WHITE PAPER

ExtremeCloud™ Platform: Cloud Architecture & Security Overview

This document is intended to be used as a general reference guide to Extreme Networks' cloud architecture and security policies. It is updated infrequently and should not be relied on as a development guide. All statements made, including representations about certifications, are current as of the date of publication. For more up to date information, please visit extremenetworks.com.

Extreme networks

Product Overview

Extreme Networks ExtremeCloud IQ is a globally distributed, cloud-based, network management solution offered as software-as-a-service (SaaS) and sold as a subscription through Value-Added Resellers (VARS) and managed service providers (MSPs) around the world. It is one of several applications in the Extreme portfolio that operates on Extreme's cloud services architecture. The platform was built with security in mind, 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 also has SOC 2 compliance certification to protect customer data from unauthorized access, security incidents, and other vulnerabilities. The software-centric architecture is cloud-hosting agnostic. It is available on points of presence (PoPs) worldwide with a choice of IaaS providers Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

ExtremeCloud IQ can support millions of infrastructure devices and hundreds of millions of clients devices. It facilitates centralized configuration, orchestration, monitoring, reporting, alarms, and AI for all cloud-enabled Extreme Networks devices.

The solution offers a range of deployment options to provide greater flexibility and facilitate data privacy and residency options:

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 innovation.

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 private 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 full control over data residency and security, 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.

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

Table 1: Cloud continuum deployment options

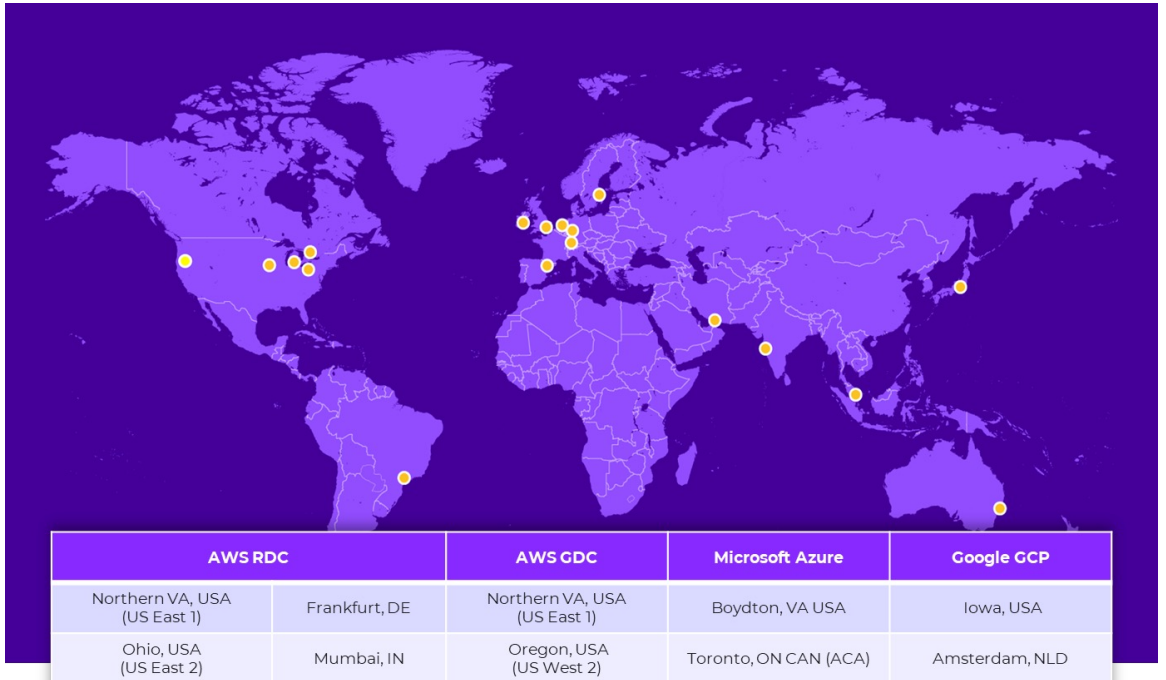
Deployment Type	Public Cloud	Private Cloud	ExtremeCloud Edge
Description	SaaS-based delivery of services in a public Regional Data Center (RDC)	Dedicated customer instance in public cloud	Extreme or customer orchestration of applications in on-prem Universal Compute Platform (UCP)
Product Hosted	ExtremeCloud IQ, ExtremeCloud SD-WAN	ExtremeCloud IQ	ExtremeCloud IQ, ExtremeCloud SD-WAN
Deployment Options	AWS, Azure, or GCP	AWS, Azure, or GCP	UCP configurations on MSP or enterprise
Value / Differentiator	Simple SaaS delivery model	Data privacy and isolation	Data sovereignty and low latency performance

Architecture Overview

Data Centers

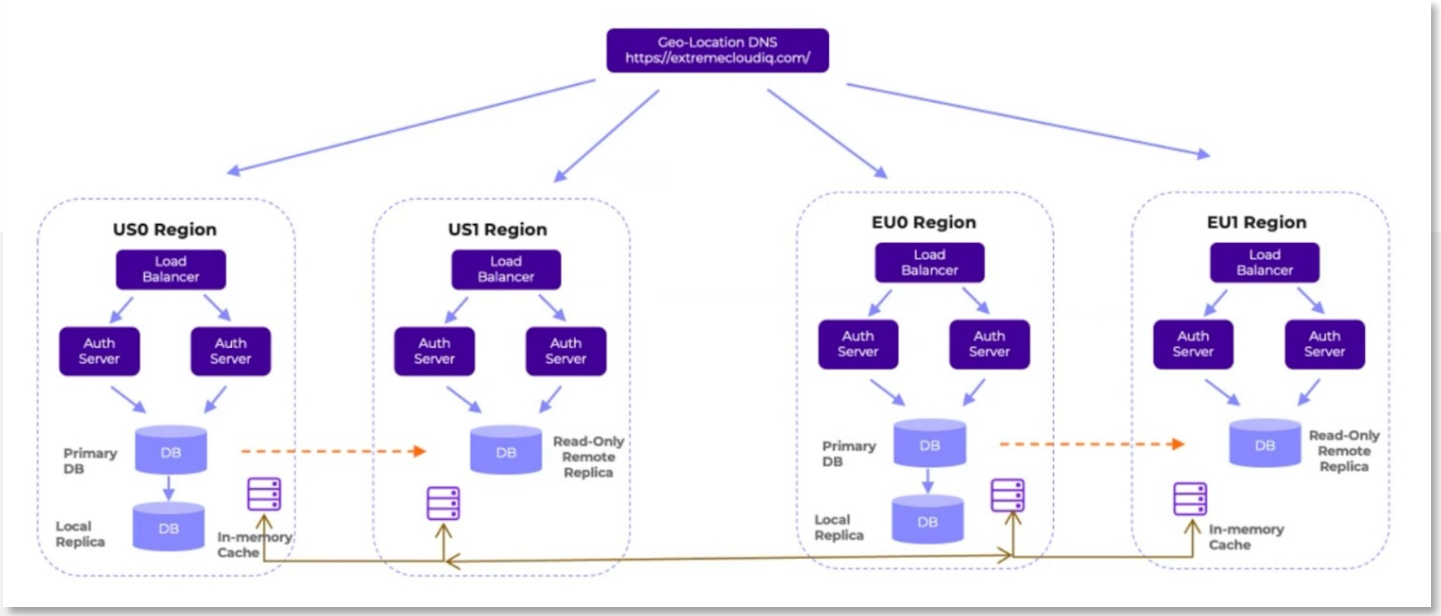
The ExtremeCloud Platform operates in RDCs and global data centers (GDC). An RDC is a geographic instance of the SaaS solution where customer data is hosted. The RDC, or Regional Data Center, is hosted among various cloud providers, which offer different options for data retention time and location. The RDC consists of virtual environments known as a VIQ. Each customer has their own VIQ, which is where all interaction with the product occurs and where customer-owned devices connect. The VIQ exists only on a single RDC, resulting in all customer data being stored within that particular location.

The GDC, or Global Data Center is geographically disbursed and load-balanced between the US and Ireland. US login information exists only on the US instance of the GDC, while EU and other nations exist in the Ireland instance to maintain geographic data protection. The European-based data center performs data replication solely within the EU region and all backups are kept solely within the EU. In addition to serving as the primary authentication mechanism to the ExtremeCloud IQ SaaS platform, the GDC also performs device redirection and other global services as required. All instances of the GDC are hosted within Amazon AWS.



AWS RDC		AWS GDC	Microsoft Azure	Google GCP
Northern VA, USA (US East 1)	Frankfurt, DE	Northern VA, USA (US East 1)	Boydton, VA USA	Iowa, USA
Ohio, USA (US East 2)	Mumbai, IN	Oregon, USA (US West 2)	Toronto, ON CAN (ACA)	Amsterdam, NLD
Dublin, IE	Toyoko, JP	Dublin, IE	Zurick, CH (ACH)	Jurong West, SG (SG-SGP)
Sao Paulo, BR	Sydney, AU	Frankfurt, DE	London, UK (AGB)	
Stockholm, SE	Manama, BH			

Image 1 above shows an overview of our GDC & RDC locations as of the date of this publication. Please see the Cloud Status (extremecloudiq.com) page for current and additional information.



Cloud Usage

The ExtremeCloud Platform scales by taking advantage of the inherent elasticity of the cloud and containerized microservices. New servers and back-end infrastructure can be instantiated as needed based on load, customer, and partner growth and as a consequence of monitoring operations for learned patterns of system performance.

ExtremeCloud IQ is a micro-service driven SaaS application that makes extensive use of container-based solutions hosted within the ExtremeCloud provider environment. These containers are orchestrated in a 100% Kubernetes environment, and are maintained, monitored, and operated continuously by Extreme Networks' Cloud Operations team. It leverages the following cloud providers.

For the purposes of GDPR compliance, these providers can be considered sub-processors:

- Amazon AWS
- Google GCP
- Microsoft Azure

Extreme Networks adheres to a gold standard approach to data privacy, implementing processes and designing ExtremeCloud IQ to facilitate customers' compliance with applicable data privacy regulations. Data subject access requests are among the data privacy issues that ExtremeCloud IQ can help customers address, including deletion requests, access requests, etc. Administrators can search, download, and delete personal data within their network management platform with auto-generation of audit logs.

For additional information on data privacy see the Extreme privacy policy.

API Policy

Extreme makes extensive use of an API driven architecture to provide robust, consistent data directly to our applications and customers. We endeavor to support each API in its native form as long as possible, however, to improve the capability and performance of the API, some may be deprecated. Where an API is to be deprecated, advance notice will be given before the deprecation date. Post-deprecation, the backward compatibility will be maintained to give a sufficient time window for partners and end users to migrate their API dependent applications. The notifications will be sent out as part of the regular feature updates.

Compliance & Certifications

ExtremeCloud IQ utilizes Amazon AWS, Google GCP, and Microsoft Azure as infrastructure providers. These providers feature public statements of SOC 1, 2, 3, PCI, ISO, and other compliance which can be reviewed at the following locations:

- https://aws.amazon.com/compliance/programs/
- https://cloud.google.com/security/compliance/offerings/
- https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home

Extreme Networks reviews vendor capabilities, scale, and SLAs on a regular basis. ExtremeCloud IQ is ISO27001 certified.

See https://cloud. kapostcontent.net/pub/d8b0c577-e7f3-457d-9669-daa3d666df61/iso- 27001-certification-1

ExtremeCloud IQ Security

Data

All network traffic to or from the solution is encrypted in transit and at rest. ExtremeCloud IQ uses CAPWAP and HTTPS protocols which utilize DTLS and TLS respectively for uploading and downloading relevant traffic such as device software image full configurations, captive web portal pages, and certificates. TLS 1.2 and optionally TLS 1.3 are used, with encryption ciphers supported including AES. Network statistics and monitoring data are also sent via CAPWAP using DTLS and/or HTTPS protocol.

All data at rest within ExtremeCloud IQ stored as file or in databases are housed on encrypted storage volumes. AES-256 is used with keys managed via the cloud provider. By default, keys are rotated automatically by the providers on a regular basis, or as configured by the cloud provider managed services. Customers cannot manage encryption keys.

ExtremeCloud IQ provides access to device configuration, management, and network monitoring statistics. Stored data does not include personal data such as social security, driver's license, financial account numbers, or personal medical or insurance information for connected devices and users. Only session-based usage statistics such as IP address, device type, mac address, and other information related to a connected device's experience is collected and reported against. Some of this data, such as IP address and mac address, may be considered personal data. All personal data is treated to the same transmission and storage security as all data and is always encrypted.

No raw TCP/IP session (packet capture) or other data traversing managed network devices (e.g., User A logging into Server B to check banking info via managed wireless APs, switches, and routers) traverses, contacts, or is stored in the ExtremeCloud IQ SaaS Platform.

All customer data is private and remains the property of the customer and can be deleted at any time.

Data and PII Available in ExtremeCloud IQ

Below is a table of all data collected by ExtremeCloud IQ:

Provider	End User Personal Data Visibility Details
Infrastructure Provider (AWS, Google, Azure)	Cloud infrastructure providers are not authorized to access/view data in ExtremeCloud IQ. All access is isolated to private instances only accessible via Extreme Networks assets and by a limited set of Extreme Networks employees.
Customer Support Provider (Extreme GTAC)	**No data is accessible to GTAC unless shared by customer**
DevOps/Development (Extreme Engineering)	**Access to list of customers (MSP, Customers) who purchased ExtremeCloud**
End user device-specific data	• MAC address • Device manufacturer (Apple, Samsung, Intel, etc...) • Last assigned IPv4 and IPv6 address • Hostname • Radio attributes and capabilities • Location (Wi-Fi Ap to which the device is associated)
End user "Where in the network" data	• Last time user was seen on the network • Last AP connected • Network VLAN assigned • Historical roaming history (where have you been at X time) • Last specific network/SSID connected
End user "which network location" data	• Geographic location where user was last seen • Specific "site: where user was last seen
End device network usage data	• Wireless statistics and summary events over time • Error rates over time • Last radio channel, band and RSS reported for user's device • Applications used by the device/user
User specific data (non captive portal)	• If using 802.1x, logged in user name • If using PPSK, PPSK user name or email address • Email address
User specific data (guest captive portal/social login)	• Telephone number (if submitted and required, for PPSK authentication) • Email address (if submitted and required, for PPSK authentication)
Administrator date (used to create cloud administrators)	• Admin first and last name • Admin email address • Admin city, state, country • Company name • Company business vertical (retail, education, etc) • Admin phone number • Vendors- Vendors have no access to data

Appendix

Data Category	Types of Potential Personal Information Collected	Personal Information Source	Extreme Uses for Personal Information
Administrators (information we collect about you, the Customer)	• Login Name (email address) • First and Last Name • Display Name • Phone Number • Job Title • Admin Alternate Email Address • Time Zone • Locale • Country • Street Address • City • State / Province • Postal Code / ZIP Code • User ID • MAC address • IP address	Information entered by Administrator when creating the account	ExtremeCloud IQ account support, allow administrators to access.
Wireless Clients	• Client Host Name • Client MAC Address • Client IP Address • Client IPV6 Address • Client OS Name • User Name • User Profile Name • Email and/or SMS phone number (where PPSK (private pre-shared key) is enabled by customer for registration portal)	Access Points, Branch routers with built-in wireless	(1) Provide wireless services to the Wireless Client. (2) Provide Analytics data to ExtremeCloud IQ Customer.
Wired Clients	• Client Host Name • Client MAC Address • Client IP Address • Client IPV6 Address • Client OS Name	Switches, Access Points, Branch routers.	(1) Provide wired services to the Wireless Client. (2) Provide analytics data to ExtremeCloud IQ Customer.
Social Login Clients (in addition to Wireless Client)	• Client MAC • AP MAC • SSID • ID Provider (e.g., Google, Facebook, or LinkedIn) • Email address	Access Points, Branch routers with built-in wireless, and Cloud Captive Web Portal	Support social login
Passerby Client	• Client MAC Address	Access Points, Branch routers with built-in wireless	Support Analytics data of passerby traffic to respective ExtremeCloud IQ Customers
ExtremeGuest (if enabled)	• End user name/email address (if customer chooses to implement) • End user mobile number (if customer chooses to implement) • Client MAC • Client IP address	If customer opts-in to collecting end user name/email address and/or mobile number, these will be provided by end user	Provide customer guest network usage information SMS notifications to guest user of secure credentials and reporting on such access
ExtremeLocation (if enabled)	• Client MAC • Client IP address • Geolocation	Access Points, Branch routers with built-in wireless	Provide location of users on customer network
ExtremeAirDefense (if enabled)	• Client MAC • Client IP address	Access Points, Branch routers with built-in wireless	Monitor networks for security threats
ExtremeIoT (if enabled)	• Client MAC • Client IP address	Access Points, Branch routers with built-in wireless	Protect wired IoT devices

Logical and Physical Security

ExtremeCloud IQ Cloud Operations proactively manages firewall and networking security policies for the services hosted. Extreme utilizes current industry best practices regarding security and access procedures to limit logical and physical access and permissions to these systems. All access to physical data centers in which ExtremeCloud IQ is hosted are not accessible by Extreme Networks employees for any reason. All access to Extreme Networks' owned facilities and properties is via continuously monitored and locked access, including security cameras. All use of Extreme Networks' network services are monitored.

Logical Access

Third-party cloud providers, sub-processors, and contractors do not possess logical access to the platform. All access to the platform by cloud operations staff is via multi-factor authentication of vetted and authorized individuals with a need-to-know, and all access is logged and strictly controlled from authorized bastion hosts using encrypted communications.

Extreme's Cloud Development teams are geographically located worldwide using a follow the sun method of support. All Cloud Operations and other integral staff such as product management and developers undergo background checks and screenings prior to hire.

All access to the cloud infrastructure and any customer data created by the cloud services is accessed via VPN and multi-factor authentication. Servers in North Carolina and New Hampshire data centers are intended to be used as bastion hosts for the Cloud Operations team and QA/Engineering for access to the cloud infrastructure. These systems are logged, secured, and maintained in accordance with Extreme's Business Continuity Plan and as part of the ISO 27001 ISMS.

Software Upgrades and QA.

Extreme Networks performs all maintenance and updates on a regular basis to the cloud platform. All updates are tested, and QA processed prior to release, and are tested in production once released. At all times, customers control and decide when to upgrade their Extreme Networks hardware devices (access points, switches, routers) as the operating system on these devices is disparate and not dictated by the cloud platform.

Malicious and Vulnerable Code

All code written for the cloud platform undergoes daily malicious code and code vulnerability scanning using automated test systems. All existing code and newly developed patches and features are all subject to this analysis. The results of those tests are acted on by our internal development teams and are not publicly disclosed, nor do we disclose any test results to external or internal customers.

System Hardening

All systems used in the cloud infrastructure are hardened according to Center of Internet Security (CIS) benchmarks and leverage a modified tuned and specific secured operating system environment developed by ExtremeCloud Operations. Separate environments are maintained for Development, User-Acceptance, and Production.

Third Party Software Patches

Third-party patches are applied into Extreme's systems following the same Change Control Policy as production cloud releases. Major version upgrades of third-party software are planned as part of main development cycles, implying a longer duration testing cycle and gained stability for intermediate software releases.

User Roles and Policies

ExtremeCloud IQ provides administrative options to manage user roles and levels of permissions for end-users. A customer will have a single "super user" account with ability to create additional administrators and users with granular permissions to various application functions.

Customers having accounts managed by an Extreme partner (an integrator or managed service provider) will be able to restrict/grant access to their parent partner (i.e., for preventing partner staff from monitoring or configuring their system, or alternatively granting them access for partner maintenance). Partners can disable a customer account (e.g., for non-paying or terminated customers).

Account Provisioning

New accounts are provisioned when a customer registers at https://extremecloudiq.com The account will be registered with admin permissions and can create other users within the account realm. Extreme's Cloud Operations have potential logical access to the system for troubleshooting purposes.

Password Policies (Resets, Storage)

No passwords are stored in clear text. Users can utilize the "Forgot Password" option in the login page available at https://extremecloudiq.com to reset passwords.

SSO, Session Timeouts

ExtremeCloud IQ supports SSO using SAML. SAML is not available by default and must be separately requested and configured by Extreme Cloud Operations for the customer. Sessions automatically time out after 30 minutes by default and are configurable by the administrator, and all administrative access is logged to an audit log within the cloud platform

Change Control Policy

ExtremeCloud IQ is an ISO27001-certified platform and employs multi- stage change control process (Continuous Integration/Continuous Delivery) for all architectural changes and software releases and updates. After development, all updates are moved to a staging environment for Quality Assurance production testing, prior to being scheduled for production deployment during pre-scheduled, announced maintenance windows.

Availability

Uptime

The SLA for ExtremeCloud IQ is provided in the ExtremeCloud IQ Service Agreement:

https://extr-p-001.sitecorecontenthub.cloud/api/public/content/44c02de638bc4fe1a6541fcd1215d70f?v=f00e58e7

Disaster Recovery (DR)

Extreme Cloud IQ's Disaster Recovery Plan includes daily backups for all data within a Regional Data Center and the replication of those backups between geographic regions. Backups are held for 30 days. All replicated backup data is kept within the United States for all US-based data centers, and within Europe for all other data centers to protect data localization concerns.

Availability and System Monitoring

Extreme employs a distributed availability and performance monitoring system on our cloud infrastructure that operates continuously. Anomalies in the behavior and function of the application are monitored and alerts are sent to ExtremeCloud IQ Cloud Operations for immediate action as required. It is important to note that ExtremeCloud IQ is a network management and configuration orchestration platform and is not in the data path of customer data, nor does its operation impact the ability of end users or devices to access the network.

Backup and Storage Strategy

Backups are performed daily by Extreme Networks for the ExtremeCloud IQ environment.

Backups are retained for thirty (30) days and are duplicated. One master copy of the backup is stored within the geographic region for the RDC, and the secondary copy is stored within an alternate RDC within the same geographic region. Backups are tested at least annually in accordance with documented Extreme Networks' disaster recovery testing requirements.

Backups are stored on both local and remote servers in a compressed and encrypted format and inaccessible to users. Only an authenticated administrative-level user can access any backup. Individual case-by-case customer data restoration is not possible, as backups can only be used to restore an entire Regional Data Center (RDC).

However, within the application, an individual backup of customer configuration is permitted. Customers are responsible for performing regular backups of their environment if they anticipate needing to recover a lost object caused by administrative error, accident, or malicious employee actions. Backup of customer VIQ can be performed from the ExtremeCloud IQ GUI easily by any authorized administrator and information on this can be found in the application help documentation or by contacting Extreme Networks technical support (GTAC).

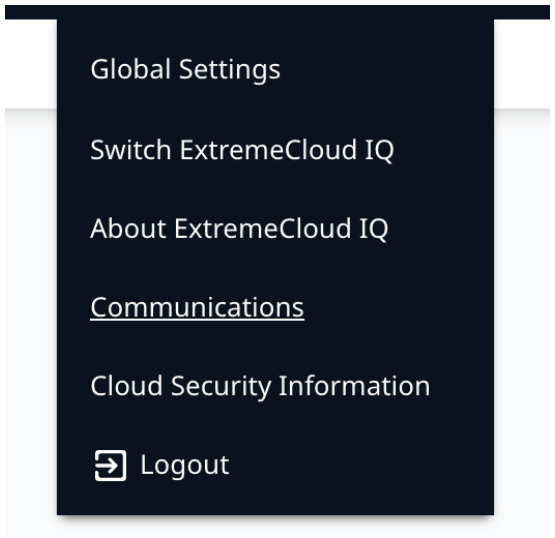
Notification and Support

Technical Support

Support for ExtremeCloud IQ is available 24x7x365 via the support portal. Tickets with GTAC (Global Technical Assistance Center) can be opened via the support portal, and users have access to a full knowledgebase and documentation.

Customer Notifications

Notification to customers for upcoming releases, standard maintenance, and other bulletins are provided via the Notification Tab within Extreme Cloud IQ. To access this, click on the upper-right corner of the screen when logged in, and visit the "Communication" link as shown below.



On rare occasion, ExtremeCloud IQ Cloud Operations may notify you by email for urgent or otherwise important maintenance announcements that may require action on behalf of the customer, in addition to the notification page. We highly recommend that you permit all emails from "communication@extremecloudiq.com" within your SPAM solution and email client to avoid missing important notifications.

For email notifications as indicated above, notification will be generally sent within thirty (30) days in advance of any maintenance or update that will require customer action. A notice will be generally sent seven (7) days prior to the commencement of activity.

Monitoring and Incident Response

Extreme Networks has technical support personnel available 24x7, with additional staff on call for incident escalation responses. If Extreme detects any breach or other major security incident, Extreme's staff will immediately escalate, investigate, and remediate as necessary.

Breach Notifications

In the event of breach and upon determination that customer-specific data has been compromised, Extreme shall notify affected customers per the CloudIQ Privacy Policy.

Shared Responsibility Model

As with any SaaS solution, security of your data is a shared responsibility. Extreme Networks will work with you, as only together can we provide a secure environment.

Extreme Networks' Responsibility

Extreme Networks is responsible for:

- Maintaining operational posture of the ExtremeCloud IQ platform, including
    - Networking and Connectivity
    - Operating systems, containers, and container management solutions (Kubernetes)
    - Storage and data retention
    - Disaster recovery planning, testing, and backups of the solution.
- Maintaining the SLA of ExtremeCloud IQ at or above the published SLA requirements
- Ensuring timely security patches and maintenance for all services and systems that make up ExtremeCloud IQ
- Securing all data at rest and data in transit using industry standard encryption protocols and methods and managing all cryptographic controls within the solution
- Protecting data with architecture and processes to maintain data durability

Customer's Responsibility

- The subscriber (customer) using ExtremeCloud IQ is responsible for:
- Creating and implementing all managed device configurations and individual device security standards used in the customer environment
- Ensuring that configuration and security practices used to configure and secure devices on the customer network meet industry best practices
- Maintaining internet connectivity through proper firewall rules and appropriate bandwidth and latency to guarantee managed device connectivity to ExtremeCloud IQ
- Securing usernames and passwords and other credentials used to access ExtremeCloud IQ to prevent their disclosure to unauthorized persons
- Updating attached network device firmware and applying issued patches for security concerns as recommended by Extreme Networks
- Performing backups of their VIQ environment using tools within the application to assist the customer in recovering from customer administrative error, accident, or malicious employee actions
- Use the solution in a manner consistent with the ExtremeCloud IQ Cloud Terms of Service
- Timely addressing data privacy requests that you receive and addressing any requests that you have with Extreme in an expedient manner