Customer Release Notes

ExtremeCloud IQ Controller

Firmware Version V.10.04.03.0003
April 17, 2023

INTRODUCTION:

The ExtremeCloud IQ Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud IQ Controller includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer (Layer 7), integrated location services, and IoT device onboarding through a single platform. Built on field proven architectures with the latest technology, the embedded operating system supports containerization of applications enabling future expansion of value-added applications for the unified access edge.

The E3120 is a large application appliance meeting the needs of high-density and mission critical deployments with support for up to 20,000 APs/Defenders, 2000 switches, and 100,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

The E2120 is an application appliance meeting the needs of medium sized high-density and mission critical deployments with support for up to 4,000 APs/Defenders, 800 switches and 32,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

The E2122 is an application appliance meeting the needs of medium sized high-density and mission critical deployments with support for up to 4,000 APs/Defenders, 800 switches and 32,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

The E1120 is an entry to mid-level platform expandable to 250 APs/Defenders, 100 switches, and 4,000 mobility sessions in high-availability mode.

The VE6120 is an elastic virtual appliance that supports up to 1,000 APs/Defenders, up to 400 switches and 16,000 mobility sessions in high-availability mode depending on the hosting hardware.

The VE6120 VE6120H and VE6120K offer elastic capacities to cover the full range of offering as VMWare/MS Hyper-V/Linux KVM, ranging from VE6120/VE6120H/VE6120K-Small to VE6120/VE6120H/VE6120K-Large.

The VE6125/VE6125K XL are virtual appliances that support up to 4,000 APs/Defenders, up to 400 switches and 32,000 mobility sessions in high-availability mode, depending on the hosting hardware.

The ExtremeCloud IQ Controller offers the ability to expand capacity to meet any growing business needs. The hardware and virtual packages are available for purchase. The customer purchases adoption capacity as a Right-To-Use Subscription model, supporting flexible quantities (per managed device) and a term (multiple-year extended term) option.

Changes in 10.04.03.0003	
Improved the accuracy in reporting of connected wireless clients on the Dashboard.	CFD-8247
Rectified encapsulation logic for calculation of checksums for tunneled IPv6 traffic that could result in packet discards.	CFD-8665
Adjusted enforcement of path minimum transmit unit (MTU) between Access Points and Controllers to enforce a minimum size of 1024.	CFD-8977
Improved logic for statistics processing (Historian) to protect against edge conditions where no-data events could stall cleanup operations.	CFD-8987
Adjusted logic to only deliver channel neighborhood reports to the controller for APs on which Channel Inspector is explicitly enabled.	CFD-9042

Changes in 10.4.3.0-001R	
Prevented APs from sending unsolicited Neighbor Statistics messages to the controller.	WOS-5098

Changes in 10.04.02.0003	
Corrected configuration handover between ExtremeCloud IQ Controller and access points where the access points rejected an AP Name longer than 32 characters.	CFD-8700
Introduced more intuitive transitioning between different user account Admin roles.	CFD-8681
Improved retention, through upgrades, of the IPv6 'Deny' action for policy rule configuration.	CFD-8565
Corrected an issue with subscription management that may have prevented licensing to automatically up-consume into PILOT capacity when there was insufficient Navigator subscription capacity.	CFD-8684
Corrected the display of a floor map where a portion of a wall would disappear after saving a change.	CFD-8296

Changes in 10.4.2.0-002R	
Addressed an issue with potential lock of secure encapsulation (IPSEC) between AP and controllers.	CFD-6428
Improved handling of different sized keys for Fast Transition (FT).	WOS-4887
Corrected an AP issue with reporting of current operational channel to SmartRF.	CFD-8823
Addressed an issue with potential miscalculation of checksums for multicast frames with variable header options, when COS override was enabled.	CFD-8776

Enhancements in 10.04.01.0017	
Support for Single-Sign-On (SSO) to directly log in to a managed ExtremeCloud IQ Controller from an ExtremeCloud IQ account. The Administrator account in ExtremeCloud IQ provides administrator access to the controller. All other ExtremeCloud IQ account roles provide read-only access to the controller.	XCC-2800
Introduced support for AP5050D-WW Universal and Worldwide 6E capable access points. The AP5050D provides integrated support for a directional sector of 30 (default) or 70 degrees beam-width.	XCC-2730

Enhancements in 10.04.01.0017	
Note: Per current regulatory rules, at this release point, these models operate only for 2.4 and 5 GHz service, and only for outdoor deployments. This model cannot be deployed in an indoor setting. 6GHz (Wi-Fi 6E) radio is disabled at this time. Support for 6 GHz operation (Wi-Fi 6E) will be enabled in a future release.	
Introduced support for AP5050U-WW Universal and Worldwide 6E capable access points. This model provides Omni-pattern support for standard and under-seat installations. Note: Per current regulatory rules, at this release point, these models operate only for 2.4 and 5 GHz service, and only for outdoor deployments. This model cannot be deployed in an indoor setting. 6GHz (Wi-Fi 6E) radio is disabled at this time. Support for 6 GHz operation (Wi-Fi 6E) will be enabled in a future release.	XCC-2729

Changes in 10.04.01.0017	I.D
Hardened the user interface validation mechanism and prevented the entry of invalid characters into the configuration file.	XCC-3104
Fixed an issue where mobile devices were getting stuck on the Registration in Progress screen in a captive portal.	XCC-3052
Improved presentation of the customized captive portal page.	XCC-3051
Improved stability of the VE6125 by increasing the size of database tables and throttling non-critical reporting.	XCC-3025
Increased the size of the needed resource table for proper data flow on the backup controller.	XCC-2792
Addressed a possible stall issue of the RF Manager components for SmartRF.	XCC-2591
Corrected issue with zeroing of the source IP address for Wi-Fi RTLS and/or BLE Beacon listen reports. Controller interface is used as frame source.	CFD-8264

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	V.10.04.03.0003	Maintenance Release	April 17, 2023
Previous Version	V.10.04.02.0003	Maintenance Release	March 8, 2023
Previous Version	V.10.04.01.0017	Feature Release	December 15, 2022

SUPPORTED APPLIANCES, ACCESS POINTS AND SWITCHES:

Product Name	Image
ExtremeCloud IQ Controller VE6120 VMware Min Supported ESXi version 5.1 or later, (tested 7.0)	XIQC-10.04.03.0003-1.dle
ExtremeCloud IQ Controller VE6120H (Windows server 2016 or later)	XIQC-10.04.03.0003-1.spe
ExtremeCloud IQ Controller VE6120K Linux KVM	XIQC-10.04.03.0003-1.dve
ExtremeCloud IQ Controller VE6125 Min Supported ESXi version 5.5 or later, (tested 7.0)	XIQC-10.04.03.0003-1.rse
ExtremeCloud IQ Controller VE6125K Linux KVM	XIQC-10.04.03.0003-1.mfe
ExtremeCloud IQ Controller E1120	XIQC-10.04.03.0003-1.sme
ExtremeCloud IQ Controller E2120	XIQC-10.04.03.0003-1.jse
ExtremeCloud IQ Controller E2122	XIQC-10.04.03.0003-1.wze
ExtremeCloud IQ Controller E3120	XIQC-10.04.03.0003-1.ose
AP302W-CAN AP302W-FCC AP302W-IL AP302W-WR	AP302W-LEAN-10.4.3.0-001R.img
AP305C-1-CAN AP305C-1-FCC AP305C-1-IL AP305C-1-WR AP305C-CAN AP305C-FCC AP305C-IL AP305C-WR AP305CX-CAN AP305CX-FCC AP305CX-IL AP305CX-WR	AP3xxC-LEAN-10.4.3.0-001R.img
AP310e-1-WR AP310e-CAN AP310e-FCC AP310e-IL AP310e-WR AP310i-1-WR AP310i-CAN AP310i-FCC AP310i-IL AP310i-WR	AP3xx-LEAN-10.4.3.0-001R.img
AP360e-CAN AP360e-FCC AP360e-IL AP360e-WR AP360i-CAN AP360i-FCC	AP3xx-LEAN-10.4.3.0-001R.img

Product Name	Image
AP360i-IL AP360i-WR	
AP3912i-FCC AP3912i-ROW	AP391x-10.51.24.0003.img
AP3915e-FCC AP3915e-ROW AP3915i-FCC AP3915i-ROW	AP391x-10.51.24.0003.img
AP3916ic-FCC AP3916ic-ROW	AP391x-10.51.24.0003.img
AP3916-camera	AP3916IC-V1-0-14-1.dlf
AP3917e-FCC AP3917e-ROW AP3917i-FCC AP3917i-ROW AP3917k-FCC AP3917k-ROW	AP391x-10.51.24.0003.img
AP3935e-FCC AP3935e-ROW AP3935i-FCC AP3935i-IL AP3935i-ROW	AP3935-10.51.24.0003.img
AP3965e-FCC AP3965e-ROW AP3965i-FCC AP3965i-ROW	AP3935-10.51.24.0003.img
AP4000-1-WW AP4000-WW	AP4000x-LEAN-10.4.3.0-001R.img
AP4000U-WW	AP4000x-LEAN-10.4.3.0-001R.img
AP410C-1-CAN AP410C-1-FCC AP410C-1-IL AP410C-1-WR AP410C-CAN AP410C-FCC AP410C-IL AP410C-WR	AP4xxC-LEAN-10.4.3.0-001R.img
AP410e-CAN AP410e-FCC AP410e-IL AP410e-WR AP410i-1-FCC AP410i-1-WR AP410i-CAN AP410i-FCC AP410i-IL AP410i-WR	AP4xx-LEAN-10.4.3.0-001R.img

Product Name	Image
AP460C-CAN AP460C-FCC AP460C-IL AP460C-WR AP460S12C-CAN AP460S12C-FCC AP460S12C-IL AP460S12C-WR AP460S6C-CAN AP460S6C-FCC AP460S6C-IL AP460S6C-WR	AP4xxC-LEAN-10.4.3.0-001R.img
AP460e-CAN AP460e-FCC AP460e-IL AP460e-WR AP460i-CAN AP460i-FCC AP460i-IL AP460i-WR	AP4xx-LEAN-10.4.3.0-001R.img
AP5010-WW	AP5xxx-LEAN-10.4.3.0-001R.img
AP5050D-WW	AP5xxx-LEAN-10.4.3.0-001R.img
AP5050U-WW	AP5xxx-LEAN-10.4.3.0-001R.img
AP505i-FCC AP505i-WR	AP5xx-LEAN-10.4.3.0-001R.img
AP510e-FCC AP510e-WR AP510i-1-FCC AP510i-1-WR AP510i-FCC AP510i-WR	AP5xx-LEAN-10.4.3.0-001R.img
AP560h-FCC AP560h-WR AP560i-FCC AP560i-WR	AP5xx-LEAN-10.4.3.0-001R.img
SA201	AP391x-10.51.24.0003.img
APVMAP10i-FCC APVMAP10i-WR	APVMAP10-10.4.2.0-001R.img
Switches	
210-12p-10GE2 210-24p-10GE2 210-48p-10GE2 210-12p-10GE2 POE 210-24p-10GE2 POE 210-48p-10GE2 POE	210-series_V1.02.05.0013.stk fp-connector-3.3.0.4.pyz (cloud connector)
220-12p-10GE2 220-24p-10GE2 220-48p-10GE2	220-series_V1.02.05.0013.stk fp-connector-3.3.0.4.pyz (cloud connector)

Product Name	Image
220-12p-10GE2 POE 220-24p-10GE2 POE 220-48p-10GE2 POE	
X435-24P/T-4S	summitlite_arm-30.7.1.1.xos summitlite_arm-30.5.0.259-cloud_connector-3.4.2.6.xmod
X440G2-12t-10G4 X440G2-24t-10G4 X440G2-48t-10G4 X440G2-12t-10G4 POE X440G2-24t-10G4 POE X440G2-48t-10G4 POE	summitX-30.2.1.8-patch2-5.xos summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector)
X465_24W X465_48T X465_48P X465_48W X465_24MU X465_24MU_24W	onie-30.2.1.8-patch2-5-vpex_controlling_bridge.lst onie-30.2.1.8-cloud_connector-3.4.1.20.xmod
X620-16x	summitX-30.2.1.8-patch2-5.xos summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector)

NETWORK MANAGEMENT SOFTWARE SUPPORT

Network Management	Version
ExtremeControl™	22.3 or higher
ExtremeAnalytics™	22.3 or higher
ExtremeCloud™ A3	4.0
ExtremeCloud™ IQ-Site Engine	22.3 or higher

Air Defense	Version
ExtremeAirDefense™	10.5
ExtremeGuest	**Version**
ExtremeGuest™	6.0.1.0-001

Note:

Platform and AP Configuration functions are not supported by ExtremeManagement™. ExtremeCloud™ IQ Site Engine v21.9 or greater is required.

INSTALLATION INFORMATION:

Appliance Installations	
E1120	[Extreme Campus Controller E1120 Installation Guide](#)
E2120	[Extreme Campus Controller E2120 Installation Guide](#)
E2122	[Extreme Campus Controller E2122 Installation Guide](#)
E3120	[Extreme Campus Controller E3120 Installation Guide](#)
VE6120/VE6125	[Extreme Campus Controller VE6120/VE6125 Installation Guide](#)
VE6120H	[Extreme Campus Controller VE6120H Installation Guide](#)
VE6120K/VE6125K	[Extreme Campus Controller VE6120K/VE6125K Installation Guide](#)

Known Restrictions and Limitations:

Known Restrictions or Limitations	I.D
With 11r enabled on an 802.1x network, a Windows 10 PC with an Intel Wi-Fi card (ax200, ax210), running driver version 22.170.0.3 cannot reconnect automatically after an MU is disconnected. The workaround is to toggle the Wi-Fi off and on from the PC.	WOS-4480
Controller functions, including internal communications and containerized applications, require the usage of reserved address space. Two subnets are reserved internally to the controller: • 172.17.0.0/24 • 172.31.0.16/28 The user interface prevents assigning IP addresses to local interfaces (physical or virtual) that conflict with these ranges.	XCC-3121
Following an upgrade of controller firmware, the Fast-Transition setting may be lost for WPA3-Enterprise networks (resulting in Fast-Transition being disabled). Please check your network settings and re-apply if necessary. This issue will be corrected in a future release.	XCC-3172
AP3900 series requires a minimum firmware revision of 10.41.01 (or later) for onboarding into ExtremeCloud IQ Controller. Customers migrating from ExtremeWireless installations or onboarding new AP3900 inventory to ExtremeCloud IQ Controller must ensure APs are running at least the minimum revision prior to onboarding. Depending on the age of the inventory, this may require a manual upgrade of the unit firmware outside of the management framework.	XCC-3178
Certain wireless clients (such as Qualcomm Killer Wireless 1535 and Intel 7265D/8260/8265) have been known to not complete the 4-way handshake in order to fulfill the association process in networks that have both PMF/MFP (802.11w) and Fast-Transition (802.11r [FT]) enabled. The currently recommended workaround is to not enable PMF/MFP configuration on a service that is also using 802.11r. Such clients have been demonstrated to work correctly on services with just 802.11r (FT) enabled.	nse0003416
For systems previously onboarded into an ExtremeCloud IQ account for visibility, following an upgrade from the previous release (V5) to ExtremeCloud IQ Controller (v10) the controller entry in ExtremeCloud IQ needs to be removed and re-	XCC-2463

F0615-O

Known Restrictions or Limitations	I.D
declared. This will facilitate the re-synchronization of the controller with the account.	
Before installing a new ExtremeCloud IQ Controller license, you must configure Network Time Protocol (NTP) Server settings. Licensing management is dependent on accurate NTP configuration. Configure NTP via the ExtremeCloud IQ Controller initial Configuration Wizard, or go to Admin > System > Network Time to configure and verify the NTP settings.	XCC-2353
For ExtremeCloud IQ Controller configured for authentication of administrators over RADIUS server, the GUI responsiveness may be slow, possibly over 30 seconds if the target server(s) are unavailable or unreachable at login time. If the outage is extensive, the system will eventually timeout to validate against local credentials when provisioned.	XCC-2350
A reboot of the peer ExtremeCloud IQ Controller is required when High Availability is configured for the first time to ensure synchronization of the configuration of ONBOARD attributes, such as device groups. This issue will be addressed in a future release.	XCC-2349
ExtremeCloud IQ-Site Engine 22.3.10 is the minimum required revision for representation of ExtremeCloud IQ Controller 10.01.01 or later revisions. Extreme Management Center (8.5.x or later) does NOT recognize a controller running ExtremeCloud IQ Controller 10.01.01 or later.	XCC-2348
To improve stability of mesh when SmartRF is used with a mesh root AP: * Use fixed channel width. * Set SmartRF sensitivity to "Low" to decrease the time that the AP will abandon the channel for scanning.	XCC-1684
When an infrastructure WLAN (used for connecting client bridge APs) has Quiet IE enable, the client bridge link becomes unstable. It is a best practice to disable Quiet IE when a WLAN is used for a client bridge connection.	XCC-1570
The ADSP spectral analysis function may not work on AP5010x models. This issue will be addressed in a future release.	WOS-4694
The switch primary/backup availability is not supported on the EXOS switches running the 3.4.1.8 Cloud Connector. This affects the deployments where two appliances are configured in an Availability Pair. If the primary appliance is going down, then the EXOS switches will not send statistics to the backup appliance and will be marked in red "Critical" state. When the primary appliance is coming up again, the switches will resume sending statistics information to the primary appliance and the state of the switch will be marked with a green "Running" state.	ECA-455
Allow UTF-8 characters in JSON payload for all Rest API so non-ASCII / Unicode characters are accepted in Rest API requests to comply with current Rest API standards.	ECA-321
MAC-based authentication and WPA3-Compatibility (SAE or WPA2-PSK) and PMF "Required" may not work. This issue will be addressed in a future release.	ECA-1961
For High-Availability installations, on systems configured with RADIUS Accounting or Smart RF enabled, clients (end-systems) may experience a momentary disconnect during the upgrade process (maintenance window). Users immediately reconnect to the available infrastructure, so impact is negligible. For smoother session availability with fast-failover during a failover event, it is recommended to not run these options. This issue is being investigated and will be addressed in a future release.	ECA-1264

F0615-O

Known Restrictions or Limitations	I.D
Upgrade failure will occur when using special characters (escape back slash) in topology.	ECA-466
In SmartRF mode, the AP510 power may temporarily drop to 0dBm and returns to 4dBm.	ECA-469
With on-air-busy channel conditions, it is possible for the ACS not to produce the expected results. In this instance, perform manual channel selection.	ECA-528
Widgets do not show tooltips for lower and upper values. This issue will be addressed in a future release.	ECA-567
Firmware for ExtremeWireless AP3900 series access points does not currently support Smart RF. No Smart RF data is displayed.	ECA-1484
Several old Intel clients (i.e. Intel dual band Wireless AC – 7260) if they are using old drivers are NOT seeing BSSID / SSID advertising 11x capability. This is a client issue (forward compatibility). Other older clients may have this issue. See: [https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html|http://example.com] See KB: [https://gtacknowledge.extremenetworks.com/articles/Solution/AP510-Unable-to-see-the-SSID-on-my-laptop|http://example.com] NB – The client driver update must be done from Intel\drivers' site because the Windows update reports that the client is running the latest driver. If the client driver cannot be controlled (in a BYOD environment), then the AP radios must be configured on a/n/ac (disable ax) until all clients will upgrade to the latest driver.	Info
Default router/gateway should be configured with a next-hop associated with one of the physical interfaces. Pointing the default route to the Admin interface will lead to issues because access points will not get the correct services from the data plane. We recommend setting the default route via data ports, and if necessary, configuring static routes on the Admin port for administration level access.	Info
For AP deployments in remote locations where access points and controllers may need to be discovered and connected over firewalls, a best practice is to leverage DNS or DHCP Option 60/43 methods for zero-touch-provisioning discovery. These methods provide direct connectivity to the defined IP address. DHCP Option 78, which refers to the controller as a Service Location Protocol – Directory Agent (SLP- DA), requires the exchange of SLP protocol between the AP and the appliance at the core, necessitating that UDP 427 be allowed by any firewall in the path. For such installations, discovery over DHCP Option 78 assist is not recommended. When using SLP, for an AP to establish connection with a controller, it must first exchange SLP Directory Agent registration before IPSEC establishment with the eventual controller. That means that SLP UDP 427 must be open along the path. Further issues can occur if Network Address Translation (NAT) is involved. While this method is popular and widely deployed within a homogenous campus, it may result in inadvertent complications for remote connections. Therefore, it should not be used in favor of an alternate method (DHCP 60/43, DNS, or static override).	Info
When configuring system for NTP time assignment, ensure that the NTP server is properly configured. Incorrect time settings (like timestamps far in the future) may adversely affect system operation, such as certificate expiration that may trigger failures in device registration or system instability.	Info nse0003696

Known Restrictions or Limitations	I.D
Appliances in a High-Availability pair must be of the same model and at the same exact software revision (and time synched) for configuration synchronization to propagate to the peer. During the upgrade process of a High-Availability pair, any configuration changes made while only one appliance has been upgraded (and therefore resulting in a version mismatch) will not be propagated until the peer is correspondingly upgraded to the same revision. We recommend that you NOT perform configuration changes to one of the members of a High-Availability pair while the peer has a different software revision.	Info nse0005086
For High-Availability configurations, during upgrade phases or configuration restore operations, wait until the availability link is established and synchronized before attempting to make any new configuration changes. The Availability status will only re-establish to Synched status when both appliances are running the exact same firmware revision. During upgrade periods, the Availability link will only re-establish when both the appliance status of availability link and synchronization status can be found. Go to: · "Network Health" widget on the Dashboard, or · Administration -> System -> Availability	Info ECA-776
Recommendation settings for setup of redundant RADIUS server authentication: · Response Window to 5s [Default: 20s] · Revival Interval to 10s [Default: 60s]	Info ECA-875

SUPPORTED WEB BROWSERS

For ExtremeCloud IQ Controller management GUI, the following Web browsers were tested for interoperability:

- Firefox 81.0
- Google Chrome 86.0

Note: Microsoft IE browser is not supported for UI management.

The Wireless Clients (Captive Portal, AAA):

Browsers	Version	OS
Chrome	108.0	Windows 7 Windows 10 Windows 11
Microsoft Edge	108.0	Windows 10 Windows 11
Firefox	68.0	Windows 10
Safari	Preinstalled with iOS 12.2	iOS 12.2
Safari	Preinstalled with iOS 9.3.5	iOS 9.3.5

PORT LIST

The following list of ports may need to remain open so that the Appliances and APs will function properly on a network that includes protection equipment like a firewall.

ExtremeCloud IQ Controller TCP/UDP Port Assignment Reference

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
			Ports for AP/Appliance Communication				
Appliance	Access Point	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Appliance	Yes
Access Point	Appliance	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Appliance	Yes
Appliance	Access Point	UDP	4500	Any	Secured WASSP	Management Tunnel between AP and Appliance	Optional
Access Point	Appliance	UDP	Any	4500	Secured WASSP	Management Tunnel between AP and Appliance	Optional
Access Point	Appliance	UDP	Any	13907	WASSP	AP Registration to Appliance	Yes
Access Point	Appliance	UDP	Any	67	DHCP Server	If Appliance is DHCP Server for AP	Optional
Access Point	Appliance	UDP	Any	68	DHCP Server	If Appliance is DHCP Server for AP	Optional
Access Point	Appliance	UDP	Any	427	SLP	AP Registration to Appliance	Optional
Appliance	Access Point	TCP/UDP	Any	69	TFTP	AP image transfer	Yes
Access Point	Appliance	TCP/UDP	Any	69	TFTP	AP image transfer	Yes
Appliance	Access Point	TCP/UDP	Any	22	SCP	AP traces	Yes
Any	Access Point	TCP	Any	2002, 2003	RCAPD	AP Real Capture (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	22	SSH	Remote AP login (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	445	Microsoft CIFS	LDAP support	Optional

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
Any	Access Point	TCP/UDP	Any	137, 138, 139	NetBIOS	LDAP support	Optional
Ports for Appliance Management							
Any	Appliance	TCP/UDP	Any	22	SSH	Appliance CLI access	Yes
Any	Appliance	TCP/UDP	Any	5825	HTTPS	Appliance GUI access	Yes
Any	Appliance	TCP/UDP	Any	161	SNMP	Appliance SNMP access	Yes
Any	Appliance	TCP/UDP	Any	162	SNMP Trap	Appliance SNMP access	Yes
Any	Appliance	TCP	Any	80	HTTP	Appliance SNMP access ICP Self Registration	Yes
Any	Appliance	TCP	Any	443	HTTPS	ICP Self Registration	Yes
Any	Appliance	UDP	500	500	IKE	IKE phase 1	Yes
Any	Appliance	TCP/UDP	Any	69	TFTP	TFTP support	Yes
Any	Appliance	UDP	Any	4500	IPSec	IPSec NAT traversal	Yes
Any	Appliance	UDP	Any	13907	Discovery	Used by Discovery	Yes
Any	Appliance	UDP	Any	13910	WASSP	Used by L3 WASSP	Yes
Ports for Inter Controller Mobility[1] and Availability							
Appliance	Appliance	UDP	Any	13911	WASSP	Mobility and Availability Tunnel	Yes
Appliance	Appliance	TCP	Any	427	SLP	SLP Directory	Yes
Appliance	Appliance	TCP	Any	20506	Langley	Remote Langley Secure	Yes
Appliance	Appliance	TCP	Any	60606	Mobility	VN MGR	Yes
Appliance	Appliance	TCP	Any	123	NTP	Availability time sync	Yes
Appliance	DHCP Server	UDP	Any	67	SLP	Asking DHCP Server for SLP DA	Yes

---

[1]For extension of ExtremeWireless deployment via Inter Controller Mobility.

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
DHCP Server	Appliance	UDP	Any	68	SLP	RespoECA from DHCP Server for SLP DA request	Yes
Core Back-End Communication							
Appliance	DNS Server	UDP	Any	53	DNS	If using DNS	Optional
Appliance	Syslog Server	UDP	Any	514	Syslog	If Appliance logs to external syslog server	Optional
Appliance	RADIUS Server	UDP	Any	1812	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Appliance	RADIUS Server	UDP	Any	1813	RADIUS Accounting	If enabled RADIUS accounting	Optional
Appliance	RADIUS server	UDP	Any	1814	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Appliance	RADIUS server	UDP	Any	1815	RADIUS Accounting	If enabled RADIUS Accounting	Optional
Dynamic Auth. Server (NAC)	Appliance	UDP	Any	3799	DAS	Request from DAS client to disconnect a specific client	Optional
Appliance	AeroScout Server	UDP	1144	12092	Location Based Service Proxy	Aeroscout Location-Based Service	Optional
AeroScout Server	Appliance	UDP	12092	1144	Location Based Service Proxy	Aeroscout Location-Based Service	Optional
Appliance	Extreme Cloud IQ	TCP	Any	443	NSight	Statistics Report into ExtremeCloud IQ	Yes

IETF STANDARDS MIB SUPPORT:

RFC No.	Title	Groups Supported
Draft version of 802.11	IEEE802dot11-MIB	
1213	RFC1213-MIB	Most of the objects supported
1573	IF-MIB	ifTable and interface scalar supported
1907	SNMPv2-MIB	System scalars supported
1493	BRIDGE-MIB	EWC supports relevant subset of the MIB
2674	P-BRIDGE-MIB	EWC supports relevant subset of the MIB
2674	Q-BRIDGE-MIB	EWC supports relevant subset of the MIB

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Extreme Networks Private Enterprise MIBs are available in ASN.1 format from the Extreme Networks website at: *https://extremeportal.force.com/.*

Standard MIBs

Title	Description
IEEE802dot11-MIB	Standard MIB for wireless devices
RFC1213-MIB.my	Standard MIB for system information
IF-MIB	Interface MIB
SNMPv2-MIB	Standard MIB for system information
BRIDGE-MIB	VLAN configuration information that pertains to EWC
P-BRIDGE-MIB	VLAN configuration information that pertains to EWC
Q-BRIDGE-MIB	VLAN configuration information that pertains to EWC

Siemens Proprietary MIB

Title	Description
HIPATH-WIRELESS-HWC-MIB.my	Configuration and statistics related to EWC and associated objects
HIPATH-WIRELESS-PRODUCTS-MIB.my	Defines product classes
HIPATH-WIRELESS-DOT11-EXTNS-MIB.my	Extension to IEEE802dot11-MIB that complements standard MIB
HIPATH-WIRELESS-SMI.my	Root for Chantry/Siemens MIB

802.11AC AND 802.11N CLIENTS

Please refer to the latest release notes for ExtremeWireless™ 10.41.09 or later and/or ExtremeWireless WiNG 5.9.02 or later for the list of compatibility test devices.

RADIUS SERVERS AND SUPPLICANTS

RADIUS Servers Used During Testing

Vendor	Model OS	Version
FreeRADIUS	1.1.6	FreeRADIUS
FreeRADIUS IAS	1.0.1	FreeRADIUS
	5.2.3790.3959	Microsoft Server 2003 IAS
SBR50	6.1.6	SBR Enterprise edition
NPS	6.0.6002.18005	Microsoft Server 2008 NPS

802.1x Supplicants Supported

Vendor	Model OS	Version
Juniper Networks® / Funk	Odyssey client	Version 5.10.14353.0
		Version 5.00.12709.0
		Version 4.60.49335.0
Microsoft®	Wireless Zero Configuration	Version Windows XP-4K-891859-Beta1
	Wireless Network Connection Configuration	Version Microsoft Window Server 2003, Enterprise Edition R2 SP2
	Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2	Version WindowsXP-KB893357-v2-x86-ENU.exe
Intel®	Intel PRO Set/Wireless	Version 13.0.0.x (with Windows® Intel® driver version 13.0.0.x)
Microsoft® Wireless Zero	Windows 7, 8, 8.1 Pro, 10 Pro Windows Phone 8.1, Windows Mobile 10	Provided with Windows®

F0615-O

Appliance LAN Switch Verification

Vendor	Model OS	Version	Role
Extreme	X-460-G2	12.5.4.5	XIQC connection
Extreme	X440G2-48p-10G4	21.1.1.4	XIQC connectivity
Extreme	Summit 300-48	7.6e1.4	XIQC connection
Extreme	VSP-4850GTS-PWR	(6.0.1.1_B003) (PRIVATE) HW Base: ERS 4850	XIQC connection
Extreme	K6	08.63.02.0004	XIQC connection
Extreme	K6	08.42.03.0006	XIQC connection
Extreme	X440G2-48p-10GE4	21.1.5.2	XIQC connection
Extreme	X440-G2-12p	21.1.1.4	XIQC connection
Extreme	X460-48p	12.5.4.5	XIQC connection
Cisco	Catalyst 3550	12.1(19)EA1c	XIQC connection

CERTIFICATION AUTHORITY

Server Vendor	Model OS	Version
Microsoft CA	Windows Server 2003 Enterprise Edition	5.2.3790.1830
Microsoft CA	Windows Server 2008 Enterprise Edition	6.0
OpenSSL	Linux	1.1.1g

RADIUS ATTRIBUTES SUPPORT

RADIUS Authentication and Authorization Attributes

Attribute	RFC Source
Called-Station-Id	RFC 2865, RFC 3580
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Event-Timestamp	RFC 2869
Filter-Id	RFC 2865, RFC 3580
Framed-IPv6-Pool	RFC 3162
Framed-MTU	RFC 2865, RFC 3580
Framed-Pool	RFC 2869
Idle-Timeout	RFC 2865, RFC 3580

F0615-O

Attribute	RFC Source
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-IPv6-Address	RFC 3162
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
Password-Retry	RFC 2869
Service-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
Tunnel Attributes	RFC 2867, RFC 2868, RFC 3580
User-Name	RFC 2865, RFC 3580
Vendor-Specific	RFC 2865

RADIUS Accounting Attributes

Attribute	RFC Source
Acct-Authentic	RFC 2866
Acct-Delay-Time	RFC 2866
Acct-Input-Octets	RFC 2866
Acct-Input-Packets	RFC 2866
Acct-Interim-Interval	RFC 2869
Acct-Output-Octets	RFC 2866
Acct-Output-Packets	RFC 2866
Acct-Session-Id	RFC 2866
Acct-Session-Time	RFC 2866
Acct-Status-Type	RFC 2866
Acct-Terminate-Cause	RFC 2866

F0615-O

GLOBAL SUPPORT:

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
https://extremeportal.force.com/

By Email: support@extremenetworks.com

By Web: https://extremeportal.force.com/

For information regarding the latest software release, recent release note revisions and documentation, or if you require additional assistance, please visit the Extreme Networks Support website.

F0615-O