Customer Release Notes

Extreme Campus Controller

Firmware Version V.05.46.09.0008
December 8, 2022

INTRODUCTION:

The Extreme Campus Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The Extreme Campus 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 10,000 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 Extreme Campus Controller offers the ability to expand capacity to meet any growing business needs. Extreme Campus Controller (V5) has now reached End-of-Sale. Please consider upgrading to ExtremeCloud IQ Controller (V10)

Changes in 05.46.09.0008	
Fixed Duplicate Signature Error that occurred when modifying Walled Garden Rules. Increased the FQDN address field to 64 bytes and added validation.	XCC-2854
Adjusted reference counting of VLANs in a VLAN Group to address issues with maximum limits.	XCC-2855
Corrected messaging mechanism between Extreme Campus Controller and Extreme A3 where Change of Authorization message from A3 was not acknowledged by Extreme Campus Controller.	XCC-2922
Improved responsiveness of GUI pages when thousands of items must be displayed.	XCC-2923
Improved presentation of customized captive portal page.	XCC-2933
Updated the Ekahau plan importer with better support for 6GHz radios.	XCC-2936
Fixed issue where mobile devices get stuck on registration in progress screen in a captive portal.	XCC-2937
Addressed stability issue with application Sensor component.	XCC-2952
Corrected a problem where enabling the Band Steering feature is not successful when an AP WLAN override is enabled.	XCC-2989
Improved stability of VE6125 by increasing size of data plane tables and throttling non-critical reporting.	CFD-8519

Changes in 7.8.6.0-002R	
Allow all WLAN services to start up correctly regarding the order of when session persistence is enabled.	WOS-4420

Changes in 05.46.09.0008	
Improved robustness of Extreme Campus Controller when moving multiple access points into a new device group.	XCC-2750
Strengthened the integrity of the system file to ensure uninterrupted functionality of the graphical interface.	XCC-2783
Increased the size of the needed resource table for proper data flow on the backup controller.	XCC-2793
Corrected communication disruption between Extreme Campus Controller and Extreme Wireless Controller for the Inter-Controller Mobility feature when Remote WLAN is enabled. Remote WLAN is not supported by Extreme Campus Controller.	XCC-2812

Changes in 7.8.6.0-002R	
Renewed access point commercial certificate for one year.	WOS-3930

Changes in 05.46.07.0009	
Increased scalability and improved performance of SmartRF to support larger sites.	CFD-6597
Refined the mechanism for removal of local users from secondary controller after expiration time.	CFD-7112
Removed the condition that prevented smooth client roaming in mobility domain between Extreme Campus Controller and Extreme Wireless Controllers	CFD-7395
Improved overall AP3915 stability by modifying DRAM memory initialization procedure.	CFD-7455
Adjusted logic to improve user's experience when using Guest captive portal with Topology Groups feature.	CFD-7702

Changes in 05.46.07.0009	
Corrected the condition that prevented wireless clients to obtain correct IP address when using multicast to unicast functionality.	CFD-7890
Updated theme of PDF reports to improve visual appearance	XCC-2584
Provide the administrative option to control multicast to unicast delivery for connected clients. The option is disabled by default, meaning access point radios will deliver multicast traffic as broadcast unless enabled.	XCC-2731

Changes in 7.8.4.0-007R	
Updated compliance table for AP4000 with disabled channel 50/160 (5G lower band) for all countries, channel 100/160 remains enabled.	WOS-3730
Enhanced robustness of processing Radio Calibration data to prevent memory corruption.	WOS-3806
Corrected wireless client connectivity issue on DFS channels when used with Hotspot feature.	WOS-3823

Changes in 05.46.06.0007	
Corrected the condition that caused a partial display of the list of registered guest users.	XCC-2452
Cleaned up superfluous UI logic that could result in HTTP 405 (Method not allowed) errors when configuring WPA3 settings.	XCC-2481
Corrected the issue whereby Chargeable User Identity (CUID) may not consistently be included in RADIUS Accounting Stop messages in High-Availability controller installations.	XCC-2485
Enhanced processing of various fields that belong to RADIUS Accounting packets to prevent random Accounting discards.	XCC-2507
Corrected the issue with Maps where access points and badges were not properly displayed on floor plans.	XCC-2527

Changes in 05.46.05.0002	
Corrected use of security manager token for clients that had issues with 802.1x authentication.	XCC-2388
Improved handling for scheduled events when Change to Daylight Saving Time event is within the scheduled period.	CFD-7286
Increased DPI resolution for PDF reports from 96 to 300.	XCC-2379
Enhanced option to restrict critical layer 2 broadcast per topology.	XCC-2332

Changes in 05.46.04.0010	
Improved controller stability with additional protective code to deal with malformed, encrypted packets coming to the data plane.	CFD-6616
Corrected the issue where a long URL was created erroneously after editing floor plans.	CFD-7469
Corrected the issue that could affect synchronization of configuration updates between two controllers in a High Availability Pair.	CFD-7470
Adjusted the Automatic Channel Selection logic for the AP3900 series, removing options for non-supported channel widths.	CFD-7488

Changes in 05.46.04.0010	
Adjusted interface settings for the E3120 40Gbps ports, improving performance handling for large frame bursts.	XCC-2203
Corrected the situation that prevented the Save action from storing Defined User Groups for Venue Reports.	XCC-2293
Corrected the issue where topology changes (Add/Remove) to Bridged@AP or Fabric Attach VLAN did not always propagate correctly.	XCC-2316
Corrected the Ethertype value for IPv6 policy rule definition.	XCC-2324
Adjusted the limitation of CoA shared secret to 64 characters.	XCC-2337

Enhancements in 05.46.03.0013	
Added support for the adoption of AP5xx-1/AP4xx-1/AP3xx-1. All functionality from similar 11ax AP models is supported, except for the following features:No support for Bluetooth Low Energy (BLE) (iBeacon, Eddystone) , Zigbee, or Thread Gateway - No 160 MHz operation in 5 GHz radio	XCC-1960
Introduced support for WPA3-Personal SAE Hash-to-Element (H2E) wireless encryption for AP4000 models.	XCC-2145
Exposed configuration for RADIUS accounting mode selection as Broadcast vs Failover.	XCC-1834
Added warning of impending license expiration in the System Health Widget.	XCC-2045
Added the ability to override the default WLAN assignment to client ports for individual APs.	XCC-1937

Changes in 05.46.03.0013	I.D
Channel 103 (in 6 GHz band: 103e/80Mhz) is now available for direct manual assignment for AP4000 devices.	XCC-2048
Improved Floorplan representation of channel coverage for 6 GHz operation. The channel range was increased to 233 for 6 GHz radio.	XCC-1998
Updated Power Source column on AP List for clarity. Possible values are DC, AF, AT.	XCC-2052

Enhancements in 05.46.02.0019	
Enforced compatibility check for 6 GHz operation, in accordance with WFA 6E rules. WFA 6E dictates that WPA3 and OWE are minimum required security options for network operation. Network definition will identify compliant networks. Network assignment to Radio 3 for 6 GHz restricts assignment to only compliant networks.	XCC-1649
Added option to enable Fast Initial Link Setup (FILS) for in-channel service advertisement on 6 GHz operation. Disabled by default in accordance with WFA requirements.	XCC-1774
Enhanced Site Floorplan visualization to represent Channel and RF coverage for 6 GHz operation.	XCC-1645
Deprecated "AUTO" configuration option for SmartRF configuration. Adjusted algorithm to use requested width as designation for desired bandwidth. Algorithm will try to resolve channel/power plan at desired width. SmartRF automatically adjusts to lower widths when unable to fulfill the requested width.	XCC-1794
Enhanced AAA definitions to allow definition of threshold values to cap repetitive authentication attempts by failed clients. Threshold can hold off clients that exceed	XCC-1484

Enhancements in 05.46.02.0019	
threshold values of authentication attempts in time period from re-authenticating for a given timeout period, thus reducing load on backend authentication servers.	
Enhanced SmartRF Neighbor reports to display SSID along with BSSID for detected networks.	XCC-1335
Added a new Best Practices Assessment of Poll timeout for mesh nodes.	XCC-1751
Provided visual notification alert in application banner of impending expiration of subscriptions within 90 days.	XCC-1788
Enhanced tooltip on data-series for each SSID in multi-SSID performance widgets, displaying the actual SSID. This enhancement makes it easier to identify which time-series maps to which network.	XCC-1647

Changes in 05.46.02.0019	I.D
Corrected issue with cloning Profiles that could result in incorrect radio settings, preventing assigned APs from providing service.	XCC-1944

Enhancements in 05.46.01.0024	
Added support for the adoption of the AP4000-WW access point. The AP4000 is a tri-band Worldwide (WW) SKU. The AP provides the option to operate three radios of Wi-Fi 6 Connectivity for 2.4 GHz, 5.0 GHz, and 6.0 GHz (Wi-Fi___33 6E) or alternatively, 2.4 GHz, 5 GHz, and tri-band sensor. This AP can also be deployed in support of (Policy) Mesh and/or Client Bridge, including leveraging the 6 GHz radios to carry the backhaul traffic.	XCC-1644
Introduced the VE6120K, a KVM-based virtual appliance configuration supporting up to 500 APs and 8,000 end-users in a single appliance, or 1000 APs and 16,000 end-users in High Availability.	XCC-643
Introduced the VE6125K, a virtual appliance configuration for KVM hypervisors, supporting up to 2000 APs and 16,000 end-users in a single appliance, or 4000 APs and 32,000 end-users in High Availability.	XCC-15
Added an enhanced access point details view that provides a graphical topology representation of AP connectivity into the upstream switches and the logical association with managing appliances. The Topology view is an alternative to the Floorplan view.	XCC-1394
Added support to define Allow/Deny MAC list per site. The site-level definition list overrides values from the global list.	XCC-1483
Increased upper range for policy rate limit to 500Mbps.	XCC-1176
Deprecated support of TLS 1.1 as a default option. TLS 1.1 support has been moved to the Weak Cypher category.	XCC-1643

Changes in 05.46.01.0024	I.D
Improved UI performance for loading client details listing for large installations.	CFD-6835
Improved performance of authentication services to handle larger transactional rates in larger installations.	CFD-6813

Changes in 05.46.01.0024	I.D
Introduced option to control whether to remove client sessions in the presence of Disconnect requests by clients.	XCC-1814

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.05.46.09.0008	Maintenance Release	December 8, 2022
Previous Version	V.05.46.08.0004	Maintenance Release	August 15, 2022
Previous Version	V.05.46.07.0009	Maintenance Release	July 7, 2022
Previous Version	V.05.46.06.0007	Maintenance Release	May 6, 2022
Previous Version	V.05.46.05.0002	Maintenance Release	March 16, 2022
Previous Version	V.05.46.04.0010	Maintenance Release	February 25, 2022
Previous Version	V.05.46.03.0013	Feature Release	December 16, 2021
Previous Version	V.05.46.02.0019	Feature Release	November 08, 2021
Previous Version	V.05.46.01.0024	Feature Release	September 30, 2021

SUPPORTED APPLIANCES, ACCESS POINTS AND SWITCHES:

Product Name	Image
Extreme Campus Controller VE6120 VMware Min Supported ESXi version 5.1 or later, (tested 6.7)	ECA-05.46.09.0008-1.dle
Extreme Campus Controller VE6120H (Windows server 2016 or later)	ECA-05.46.09.0008-1.spe
Extreme Campus Controller VE6120K Linux KVM	ECA-05.46.09.0008-1.dve
Extreme Campus Controller VE6125 Min Supported ESXi version 5.5 or later, (tested 6.7)	ECA-05.46.09.0008-1.rse
Extreme Campus Controller VE6125K Linux KVM	ECA-05.46.09.0008-1.mfe
Extreme Campus Controller E1120	ECA-05.46.09.0008-1.sme
Extreme Campus Controller E2120	ECA-05.46.09.0008-1.jse
Extreme Campus Controller E2122	ECA-05.46.09.0008-1.wze
Extreme Campus Controller E3120	ECA-05.46.09.0008-1.ose
SA201	AP391x-10.51.23.0003.img
AP302W-CAN AP302W-FCC	AP302W-LEAN-7.8.6.0-002R.img

Product Name	Image
AP302W-IL AP302W-WR	
AP305C-CAN AP305C-FCC AP305C-IL AP305C-WR AP305CX-CAN AP305CX-FCC AP305CX-IL AP305CX-WR	AP3xxC-LEAN-7.8.6.0-002R.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-7.8.6.0-002R.img
AP360e-CAN AP360e-FCC AP360e-IL AP360e-WR AP360i-CAN AP360i-FCC AP360i-IL AP360i-WR	AP3xx-LEAN-7.8.6.0-002R.img
AP3912i-FCC AP3912i-ROW	AP391x-10.51.23.0003.img
AP3915e-FCC AP3915e-ROW AP3915i-FCC AP3915i-ROW	AP391x-10.51.23.0003.img
AP3916ic-FCC AP3916ic-ROW	AP391x-10.51.23.0003.img
AP3916-camera	AP3916IC-V1-0-14-1.dlf
AP3917e-FCC AP3917e-ROW AP3917i-FCC AP3917i-ROW AP3917k-FCC AP3917k-ROW	AP391x-10.51.23.0003.img
AP3935e-FCC AP3935e-ROW AP3935i-FCC AP3935i-IL AP3935i-ROW	AP3935-10.51.23.0003.img

Product Name	Image
AP3965e-FCC AP3965e-ROW AP3965i-FCC AP3965i-ROW	AP3935-10.51.23.0003.img
AP4000-WW	AP4000x-LEAN-7.8.6.0-002R.img
AP4000U-WW	AP4000x-LEAN-7.8.6.0-002R.img
AP410C-CAN AP410C-FCC AP410C-IL AP410C-WR	AP4xxC-LEAN-7.8.6.0-002R.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-7.8.6.0-002R.img
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-7.8.6.0-002R.img
AP460e-CAN AP460e-FCC AP460e-IL AP460e-WR AP460i-CAN AP460i-FCC AP460i-IL AP460i-WR	AP4xx-LEAN-7.8.6.0-002R.img
AP505i-FCC AP505i-WR	AP5xx-LEAN-7.8.6.0-002R.img
AP510e-FCC AP510e-WR AP510i-1-FCC AP510i-1-WR AP510i-FCC AP510i-WR	AP5xx-LEAN-7.8.6.0-002R.img

Product Name	Image
AP560h-FCC AP560h-WR AP560i-FCC AP560i-WR	AP5xx-LEAN-7.8.6.0-002R.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 220-12p-10GE2 POE 220-24p-10GE2 POE 220-48p-10GE2 POE	220-series_V1.02.05.0013.stk fp-connector-3.3.0.4.pyz (cloud connector)
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™	21.9 or higher
ExtremeAnalytics™	21.9 or higher
ExtremeCloud™ A3	4.0
ExtremeCloud™ IQ-Site Engine	21.9 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 Restriction or Limitation	I.D
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
ExtremeCloud IQ-Site Engine 21.4.11 or Extreme Management Center 8.5.6 is the minimum required revision for representation of Extreme Campus Controller 5.36.01 or later revisions. ExtremeCloud IQ-Site Engine 21.9 is the minimum required revision for representation of Extreme Campus Controller 5.46.01 or later revisions. Extreme Management Center (8.5.x or later) does NOT properly recognize an controller running 5.46.01 or later.	XCC-1486
A reboot of the peer Extreme Campus Controller is required when 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.	ECA-622

Known Restriction or Limitation	I.D
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 Extreme Campus Controller configured for authentication of administrators over RADIUS server, the GUI responsiveness may be slow, possibly over 30 seconds if target server(s) are unavailable/unreachable at login time. If outage is extensive, system will eventually timeout to validate against local credentials when provisioned.	ECA-1396
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
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

Known Restriction or Limitation	I.D
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
Before installing a new Extreme Campus Controller license, you must configure Network Time Protocol (NTP) Server settings. Licensing management is dependent on accurate NTP configuration. Configure NTP via the Extreme Campus Controller initial Configuration Wizard, or go to Admin > System > Network Time to configure and verify the NTP settings.	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
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

Known Restriction or Limitation	I.D
Maximum Transmission Unit (MTU) 256 or higher between APs and Controllers is required for uninterrupted service.	Info CFD-7804

SUPPORTED WEB BROWSERS

For Extreme Campus 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	75.0.37770.142	Windows 7 Windows 10
Microsoft IE	11	Windows 7 Windows 8.1 Windows 10
Microsoft Edge	42.17134	Windows 10
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.

Extreme Campus 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	Yes

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
						between AP and Appliance	
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
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

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
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
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

[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
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	1.0.1	FreeRADIUS
IAS	5.2.3790.3959	Microsoft Server 2003 IAS

Vendor	Model OS	Version
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®

Appliance LAN Switch Verification

Vendor	Model OS	Version	Role
Extreme	X-460-G2	12.5.4.5	ECA connection
Extreme	X440G2-48p-10G4	21.1.1.4	ECA connectivity
Extreme	Summit 300-48	7.6e1.4	ECA connection
Extreme	VSP-4850GTS-PWR	(6.0.1.1_B003) (PRIVATE)Â HW Base: ERS 4850	ECA connection
Extreme	K6	Â 08.63.02.0004	ECA connection
Extreme	K6	08.42.03.0006	ECA connection

Vendor	Model OS	Version	Role
Extreme	X440G2-48p-10GE4	21.1.5.2	ECA connection
Extreme	X440-G2-12p	21.1.1.4	ECA connection
Extreme	X460-48p	12.5.4.5	ECA connection
Cisco	Catalyst 3550	12.1(19)EA1c	ECA 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
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

Attribute	RFC Source
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

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.