6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

Extreme Campus Controller

Firmware Version V05.06.01.0035
June 23, 2020

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

The VE6125 XL is an virtual appliance that supports 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 growing business needs. The hardware and virtual packages are available for purchase using a traditional CAPEX model. The customer has the option to purchase adoption capacity via a Perpetual (CAPEX) model or as a Right-To-Use Subscription model, supporting flexible quantites (per managed device) and term (multiple-year extended term) option.

Enhancements in 05.06.01.0035	
Extreme Campus Controller is the new name of the product line formerly known as ExtremeCloud Appliance.	ECA-1589
Extreme Campus Controller version 5 is a Centralized site (Campus only) distribution. Removed support for creating or upgrading Distributed sites and deprecated support for Distributed operational mode for AP300, AP400, and AP500 series access points. Also removed support for adoption of WiNG APs AP75xx, AP76xx, and AP85xx/84xx. To prevent accidental service impact, the upgrade process will abort any upgrades from Version 4 installations with configured Distributed sites. WiNG-Proxy for Extreme Management Center (XMC) mode is also deprecated with version 5 of the software. Customers can continue to leverage version 4 (4.76) for such deployments.	ECA-1230
Extreme Campus Controller version 5 requires new Activation Licenses. Version 5 introduces also a new enhanced method to access and represent Subscription entitlements. Existing customers with valid support contracts can request upgrade licenses for their registered instances via the Support Portal. Customers with Subscription Adoption license are asked to migrate existing Version 4 contracts (Assigned to parts 30327-30331) to new V5 Right-to-Use. Please refer to "Upgrade Service Contracts" guide in the Extreme Networks Documentation Portal for more details on the procedure. New customers or extensions to Extreme Campus Controller, please refer to the Datasheet for listing of Activation and Adoption (Capacity) licensing options.	ECA-388
Removed restricted DEMO operational mode. New system deployments require an activation license. Customer prospects (Proof-of-Concept) can request an evaluation license for their instances via the Support Portal (up to 30 days), or via a Partner or assigned Sales-Engineer (up to 180 days). See datasheet for listing of purchase Activation and Adoption license options.	ECA-555
Introduces support for AP360 variants: • AP360i-FCC • AP360i-WR • AP360i-CAN • AP360i-IL • AP360e-FCC • AP360e-WR • AP360e-CAN • AP360e-IL See the Access Point list for more information.	ECA-1714
Client-Bridged mode for WiFi6 access points. Provides the ability to configure an AP radio as a Client-Bridge, enabling an AP to operate as a client of the infrastructure networks. This feature enables leveraging a WiFi6 access point to enable non-WiFi capable end-system clients to attach to infrastructure network services and even roam across the infrastructure. Client-Bridge can also be used to extend Wireless network services by one-hop from last available ethernet drop. Client-Bridge functionality requires ExtremeWireless WiFi 6 access points, such as the AP300, AP400, and AP500 i/e series.	ECA-1513

Introduces new VxLAN Topology option, expanding the options on how customers can design the network paths for end-system traffic. New Topology can be used in Role-assigned policy to leverage the VxLAN capabilities of ExtremeXOS switches to establish different head-ends for tunneling traffic in an enterprise. This capability provides the ability to tunnel end-user traffic from the AP to an upstream aggregation switch using VxLAN, enabling bypassing of the managing controller and abstracting the interconnecting infrastructure.	ECA-1184
Support for Centralized Web Authentication (CWA) offers the ability to serve a Captive Portal experience based on a set of conditions that are defined on the AAA authentication servers. Specifics on which experience to serve are provided by the infrastructure via the inclusion of an URL-REDIRECT option in RADIUS-ACCEPT responses or Change-of-Authorization notifications. For 802.1x networks, following successful authentication, users can be redirected to a specific captive portal for further business compliance action. One typical use case is to inform the user that the password has expired offering an opportunity to update corporate access credentials.	ECA-1581
Introduces the System Health report that provides assessment of best practices for your Extreme Campus Controller configuration. System Health status is provided via the system Notification and details can be explored via a new 'System Health" Widget selectable for the main Dashboard. The system provides assessment over a set of conditions, including: • Number of SSIDs per radio (Less than 4 recommended) • Configuring a Schedule for configuration backup is highly recommended • Usage of TKIP for network privacy • Band steering enabled and 5GHz radio disabled • Active APs not assigned to site • Indication of AP with configured overrides • 40Hz channel width on 2.4GHz radio • For installations with SmartRF enabled, but SmartRF Smart-monitoring disabled • Probe suppression threshold too high • Radio in sensor mode and no scan profiles assigned • Configuration of Secure Tunnel disabled • Role with more than 64 rules is assigned to AP/profile, that does not support more than 64 rules • NTP configured A green check mark indicates that a best practice is being followed. A yellow and red warning icon indicates that your configuration is not optimal. Future revisions will expand on list of assessment criteria conditions.	ECA-1185
Policy definition was enhanced to allow expansion of rule-sets of up to 256 rules. This option is only compatible with ExtremeWireless WiFi 6 access points: AP300, AP400, and AP500 series.	ECA-1580

Smart RF configuration layout was improved to make Smart RF enablement more explicit. Smart Monitoring Enabled is now on the Smart RF Basic Settings tab. Enable Smart Monitoring to display Smart RF parameters. When Smart Monitoring is disabled, the following Smart RF options and tabs are hidden: • Sensitivity and Recovery options from the Basic tab. • Scanning tab • Recovery tab • Select Shutdown tab	ECA-1579
Enhanced client and access point views to persist column selection and sizing per user account.	ECA-1578
Provided better integration with the browser-obtained location data to automatically populate site location fields when creating new sites: • Time zone • Region • City The Location field allows admins to enter mapping coordinates directly and pinpoint on the map the location of the corresponding coordinates. Note: Requires Location Services to be enabled on the administration web browser.	ECA-1577
Enhanced the Client report to display the channel to which client is currently connected.	ECA-1576
Enhanced the Client report and dashboards to provide details on connected client's protocol capabilities: 802.11r, 802.11w (PMF).	ECA-1575
Enhanced the Client report to provide visibility on characteristics of the connecting client. Chain Count: 1x1, 2x2, 3x3, 4x4.	ECA-1574
Maximum size of a Floor plan representative size has been increased to 200,000 m2.	ECA-1573
Improved support for installations using HTTP-Proxy by providing the ability to configure the list of IP (HTTP) ports to be subjected to HTTP-Redirection.	ECA-1545
Provided option to disable Auto-Login for Captive Portal detection.	ECA-1515
Introduce a new per-access point Channel Inspector Interference Report, which provides a high level of visibility as to the occupancy of the RF spectrum around a particular AP.	ECA-1512
Provided the ability to set up authentication chaining between MAC-Based-Authentication (MBA) and 802.1x authentication, whereby only allowed devices can connect to the infrastructure with the following workflow: Perform MAC Based auth for an associating client, • if client is allowed in MBA, then client is allowed to proceed to 802.1x registration • if client is rejected by MBA, then client is disconnected from the network	ECA-1482

For installations of High-Availability, system will no longer enforce automatic upgrades for registering access points. Software upgrade of access points is under the control of the administrator (Upgrade Now or Impact Aware Upgrade). Running access point firmware revisions different than the revision included with the appliance upgrade package is strongly not recommended. System Heath will record a best practice non-compliance for this condition.	ECA-1873

Changes in 05.06.01.0035	I.D
When using dual-band configuration on the AP510e, best practice is to disable usage of the Group 2 antenna (Ports 5-8).	ECA-1074

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.05.06.01.0035	Feature Release	June 23, 2020

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-05.06.01.0035-1.dle
Extreme Campus Controller VE6120H (Windows server 2016 or later)	ECA-05.06.01.0035-1.spe
Extreme Campus Controller VE6125 Min Supported ESXi version 5.5 or later, (tested 6.7)	ECA-05.06.01.0035-1.rse
Extreme Campus Controller E1120	ECA-05.06.01.0035-1.sme
Extreme Campus Controller E2120	ECA-05.06.01.0035-1.jse
Extreme Campus Controller E3120	ECA-05.06.01.0035-1.ose
AP310e-CAN AP310e-FCC AP310e-IL AP310e-WR AP310i-CAN AP310i-FCC AP310i-IL AP310i-WR	AP3xx-LEAN-7.4.0.0-025R.img
AP360e-CAN	AP3xx-LEAN-7.4.0.0-025R.img

Product Name	Image
AP360e-FCC AP360e-IL AP360e-WR AP360i-CAN AP360i-FCC AP360i-IL AP360i-WR	
AP3912i-FCC AP3912i-ROW	AP391x-10.51.13.0003.img
AP3915e-FCC AP3915e-ROW AP3915i-FCC AP3915i-ROW	AP391x-10.51.13.0003.img
AP3916ic-FCC AP3916ic-ROW	AP391x-10.51.13.0003.img
AP3916-camera	AP3916IC-V1-0-14-1.dlf
AP3917e-FCC AP3917e-ROW AP3917i-FCC AP3917i-ROW AP3917k-FCC AP3917k-ROW	AP391x-10.51.13.0003.img
AP3935e-FCC AP3935e-ROW AP3935i-FCC AP3935i-IL AP3935i-ROW	AP3935-10.51.13.0003.img
AP3965e-FCC AP3965e-ROW AP3965i-FCC AP3965i-ROW	AP3935-10.51.13.0003.img
AP410e-CAN AP410e-FCC AP410e-IL AP410e-WR AP410i-CAN AP410i-FCC AP410i-IL AP410i-WR	AP4xx-LEAN-7.4.0.0-025R.img
AP460e-CAN AP460e-FCC	AP4xx-LEAN-7.4.0.0-025R.img

Product Name	Image
AP460e-IL AP460e-WR AP460i-CAN AP460i-FCC AP460i-IL AP460i-WR	
AP505i-FCC AP505i-WR	AP5xx-LEAN-7.4.0.0-025R.img
AP510e-FCC AP510e-WR AP510i-FCC AP510i-WR	AP5xx-LEAN-7.4.0.0-025R.img
AP560h-FCC AP560h-WR AP560i-FCC AP560i-WR	AP5xx-LEAN-7.4.0.0-025R.img
SA201	AP391x-10.51.13.0003.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)
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-3.4.1.20.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 onie-cloud_connector-3.2.5.16.xmod

Product Name	Image
X620-16x	summitX-30.2.1.8-patch2-5.xos summitX-30.2.1.8-cloud_connector-3.4.1.20.xmod (cloud connector)

NETWORK MANAGEMENT SOFTWARE SUPPORT

Network Management Suite (NMS)	Version
ExtremeManagement™ Center	8.5 or higher
ExtremeControl™	8.5 or higher
ExtremeAnalytics™	8.5 or higher

Air Defense and Location	Version
ExtremeAirDefense™	10.4
ExtremeLocation™	3.1
ExtremeGuest	**Version**
ExtremeGuest™	6.0.1.0-001R

Note:

Platform and AP Configuration functions are not supported by ExtremeManagement™.

Extreme Campus Controller does not yet expose support for ExtremeLocation™ Calibration procedure. ExtremeLocation will work correctly for Zone and Occupancy level analytics but does not fully support Position Tracking with this release. Enhanced support for Position Tracking will be added to a future release of Extreme Campus Controller.

INSTALLATION INFORMATION:

Appliance Installations	
E1120	Extreme Campus Controller E1120 Installation Guide
E2120	Extreme Campus Controller E2120 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

PREVIOUS RELEASES EXTREME CLOUD CONTROLLER

Enhancements in 04.76.04.0005	
Please see the v04.76.04.0005 release notes document for this version.	

Changes in 04.76.04.0005	I.D
Please see the v04.76.04.0005 release notes document for this version.	

Known Restrictions and Limitations:

Known Restriction or Limitation	I.D
When applying V5 Activation Bundles on an availability pair with Evaluation licenses, it is recommended that you follow this procedure: 1) Apply V5 Activation bundle on the Primary controller and select **Permanent mode**. 2) Apply V5 Activation bundle on Backup controller. 3) If using Subscription Licensing, select **Subscription mode** on the Primary controller.	ECA-1972
If a license violation is corrected, the license violation banner and GUI notification bell are not cleared until page is refreshed. Similarly, in a new installation, after a license is installed, refresh the page.	ECA-1971
For Client-Bridge configurations, it is recommended to use Radio 2 (5.0 GHz) for infrastructure uplink/connection. A possible instability with Radio 1 (2.4 GHz) usage is under investigation. This issue will be addressed in an future software release.	ECA-1962
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
Possible issue with interoperability with Aeroscout RTLS under investigation. This issue will be addressed in a future release.	ECA-1960
For customers with perpetual Activation licensing, the system allows a 7-day grace period when the system is oversubscribed (when there are more devices adopted than are installed with the license capacity). If additional capacity is not installed during the grace period, after the grace period expires, add a capacity key to clear the violation. The system will remain in readonly mode. Log out and log in again. This issue will be corrected in a future release.	ECA-1954
AP310 models are not currently supported by ExtremeLocation(TM). Do not enable ExtremeLocation settings in the configuration Profile for AP310 device groups. Doing so may have a negative impact on AP performance.	ECA-1620
Firmware for ExtremeWireless AP3900 series access points does not currently support Smart RF. No Smart RF data is displayed.	ECA-1484
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, if so 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).	ECA-1264

Known Restriction or Limitation	I.D
Users immediately reconnect to the available infrastructure, so impact is negligible. For smoother Session Availability with Fast-Failover during an Failover event, it is recommended to not run these options at this time. This issue is being investigated and will be addressed in future releases.	
Recommendation settings for set up of redundant RADIUS server authentication: 1) Response Window to 5s [Default: 20s] 2) Revival Interval to 10s [Default: 60s]	Info ECA-875
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: • "Network Health" widget on Dashboard • Administration -> System -> Availability	Info ECA-776
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 subsequent release.	ECA-622
Editing or deleting Control VLAN under the Mesh Network is not possible. This problem will be corrected into a future release.	ECA-573
Widgets do not show tooltips for Lower and Upper values. This issue will be addressed in a future release.	ECA-567
GUI Mesh Report is missing the information about Root AP with Ethernet connection. This problem will be addressed in a future release.	ECA-565
Docker requires exclusive use of subnet 172.17.0.0/16 for containers. Customers should not use an IP address in that range for any VLAN or network interface.	ECA-532
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
Extreme Campus Controller user accounts created in the pre-registration page do not propagate to the AAA policy.	ECA-521
In SmartRF mode, the AP510 power may temporarily drop to 0dBm and returns to 4dBm.	ECA-469
Upgrade failure will occur when using special characters (escape back slash) in topology.	ECA-466
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

Known Restriction or Limitation	I.D
After switching from Whitelist mode to Blacklist mode, it is possible that the traffic from the blacklisted client will not to be filtered and will be able to connect to different wireless networks and obtain Internet access. This problem will be resolved in the next release.	ECA-373
Client Badge in a Floor plan may not show correctly. This issue will be addressed in a subsequent release.	ECA-369
Wired packet captures for APs in Centralized sites may take up to 1 minute to show results. This issue will be addressed in a subsequent release.	ECA-362
Combining MAC Based Authentication and LAG for switch ports is not currently supported. Engineering is investigating. The issue will be addressed in an upcoming release.	ECA-335
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
Please allow at least 20 seconds between stopping and re-starting a packet capture on a site.	ECA-251
Enabling the appliance as a DHCP server for an attached segment is not currently recommended. Experiencing issues with persistence of Default Gateway and IP range settings. This issue will be corrected in an upcoming release.	ECA-171
MAC address for clients on ExtremeWireless WiNG™ APs are displayed in the Username column. WiNG APs send the username as a MAC Address, causing NAC to re-evaluate the rule engines. This situation will be addressed in a future release.	ECA-128
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.	nse0005086
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.	nse0003696
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
Wireless capture on Wing APs may return the wrong packet captures containing wired packets and wireless packets only for uplink. This situation will be addressed in a future release.	nse0002243

Known Restriction or Limitation	I.D
Deployment of appliances behind NAT is not officially supported. While configurations are available that enable this operation, this configuration is not validated by engineering. Therefore for installations requiring remote connectivity options, direct public address exposure is the recommended and officially supported configuration.	Info
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 See KB https://gtacknowledge.extremenetworks.com/articles/Solution/AP510-Unable-to-see-the-SSID-on-my-laptop 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
ExtremeGuest support will be finalized in the next maintenance release and by the release of eGuest server 6.0.	Info
Interaction with ExtremeManagement Center – Management of Extreme Campus Controller by ExtremeManagement Center will be enhanced over time with the roadmap. ExtremeManagement Center v8.5 is the minimum release base for integration. Version 8.5 provides recognition of an Extreme Campus Controller and representation of Wireless Clients and managed Access Points included in the Wireless tab. Additional integration will be delivered in upcoming releases. ExtremeManagement Center 8.5 is the current recommended minimum release.	Info
Several features of WiNG 7 OS are still under-development plan towards full feature parity. Several functions may be available in the user interface, due to common provisioning, but are not yet fully supported.	Info

SUPPORTED WEB BROWSERS

For Extreme Campus Controller management GUI, the following Web browsers were tested for interoperability:

- Firefox 38.0
- Google Chrome 43.0

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

The Wireless Clients (Captive Portal, AAA):

Browsers	Version	OS
Firefox	68.0	Windows 10

Browsers	Version	OS
Safari	Preinstalled with iOS 12.2	iOS 12.2
Safari	Preinstalled with iOS 9.3.5	iOS 9.3.5
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

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.

ExtremeWireless 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

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

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
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
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.	Appliance	UDP	Any	3799	DAS	Request from DAS client to disconnect a specific client	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
Server (NAC)							
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

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

Title	Description
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
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

Vendor	Model OS	Version
	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) HW Base: ERS 4850	ECA connection
Extreme	K6	08.63.02.0004	ECA connection
Extreme	K6	08.42.03.0006	ECA connection
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	0.9.8e

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
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/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119 USA

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.