Data Sheet

# ExtremeControl

## Highlights

### Access Security

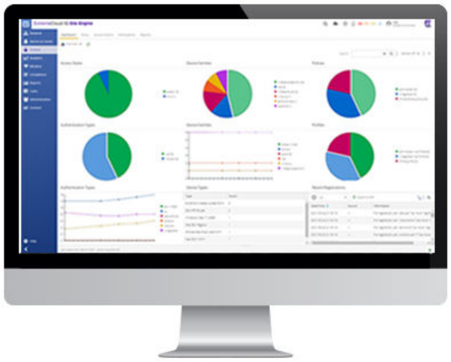
- Role-based network access control for all devices including third party networking devices
- Secure guest access and BYOD onboarding
- Integration with third party solutions such as NGFW, SIEM, CMDB, internet security and EMM/MDM
- Secure IoT network access

### Operational Efficiency

- Automatic performance alerting
- Single screen for management, policies, access control, and application analytics
- Accelerated troubleshooting via separation of network from application issues

### Business Aligned

- Context-driven, consistent policies from edge to data center
- Network access prevention for unauthorized users and compromised endpoints
- Securely enabled critical initiatives such as BYOD and IoT



## Keep the network edge secure with end-point security.

### ExtremeControl for ExtremeCloud IQ - Site Engine

With most data breaches starting at endpoints, granular control is needed over users and IoT devices and consistent policies across the entire network into multicloud. With ExtremeControl™, an application available as part of ExtremeCloud™ IQ – Site Engine[1],users have centralized in-depth visibility and control over all endpoints across their network through one simple, flexible, and easy to consume dashboard.

ExtremeControl securely enables BYOD and IoT to protect the network against external threats. It provides central management and the ability to define granular policies to meet compliance obligations, locate, authenticate, and apply targeted policies to users and devices.

ExtremeControl is integrated with major enterprise platforms including solutions for network security, enterprise mobility management, analytics, cloud, and data center. In addition, it offers an open northbound API for customized integrations to key enterprise platforms.

[1] ExtremeCloud IQ – Site Engine extends Extreme's cloud management solution to third party networking devices and non-cloud native devices. It also provides the flexibility to manage the network in the cloud and/or local (on-premises).

## Granular Policy Control

ExtremeControl enables the application of granular controls over users and endpoints allowed on the network. Users can enable secure BYOD, guest access, and IoT by rolling out real-time policies based on the security posture of devices.

ExtremeControl matches endpoints with attributes such as user, time, location, vulnerability, or access type to create an all-encompassing contextual identity. Role-based identities follow a user, regardless of where or howthey connect to the network. They can be used to enforce highly secure access policies to prevent unauthorized users and compromised endpoints from accessing the network.

Administrators can centrally manage security access profiles which may encompass a combination of VLAN, Service Identifier (L2VSNs / L3VSNs), L2-L7 ACL, and L2-L7 QoS rules as they pertain to the type of network, fabric, or non-fabric. ExtremeControl also permits the automatic distribution of security access profiles to network devices and Wi-Fi controllers, as well as converts security access profiles to downloadable Access Control Lists (dACLs) for installation on switches and routers. In addition, security access profiles can be assigned to a network device port or dynamically based on user or device authentication as downloadable or dynamic ACLs.

## Advanced Reporting

ExtremeControl makes it easy to monitor issues on the network — all on one simple-to-read dashboard. It sends advanced, customizable reports and alerts about the authentication, guest access, onboarding, device profiles and authentication, as well as end- system health. When rolling out large projects, reduce risk by testing new policies and using passive policies for what-if scenarios prior to enforcement. ExtremeControl identifies threats by profiling and tracking users and devices, as well as monitoring the health and compliance of devices before and after access. ExtremeControl can also accommodate policy audits provided by third party integrated MDM/EMM solutions to either ensure defined policies are working or to enforce those policies. It can also provide hit reports and the status regarding the number of non-compliant and/or decommissioned devices that have restricted network access with additional context regarding where, when, and how. ExtremeControl enables compliance auditors and security teams with the relevant data they need to make informed decisions regarding their network access policies.

## Ecosystem Integration

ExtremeControl is integrated with Extreme Networks' ecosystem of partners to expand network security and threat response. For example, ExtremeControl is integrated with next-generation firewall solutions and can orchestrate endpoint isolation and remediation based on the alerts received. It shares contextual information such as users, IP address, and location for powerful policy enforcement at perimeter firewalls. Policies based on ID-IP mapping follow users. ExtremeControl also offers third-party policy support, via user-based ACLs, ensuring granular control of the entire network. To prevent the accessing of a client's network from non-compliant and un-enrolled devices the integration with existing EMM/MDM partners, such as VMware Workspace ONE UEM (Airwatch), Citrix, and MobileIron is simplified.

# Specifications

### Virtual Appliance Options

The ExtremeControl for ExtremeCloud IQ – Site Engine can alsobe installed as a virtual appliance that customers can download at purchase. The ExtremeControl virtual engines must be deployed on a VMWare or Hyper-V server.

- The VMWare Management Center virtual engines are packaged in the .OVA file format (defined by VMware).
- The Hyper-V Management Center virtual engines are packaged in the .ZIP file format.

Refer to the ReleaseNotes for information on Virtual Appliance scalability.

# ExtremeControl Supported End-System Browsers

The following lists the supported desktop and mobile end-system browsers connecting to the network through the Mobile Captive Portal of ExtremeControl.

### Desktop

- Microsoft Edge: 41 and later
- Microsoft Internet Explorer: 11 and later
- Mozilla Firefox: 34 and later
- Google Chrome: 33.0 and later

### Mobile

- Internet Explorer Mobile: 11 and later (Windows Phone)
- Microsoft Edge: All Versions
- Microsoft Windows 10 Touch Screen Native (Surface Table): N/A
- iOS Native: 9 and later
- Android Chrome: 4.0 and later
- Android Native: 4.4 and later
- Dolphin: All Versions
- Opera: All Versions

## Ordering Information

| Model Number | Model Description |
|---|---|
| NAC Subscription Enterprise Licenses | |
| XIQ-NAC-S-1K-EW | ExtremeCloud IQ NAC SaaS Subscription and ExtremeWorks SaaS Support for 1K end-systems (one year) |
| XIQ-NAC-S-10K-EW | ExtremeCloud IQ NAC SaaS Subscription and ExtremeWorks SaaS Support for 10K end-systems (one year) |
| XIQ-NAC-S-100K-EW | ExtremeCloud IQ NAC SaaS Subscription and ExtremeWorks SaaS Support for 100K end-systems (one year) |
| XIQ-NAC-S-1K-PWP | ExtremeCloud IQ NAC SaaS Subscription and PartnerWorks Plus SaaS Support for 1K end-systems (one year) |
| XIQ-NAC-S-10K-PWP | ExtremeCloud IQ NAC SaaS Subscription and PartnerWorks Plus SaaS Support for 10K end-systems (one year) |
| XIQ-NAC-S-100K-PWP | ExtremeCloud IQ NAC SaaS Subscription and PartnerWorks Plus SaaS Support for 100K end-systems (one year) |

## Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy, and optimize customer networks, to customized technical training, to service and support tailored to individual customer needs. Contact your Extreme Networks account executive for more information about Extreme Networks Service and Support.