding the statistics communicated are documented here.)

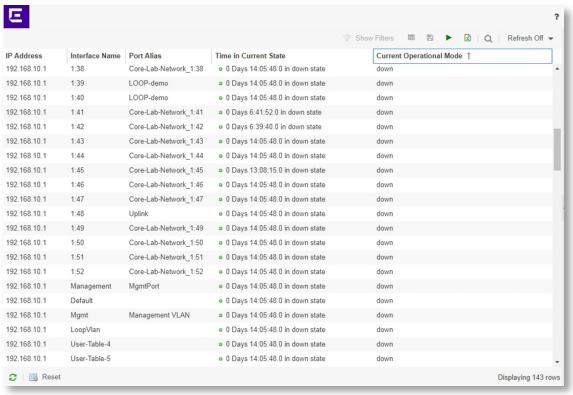
Site Engine also includes the ExtremeAnalytics and ExtremeControl capabilities and supports the following benefits for multivendor support:

Efficient Management



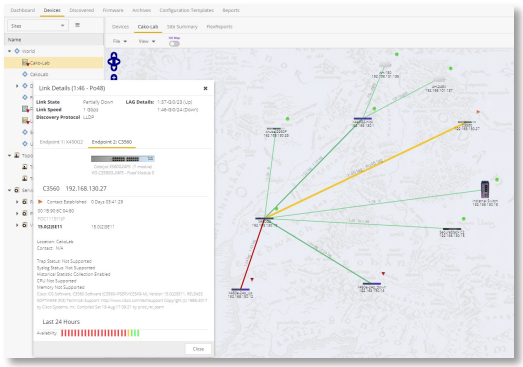
Device View:

A user can quickly determine the device status and device properties such as serial number, model type, MAC address, and port status. Status reports include analysis and troubleshooting information for wired and wireless devices.



Troubleshooting with FlexViews:

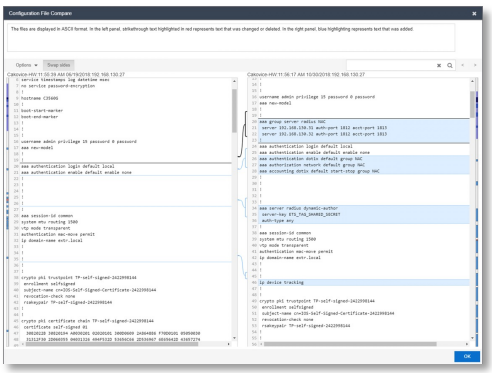
Provides insights into device status and enables powerful sorting and troubleshooting. Views can be customized to show information that is needed most often.



Device Monitoring:

Map links can be created by users or automatically discovered based on LLDP, SONMP, NDP, CDP (Cabletron Discovery Protocol), and EDP.

- Syslog events and SNMP traps/informs generated by the devices and actions initiated by the network administrator
- Events can trigger alarms and automation actions



Inventory Management:

Includes configuration backup/restore, comparison of configuration files, and firmware upgrades.

Enhanced Security and Deployment Flexibility

Access Control

Site Engine allows administrators to unify the security of wired and wireless networks with in-depth visibility and control over users, devices, and applications. It delivers granular policy controls that enable administrators to address compliance obligations including heterogeneous endpoint environments. Locate, authenticate, and apply targeted policies to end users and devices, since they can easily onboard through a single integrated user interface.

The following features are supported out-of-the-box:

- Multi-domain authentication and multi-method authentication
- Voice end-system devices are assigned a voice domain. Data end-system devices are assigned a data domain. Both data and voice end-systems can be on the same port.
- Some end-system devices do not support an IEEE 802.1X, while on other end-systems such as printers, cameras and IoT sensors, it is difficult to configure. For this reason, ExtremeControl supports multi-method authentications running concurrently.
- VLAN assignment (RFC 3580)
- ExtremeControl can send radius attributes to devices, including custom and standard VSA. Authorization of the end system to VLAN is the most standard approach.
- CoA, Deauth (RFC 5176/RFC 3576)
- Different devices require different reauthentication specifics. ExtremeControl is very flexible and supports many different options to reauthenticate/deauthenticate an end system from the network.

Deployment Flexibility

The ExtremeCloud IQ Site Engine component of ExtremeCloud IQ is deployed on premises. Site Engine features a secure cloud-linked mode of operation to facilitate cloud-based network management of third-party and Extreme Networks devices. Users can configure what data are shared with ExtremeCloud IQ, so customers with special requirements can determine the right balance. It can also be deployed in air gap mode for adherence to industry and regional data privacy and compliance requirements.

Automating Daily Tasks

Automation and Provisioning:

Workflows and scripts are defined through the CLI of the managed device. The settings in ExtremeCloud IQ Site Engine and non-Extreme devices can be set through the ExtremeCloud IQ Site Engine API. Site Engine support for common scripting languages, such as Python, provides the ability to create the sequential execution of tasks. Workflows and scripts can be started by user action or through triggers such as alarms, events, Syslog messages, and SNMP traps.

Dynamic ACL:

Some multivendor devices support dynamic assignment of predefined access control lists (ACLs) and other devices support downloadable ACLs. The ExtremeControl capability can dynamically translate Extreme policy definitions to downloadable ACLs supported by many Cisco and HPE Aruba devices.

The ExtremeCloud IQ solution is a subscription-based offering, so IT organizations can realize decreased overall cost of ownership and reduce the time-to-benefit. It provides the benefits of SaaS network management in addition to the ease of managing Extreme and multivendor devices.