

# Customer Release Notes

## ExtremeCloud Appliance

Firmware Version V04.76.06.0006

Sep 03, 2020

### INTRODUCTION:

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends all the ease-of-use and simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments. The ExtremeCloud Appliance 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 a 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 ExtremeCloud Appliance offers the ability to expand capacity to meet any growing business needs. The hardware and virtual packages are available for purchase using a traditional CAPEX model, while the adoption licenses are available as an annual subscription service in 5, 25, 100, 500 and 2000 managed device increments.

**This Release includes all previous 4.36.xx.xxxx and 4.56.xx.xxxx enhancements and changes**

| Enhancements in 04.76.06.0006  | I.D      |
|--|----------|
| Preserved value of self-generated NAS IP on upgrades.  | ECA-1867 |
| Corrected issue with inclusion of AP-hostname in AP beacon for AP3900 series.  | ECA-1993 |
| Corrected periodically displayed stale "last seen" time on Client Monitor screen.  | ECA-2031 |
| Improved appliance stability by preventing restarts of internal core component.  | ECA-2041 |
| Removed the condition that prevented addition of AP7662 to a device group.   | ECA-2098 |
| Rectified the problem that caused Samsung Galaxy A5, A8 and A10 connected to AP8432 to be shown as "Unknown" device.   | ECA-2103 |
| Enhanced robustness of appliance for handling internally generated policy references used in External captive portal. Incorrect references could lead to system instability. | ECA-2140 |
| Corrected synchronization issue with low level QOS definitions for installations in a High-Availabilty configuration.  | ECA-2154 |

**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/](http://www.extremenetworks.com/support/)

**FIRMWARE SPECIFICATION:**

| Status           | Version No.     | Type                | Release Date      |
|------------------|-----------------|---------------------|-------------------|
| Current Version  | V.04.76.06.0006 | Maintenance Release | Sep 03, 2020      |
| Previous Version | V.04.76.05.0009 | Maintenance Release | July 07, 2020     |
| Previous Version | V.04.76.04.0005 | Maintenance Release | May 19, 2020      |
| Previous Version | V.04.76.03.0015 | Feature Release     | April 20, 2020    |
| Previous Version | V.04.76.02.0035 | Feature Release     | March 30, 2020    |
| Previous Version | V.04.76.01.0081 | Feature Release     | February 11, 2020 |

**SUPPORTED APPLIANCES, ACCESS POINTS AND SWITCHES:**

| Product Name  | Image                   |
|---|-------------------------|
| ExtremeCloud Appliance VE6120 VMware<br>Min Supported ESXi version 5.1 or later, (tested 6.7) | ECA-04.76.06.0006-1.dle |
| ExtremeCloud Appliance VE6120H<br>(Windows server 2016 or later)                              | ECA-04.76.06.0006-1.spe |
| ExtremeCloud Appliance VE6125<br>Min Supported ESXi version 5.5 or later, (tested 6.7)        | ECA-04.76.06.0006-1.rse |
| ExtremeCloud Appliance E1120  | ECA-04.76.06.0006-1.sme |
| ExtremeCloud Appliance E2120  | ECA-04.76.06.0006-1.jse |

| Product Name   | Image                        |
|--|------------------------------|
| ExtremeCloud Appliance E3120   | ECA-04.76.06.0006-1.ose      |
| <b>Note:</b> With v4.76.01, all adopted APs are adopted into Campus mode for Centralized Deployments.  |                              |
| AP-7522-67030-1-WR<br>AP-7522-67030-EU<br>AP-7522-67030-US<br>AP-7522-67030-WR<br>AP-7522-67040-1-WR<br>AP-7522-67040-EU<br>AP-7522-67040-US<br>AP-7522-67040-WR<br>AP-7522E-67030-EU<br>AP-7522E-67030-US<br>AP-7522E-67030-WR<br>AP-7522E-67040-EU<br>AP-7522E-67040-US<br>AP-7522E-67040-WR | AP7522-LEAN-7.3.1.4-003R.img |
| AP-7532-67030-1-WR<br>AP-7532-67030-EU<br>AP-7532-67030-IL<br>AP-7532-67030-US<br>AP-7532-67030-WR<br>AP-7532-67040-1-WR<br>AP-7532-67040-EU<br>AP-7532-67040-US<br>AP-7532-67040-WR   | AP7532-LEAN-7.3.1.4-003R.img |
| AP-7562-670042-1-WR<br>AP-7562-670042-EU<br>AP-7562-670042-IL<br>AP-7562-670042-US<br>AP-7562-670042-WR<br>AP-7562-67040-1-WR<br>AP-7562-67040-EU<br>AP-7562-67040-US<br>AP-7562-67040-WR<br>AP-7562-6704M-1-WR<br>AP-7562-6704M-EU<br>AP-7562-6704M-US<br>AP-7562-6704M-WR                    | AP7562-LEAN-7.3.1.4-003R.img |
| AP-7612-680B30-US<br>AP-7612-680B30-WR   | AP7612-LEAN-7.3.1.4-003R.img |
| AP-7632-680B30-IL<br>AP-7632-680B30-TN   | AP7632-LEAN-7.3.1.4-003R.img |

| Product Name  | Image                        |
|---|------------------------------|
| AP-7632-680B30-US<br>AP-7632-680B30-WR<br>AP-7632-680B40-TN<br>AP-7632-680B40-US<br>AP-7632-680B40-WR   |                              |
| AP-7662-680B30-IL<br>AP-7662-680B30-TN<br>AP-7662-680B30-US<br>AP-7662-680B30-WR<br>AP-7662-680B40-TN<br>AP-7662-680B40-US<br>AP-7662-680B40-WR | AP7662-LEAN-7.3.1.4-003R.img |
| AP-8432-680B30-EU<br>AP-8432-680B30-US<br>AP-8432-680B30-WR   | AP8432-LEAN-7.3.1.4-003R.img |
| AP-8533-68SB30-EU<br>AP-8533-68SB30-US<br>AP-8533-68SB30-WR<br>AP-8533-68SB40-EU<br>AP-8533-68SB40-US<br>AP-8533-68SB40-WR                      | AP8533-LEAN-7.3.1.4-003R.img |
| SA201   | AP391x-10.51.15.0002.img     |
| AP310e-CAN<br>AP310e-FCC<br>AP310e-IL<br>AP310e-WR<br>AP310i-CAN<br>AP310i-FCC<br>AP310i-IL<br>AP310i-WR  | AP3xx-LEAN-7.3.1.4-003R.img  |
| AP3912i-FCC<br>AP3912i-ROW  | AP391x-10.51.15.0002.img     |
| AP3915e-FCC<br>AP3915e-ROW<br>AP3915i-FCC<br>AP3915i-ROW  | AP391x-10.51.15.0002.img     |
| AP3916ic-FCC<br>AP3916ic-ROW  | AP391x-10.51.15.0002.img     |
| AP3916-camera   | AP3916IC-V1-0-14-1.dlf       |
| AP3917e-FCC<br>AP3917e-ROW  | AP391x-10.51.15.0002.img     |

| Product Name   | Image                        |
|--|------------------------------|
| AP3917i-FCC<br>AP3917i-ROW<br>AP3917k-FCC<br>AP3917k-ROW   |                              |
| AP3935e-FCC<br>AP3935e-ROW<br>AP3935i-FCC<br>AP3935i-IL<br>AP3935i-ROW                                   | AP3935-10.51.15.0002.img     |
| AP3965e-FCC<br>AP3965e-ROW<br>AP3965i-FCC<br>AP3965i-ROW   | AP3935-10.51.15.0002.img     |
| AP410e-CAN<br>AP410e-FCC<br>AP410e-IL<br>AP410e-WR<br>AP410i-CAN<br>AP410i-FCC<br>AP410i-IL<br>AP410i-WR | AP4xx-LEAN-7.3.1.4-003R.img  |
| AP460e-CAN<br>AP460e-FCC<br>AP460e-IL<br>AP460e-WR<br>AP460i-CAN<br>AP460i-FCC<br>AP460i-IL<br>AP460i-WR | AP4xx-LEAN-7.3.1.4-003R.img  |
| AP505i-FCC<br>AP505i-WR  | AP5xx-LEAN-7.3.1.4-003R.img  |
| AP510e-FCC<br>AP510e-WR<br>AP510i-FCC<br>AP510i-WR   | AP5xx-LEAN-7.3.1.4-003R.img  |
| AP560h-FCC<br>AP560h-WR<br>AP560i-FCC<br>AP560i-WR   | AP5xx-LEAN-7.3.1.4-003R.img  |
| Switches   |                              |
| 210-12p-10GE2<br>210-24p-10GE2   | 210-series_V1.02.05.0013.stk |

| Product Name   | Image  |
|--|--|
| 210-48p-10GE2<br>210-12p-10GE2 POE<br>210-24p-10GE2 POE<br>210-48p-10GE2 POE   | fp-connector-3.3.0.4.pyz (cloud connector)   |
| 220-12p-10GE2<br>220-24p-10GE2<br>220-48p-10GE2<br>220-12p-10GE2 POE<br>220-24p-10GE2 POE<br>220-48p-10GE2 POE             | 220-series_V1.02.05.0013.stk<br>fp-connector-3.3.0.4.pyz (cloud connector)                       |
| X440G2-12t-10G4<br>X440G2-24t-10G4<br>X440G2-48t-10G4<br>X440G2-12t-10G4 POE<br>X440G2-24t-10G4 POE<br>X440G2-48t-10G4 POE | summitX-30.2.1.8-patch2-5.xos<br>summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector) |
| X620-16x   | summitX-30.2.1.8-patch2-5.xos<br>summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector) |

**NETWORK MANAGEMENT SOFTWARE SUPPORT**

| Network Management Suite (NMS) | Version       |
|--------------------------------|---------------|
| ExtremeManagement™ Center      | 8.4 or higher |
| ExtremeControl™                | 8.4 or higher |
| ExtremeAnalytics™              | 8.4 or higher |

| Air Defense and Location | Version      |
|--------------------------|--------------|
| ExtremeAirDefense™       | 10.3         |
| ExtremeLocation™         | 3.1          |
| ExtremeGuest             | Version      |
| ExtremeGuest™            | 6.0.1.0-001R |

**Note:**

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

**ExtremeCloud Appliance 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 ExtremeCloud Appliance.**

**INSTALLATION INFORMATION:**

| <b>Appliance Installations</b> |   |
|--------------------------------|---|
| E1120                          | <a href="#">ExtremeCloud Appliance E1120 Installation Guide</a>         |
| E2120                          | <a href="#">ExtremeCloud Appliance E2120 Installation Guide</a>         |
| E3120                          | <a href="#">ExtremeCloud Appliance E3120 Installation Guide</a>         |
| VE6120/VE6125                  | <a href="#">ExtremeCloud Appliance VE6120/VE6125 Installation Guide</a> |
| VE6120H                        | <a href="#">ExtremeCloud Appliance VE6120H Installation Guide</a>       |

**PREVIOUS RELEASES EXTREMECLOUD APPLIANCE**

| <b>Enhancements in 04.76.05.0009</b>  |          |
|---|----------|
| Corrected an issue where the AP name was not sent to Extreme Management Center or onboard reports for some events.  | ECA-1210 |
| Improved responsiveness for adding 1000s of MAC addresses to Policy Groups.   | ECA-1231 |
| Removed a delay of 15-20 seconds that was used when displaying error pages for Captive portal-based authentication. | ECA-1719 |
| Addressed an issue with importing 2000 APs using Migration tool on VE6125.  | ECA-1731 |
| Removed the condition that shut down both radios on AP310 after certain config changed.                             | ECA-1739 |
| Rectified false positive reporting of missing NTP server.   | ECA-1817 |
| Corrected a condition that caused unexpected AP rebooting following upgrade of a High-Availability pair.            | ECA-1866 |
| Addressed missing updates of Policy rule-hit counters for SA201.  | ECA-1872 |
| Fine-tuned discovery procedure to correct an issue where AP3915i wouldn't reconnect to the appliance.               | ECA-1893 |
| Improved calculation of traffic throughput and ensured that graph display is correct.                               | ECA-1914 |

| <b>Enhancements in 04.76.04.0005</b>  |                      |
|---|----------------------|
| Addressed issue where platform not applying Roles based on client's identity.   | nse0004425 / ECA-908 |
| Addressed limitation whereby the Auto-Channel Selection (ACS) for AP3900 series only triggers if the access point is directly managed (adopted) by the appliance instance from which the ACS request is issued. | ECA-1605             |
| Addressed issue where actions to "Retrieve Traces" using the graphical user interface failed for the EXOS switches.   | ECA-461              |
| Addressed issue where entering IPv6 address with notation 0:0:0:0:0:0:0:0 converts rule to IPv4 on Save action.   | ECA-1681             |

| <b>Enhancements in 04.76.03.0015</b>  |          |
|---|----------|
| Documented limits for importing Ekahau .SVG files. Documentation addresses issue where importing Ekahau map files results in ExtremeCloud Appliance hanging for a few minutes then logging you out. | ECA-1421 |

|  |          |
|--|----------|
| <p>Please observe the following limits for importing of Ekahau model files:</p> <ul style="list-style-type: none"> <li>-46 MB uncompressed .SVG files on physical appliances.</li> <li>-18 MB uncompressed .SVG files on virtual appliances.</li> </ul> <p>Files larger than these limits will not import on the corresponding appliance as noted.</p> |          |
| Addressed issue where Blacklist/Whitelist not working when network is on AP4xx.  | ECA-1486 |
| Addressed issue where client can't connect to a network with WPA3-Compatibility with PMF Required.   | ECA-1496 |
| Addressed issue where during creating a new network with auth type set to WPA3-Compatibility mode and setting the Protected Management Frames as Required.   | ECA-1488 |
| Addressed incompatibility between Defender for IOT Application (3.31) and ExtremeCloud Appliance 4.76.02.  | ECA-1538 |

| <b>Enhancements in 04.76.02.0035</b>  |          |
|---|----------|
| <p>Re-introduced support for Distributed site deployments through upgrade. Upgrade process grandfathers Distributed sites through upgrade from 4.56 release or configuration import.</p> <p>Settings and assignments for Legacy WiNG (AP75xx, AP76xx, AP8533/8432) or AP5xx models are preserved on upgrade. Grandfathering supports:</p> <ul style="list-style-type: none"> <li>- Creation of new sites (per 4.56 adopted device set)</li> <li>- Adoption of WiNG Legacy or AP5xx devices to existing or new sites</li> <li>- Leveraging auto-adoption rules to Distributed Sites.</li> </ul> <p>Caveats:</p> <p>AP4xx access points are supported in a Centralized site only. AP4xx will not adopt or extend a Distributed site.</p> <p>A fresh installation of 4.76.02:</p> <ul style="list-style-type: none"> <li>- Does not support Distributed sites or adoption of Legacy AP models</li> <li>- AP5xx and AP4xx models adopt only to a Centralized site.</li> </ul> | ECA-1150 |
| <p>Advanced Override option to manually adjust the WLAN assignment configuration per AP radio.</p> <p>Enables customer to adjust radio assignments for specific APs without adjusting the associated configuration Profile. Once overridden, the AP WLAN list is per specific assignment. Override is intended for diagnostics and temporary validation of network settings.</p>  | ECA-450  |
| <p>Site Assigned Adoption - You can override the global load balancing mode for AP adoption, in a High-Availability setup, for a specific Site. Site advanced configuration allows you to specify the appliance, in a High-Availability Pair, to which adopted access points will be homed (Primary Appliance or Backup Appliance). Unless overridden, the default global High-Availability mode (Active-Active or Passive-Active) setting prevails.</p>  | ECA-1152 |
| Consistently use AP Name in Station Events (End-System) reports.  | ECA-1154 |
| <p>Enhancements to Access Point and Client Views:</p> <ul style="list-style-type: none"> <li>- Significantly expanded the list of available information for column display.</li> <li>- Introduced Query Builder utility that enables users to build complex, relational, multi-criteria filters. After executing a query, the distribution rendered is limited to elements returned by the query.</li> <li>- Introduced a new Visualize Column utility represents the values of a particular column as a pie chart. The pie chart displays a distribution of values based on a selected column.</li> </ul>  | ECA-1153 |



|  |          |
|--|----------|
| Support I-SID = 0 to support Fabric Attach Standalone Proxy mode on Extreme Networks Ethernet Routing Switches. Standalone Proxy mode indicates that the network does not include a Fabric Attach Server switch (and therefore does not include a Shortest Path Bridging Fabric Core).   | ECA-964  |
| Provide visual indication of ongoing upgrade operation for managed devices. Status displays blue icon during device upgrade process.   | ECA-918  |
| ExtremeWireless Migration Application is an add-on container application that facilitates migration from ExtremeWireless to ExtremeCloud Appliance. The tool provides a simple interface that allows users to provide a configuration archive for an ExtremeWireless (10.51+) controller. It will extract and import the following:<br>- AP Settings (including AP Name, Description, and radio settings) for AP39xx series access points. AP models not supported by ExtremeCloud Appliance will be ignored.<br>- Policy/Role definitions<br>- VLAN (Topology) settings.<br><b>Contact GTAC for help accessing the Migration Application.</b> | ECA-585  |
| Redesigned appliance Copy Upgrade dialog, providing more intuitive representation of upload methods and enhanced warning of maximum capacity limits for upgrade image storage.   | ECA-84   |
| Update to the channel energy chart.  | ECA-1344 |

| <b>Changes in 04.76.02.0035</b>   | <b>I.D</b> |
|---|------------|
| Addressed issue where WiNG Proxy: Proxied site/AP not displayed after manually deleted from ExtremeCloud Appliance.   | ECA-1199   |
| Addressed issue where RADIUS - Server Status configuration is not applied properly.   | ECA-1028   |
| Addressed issue where upgrading the X440-G2 from the user interface is not supported in ExtremeCloud Appliance v4.76.01 revision. An upgrade to the latest image can be performed through the CLI.  | ECA-1222   |
| During upgrade of a High-Availability Pair configuration to 4.76.01, it is recommended to start the upgrade with the Secondary appliance.   | ECA-1223   |
| Addressed issue where channel occupancy widgets have been abstracted to Radio 1 and Radio 2 to better accommodated representation of dual-5.0GHz devices, such as the AP510/AP560. Older band specific widgets (2.4 GHz and 5.0 GHz) should not be used going forward. Those widgets will be removed in future product updates. | ECA-331    |
| Improved logic on access points for Packet Capture function to address situations that impacted stability.  | ECA-515    |
| Addressed issue where after availability upgrade from 4.56 to 4.76, neither appliance was aware of the AP SW version on the AP page. Displays AP versions only after upgrading the APs to v7.3.0.   | ECA-1217   |
| Addressed issue preventing configuration of WPAv3-Personal. WPAv3-Personal privacy setting on a Network (SSID) will save correctly.   | ECA-1220   |

| <b>Enhancements in 04.76.01.0081</b>   |         |
|--|---------|
| A new LED pattern mode "Normal - Solid" is available. The LED selection on the AP was adjusted to support this new mode, which is now the default mode for APs operating in Centralized Sites. | ECA-712 |
| Support Adoption and Configuration of X465 Switch. VIM Modules are supported. Management through ExtremeCloud Appliance UI, does not support Extended Edge, Stacking or MLAG configurations.   | ECA-647 |

|  |            |
|--|------------|
| Support for AAA Policy definitions: AAA Policy profiles provide a much more detailed configuration of parameters for authentication integration with third-party servers. AAA Policy profiles directly bypass the integrated <i>OnBoard</i> engine.  | ECA-300    |
| Expand definition for Called-Station-ID encoding for authentication integration with external RADIUS server. New formats include the ability to utilize general identifiers such as Site, City or Region as identifiers during user-authentication, facilitating simpler policy constructs for large installations requiring larger/coarse references.   | ECA-300    |
| The AP inventory report was added as a file into the Tech Support Archive.   | ECA-639    |
| Persist customer entered criteria. When user moves from AP or Client List view, to Details view, and back to List view, the criteria and filtering remain intact.  | ECA-630    |
| Enable "Minimize Impact Upgrade" as the default method for AP upgrades.  | ECA-629    |
| The auto-refresh period is now configurable from the user interface. Auto-refresh period is available for intervals of 30 seconds, 1 minute, 3 minutes, and 5 minutes. By default, auto-refresh is OFF.  | ECA-628    |
| All reports for managed devices and attached clients now provide a consistent experience for the Refresh action. The Refresh function is now included on all list pages, beside the Search field option.   | ECA-627    |
| Added support for Agile Multiband for the AP500 and AP400 series access points. Agile Multiband. Multiband Operation (MBO) is configured per network. MBO enables better use of WiFi network resources and improves the roaming experience. It allows the APs and stations to exchange information and facilitates efficient use of multiple frequency bands or channels that are available in the APs and the stations. | ECA-563    |
| Provided the capability for Tech Support to include configuration and log files related to the Onboard server component.   | ECA-562    |
| Supported Adoption and configuration of AP400 series models: <ul style="list-style-type: none"> <li>AP410i-FCC, AP410e-FCC, AP410i-WR, AP410e-WR, AP410i-CAN, AP410e-CAN, AP410i-IL, AP410e-IL</li> <li>AP460i-FCC, AP460e-FCC, AP460i-WR, AP460e-WR, AP460i-CAN, AP460e-CAN, AP460i-IL, AP460e-IL</li> </ul>  | ECA-559    |
| Provided the ability to adjust the Poll-Timeout via the RestAPI. The Poll-Timeout value can be set per Profile and on a per-AP override basis.   | ECA-498    |
| Enhanced granularity of access definitions for administrator accounts. Admin accounts now have granular control over what type of configuration elements can be edited or viewed.  | ECA-451    |
| The Adoption screen allows the user to manually assign a device (AP or Switch) to a specified site. The user is presented with the option to directly create the representative device group if one is not yet defined, or if the device needs a different assignment to better meet the use case.   | ECA-296    |
| Increased the size of a floor plan's geographic representation to 200,000m <sup>2</sup>  | ECA-678    |
| <b>Changes in 04.76.01.0081</b>  |            |
|  | <b>I.D</b> |
| Fabric attach VLANs was not supported as control VLAN for mesh networks. This issue was addressed.   | ECA-578    |

|  |         |
|--|---------|
| Stability improvements for serving 802.1x and 802.11r services are included AP500 series image WiNG 7.2.1.1-06R. (Default AP image with this package). See Release Notes of 7.2.1.1-06R.   | ECA-558 |
| Reboot of the peer ExtremeCloud Appliance is required when availability is configured for the first time to ensure synchronization of configuration of ONBOARD attributes, such as Device Groups. This issue will be addressed in a subsequent release.    | ECA-551 |
| Corrected resource management issue with authentication library that could prevent administrative access to system's graphical user interface.   | ECA-545 |
| Removed limitation to 'AP Test' feature whereby it was only available for channels 1 and 36, for deployments of AP500 series as Extreme AirDefense sensor channels.  | ECA-529 |
| Corrected issue where generating tech support on All, Log, or Wireless AP, the output of the AP inventory would not include all the APs that are configured and the AP BSSIDs.   | ECA-482 |
| After switching from Whitelist mode to Blacklist mode, it's possible for the traffic from the blacklisted client not to be filtered and to be able to connect to different wireless networks and obtain Internet access.<br>This issue has been addressed. | ECA-373 |

| <b>Changes in 04.56.07.0006</b>  | <b>I.D</b> |
|--|------------|
| Updated UI behavior for AP MAC address field to allow selection of value, instead of just simply jump to AP record.  | ECA-1174   |
| Improved synchronization logic for statistics engine components to avoid possible representation of time series graphs with a 'saw' pattern.   | ECA-1167   |
| Updated floorplan logic to address issue with imported Ekahau models that contained references to 0 length lines, which could affect ability to save modifications such as boundary adjustments. | ECA-1166   |
| Provided representation of connection uptime for APs in Distributed Sites.   | ECA-1164   |
| Improved session management logic to better account for re-associations of clients during the Hold-down time (30 secs) following the client's explicit DISCONNECT request from the network.      | ECA-1133   |
| Corrected logic bug with time range filtering in <i>Station Events</i> reporting.  | ECA-1082   |
| Adjusted configuration logic for Client Ports, such as AP7612, to ensure that traffic to client ports is always untagged, regardless of whether VLAN traffic is tagged on the AP's uplink port.  | ECA-1016   |
| Corrected issue preventing the definition of Customer Layer 7 rules for user access control.   | ECA-975    |

| <b>Changes in 04.56.06.0013</b>   | <b>I.D</b> |
|---|------------|
| Corrected issue for consistent display of BSSID for network assignments on APs.   | ECA-1060   |
| Improved error handling for End-System session re-sync operations to address and prevent possible cyclic race-conditions when addressing session state discrepancies. | ECA-1081   |
| Corrected issue with handling of configuration for large channel widths that could result in the radio not starting correctly.  | ECA-1065   |
| Corrected issue with display of widgets for Top Sites by Channel Utilization/SNR charts displaying "Undefined".   | ECA-1057   |

| Changes in 04.56.06.0013   | I.D     |
|--|---------|
| Improved resilience of UI server to better address possible delays on initial startup.   | ECA-995 |
| Corrected behavior to restart AP when management connectivity lost and session persistence option is disabled.                     | ECA-972 |
| Updated description of client Whitelisting behavior, especially calling out impact of empty lists.                                 | ECA-971 |
| Updated UI representation of Events to support custom column sizing.   | ECA-927 |
| Addressed logic flaw that could result in resetting of WLAN assignments to <i>Profiles</i> after modifications to network setting. | ECA-912 |
| Improved consistency display of assigned RF Policy for Access Points for UI refresh.   | ECA-879 |
| Fixed a race condition, where RADIUS CoA-Request would not get ACK'ed by Controller while client is roaming to new AP.             | ECA-807 |

| Changes in 04.56.05.0005   | I.D     |
|--|---------|
| Corrected an issue with the evaluation of policies pushed from PolicyManager for Distributed Sites.  | ECA-856 |
| Corrected column labeling for Access Point display to reflect radio ID instead of operational frequency band.  | ECA-855 |
| Hardened logic for IP Address reporting for RADIUS accounting to address possible "race condition" (when two events happen at the same time) when clients switch networks. | ECA-840 |
| Corrected configuration option for AP500 series to enable AutoLogin Captive Portal detection by default.   | ECA-764 |
| Adjusted reporting of "Last Seen" timestamp for Clients to correspond with time of last status update vs presence in the session's table.                                  | ECA-750 |
| Improved handling and protection against possible corruption of client hostnames with non-printable characters, which could cause stats processing to stall.               | ECA-699 |

| Changes in 04.56.04.0009  | I.D     |
|---|---------|
| Corrected issue affecting the reporting of statistics in Proxy mode for WiNG controllers with serial numbers different than 14 or 16 characters long. | ECA-760 |
| Improved display of Max Transmit power setting to be scoped to regulatory allowed range of <i>Requested Channel</i> .                                 | ECA-682 |
| Enhanced configuration view of access points to display value of requested channel.   | ECA-680 |
| Improved efficiency of <i>Client</i> list views in the UI when rendering a larger number of clients.  | ECA-751 |
| Addressed issue with representation of Site status, for sites that only manage switches.  | ECA-655 |
| Corrected issue that was preventing column resizing for <i>Client</i> views.  | ECA-686 |
| Improved logic handling on Access Point management to protect against possible issues due to fragmented exchanges.                                    | ECA-709 |
| Corrected issue with offset index for interface ID in CTAlias SNMP table.   | ECA-734 |
| Addressed issue with client registration for ExtremeCloud Appliance extension of ExtremeWireless Inter-Access Controller mobility domain.             | ECA-711 |
| Adjusted default behavior for RADIUS Accounting Start to trigger after client obtains an IP address.  | ECA-743 |

| Changes in 04.56.03.0004   | I.D     |
|--|---------|
| Addressed issue with Synchronization of Session Information across both HA peers, which could affect the ability of a client to roam across APs without re-authenticating when 802.11r configured. | ECA-656 |
| Corrected UI display issue where IP mask and Default Gateway IP addressed for AP7632 may be reported as 0.0.0.0.   | ECA-654 |

### Known Restrictions and Limitations:

| Known Restriction or Limitation   | I.D      |
|---|----------|
| Reconfiguration of Link aggregation (LAG) may be needed after upgrade to 4.76.06.   | ECA-1979 |
| The names of Captive portal WLANs should be shorter than 29 characters. Longer names could cause upgrade failure and loss of configuration.   | ECA-2175 |
| To make NAS-IP identifier more deterministic, 4.76 changes the default behavior from using an internal topology bound interface (typically 127.x.x.x range) to referencing the IP address of the Admin port. If authentication policy in external servers is conditional on NAS IP address, you can transition to use a corresponding AAA policy and configuring the NAS IP to be reported as the same value as previously used with 4.56 (or earlier)  | ECA-1867 |
| AP310 models are not currently supported by ExtremeLocation(TM). Do not enable ExtremeLocation settings in the Profile configurations for AP310 device groups. Doing so may have a negative impact on AP performance.   | ECA-1620 |
| When AP510e works as dual band concurrent data forwarder - operation mode 1 – to avoid confusion it is recommended to disable group 2 antennas, port 5-8.   | ECA-1074 |
| 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 XCAs are configured in availability pair. If the primary XCA is going down, then the EXOS switches will not send statistics to the backup XCA and will be marked in red "Critical" state. When the primary XCA is coming up again, then the switches will resume sending statistics information to the primary XCA and the state of the switch will be marked with a green "Running" state | ECA-455  |
| Monitor Networks under Distributed Network, Meshpoint is missing Channel information. This problem will be addressed in a future release.   | ECA-566  |
| Editing or Deleting Control VLAN under the Mesh Network is not possible. This problem will be corrected into a future release.  | ECA-573  |
| 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  |
| For ExtremeCloud Appliance installations 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 |
| Policy rules applied to AP7632 users do not produce expected results. This issue will be resolved in a future release.  | ECA-238  |

| Known Restriction or Limitation  | I.D      |
|--|----------|
| <p>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).</p> <p>Users reconnect immediately back 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.</p> <p>This issue is being investigated and will be addressed in future releases.</p> | ECA-1264 |
| <p>GUI Mesh Report is missing the information about Root AP with Ethernet connection. This problem will be addressed in a future release.</p>  | ECA-565  |
| <p>Widgets do not show tooltips for Lower and Upper values. This issue will be addressed in a future release.</p>  | ECA-567  |
| <p>In SmartRF mode, the AP 510 power may drop to 0dBm and returns to 4dBm.</p>   | ECA-469  |
| <p>Upgrade failure will occur when using special characters (escape back slash) in topology.</p>   | ECA-466  |
| <p>Policy rules applied to AP7632 users do not produce expected results. This issue will be resolved in a future release.</p>  | ECA-238  |
| <p>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).</p> <p>Users reconnect immediately back 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.</p> <p>This issue is being investigated and will be addressed in future releases.</p> | ECA-1264 |
| <p>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.</p>  | ECA-321  |
| <p>For ExtremeCloud Appliance installations configured for authentication of administrators over RADIUS server, the GUI responsiveness may be slow, possibly over 30 seconds, if target server(s) are unavailable/un-reachable at login time. If outage is extensive, system will eventually timeout to validate against local credentials, if so provisioned.</p>   | ECA-1396 |
| <p>GUI Mesh Report is missing the information about Root AP with Ethernet connection. This problem will be addressed in a future release.</p>  | ECA-565  |
| <p>Monitor Networks under Distributed Network, Meshpoint is missing Channel information. This problem will be addressed in a future release.</p>   | ECA-566  |
| <p>Editing or Deleting Control VLAN under the Mesh Network is not possible. This problem will be corrected into a future release.</p>  | ECA-573  |
| <p>When AP510e works as dual band concurrent data forwarder - operation mode 1 – to avoid confusion it is recommended to disable group 2 antennas, port 5-8.</p>   | ECA-1074 |
| <p>Firmware for ExtremeWireless AP3900 series Access Points does not currently support Smart RF and therefore no Smart RF data is displayed.</p>   | ECA-1484 |
| <p>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</p>  | ECA-455  |

| Known Restriction or Limitation   | I.D             |
|---|-----------------|
| 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, then 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.  |                 |
| Widgets do not show tooltips for Lower and Upper values. This issue will be addressed in a future release.  | ECA-567         |
| In SmartRF mode, the AP510 power may drop to 0dBm and returns to 4dBm.  | ECA-469         |
| Special Characters such as “ @ ; / \ ” I must not be used in configuration fields of ExtremeCloud Appliance, when configuring entities such as (AP, Topology, Site, Network, etc.). Some of those characters are treated as control or escape characters. Using special characters in text fields can result in problems when exporting the system configuration and lead to failures on configuration import, such as during a system upgrade.   | Info<br>ECA-466 |
| Recommendation settings for setup of redundant RADIUS server authentication:<br>1) Response Window to 5s [Default: 20s]<br>2) Revival Interval to 10s [Default: 60s]  | Info<br>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.<br><br>During upgrade periods, the Availability link will only re-establish when both the appliance status of availability link and synchronization status can be found: <ul style="list-style-type: none"> <li>• “Network Health” widget on Dashboard</li> <li>• Administration -&gt; System -&gt; Availability</li> </ul>  | Info<br>ECA-776 |
| 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.<br>See:<br><a href="https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html">https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html</a><br><br>See KB<br><a href="https://gtacknowledge.extremenetworks.com/articles/Solution/AP510-Unable-to-see-the-SSID-on-my-laptop">https://gtacknowledge.extremenetworks.com/articles/Solution/AP510-Unable-to-see-the-SSID-on-my-laptop</a><br><br>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.<br><br>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        |
|---|------------|
| Appliances in a High-Availability pair must be 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 any configuration changes to one of the members of a High-Availability pair while the peer has a different software revision. | nse0005086 |
| Please allow at least 20 seconds between stopping and re-starting a packet capture on a Site.   | nse0004124 |
| ExtremeGuest support will be finalized in the next maintenance release and by the release of eGuest server 6.0.   |            |
| 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.   | nse0003529 |
| Wired packet captures for APs in Campus Sites may take up to 1 minute to show results. This issue will be addressed in a subsequent release.  | nse0004545 |
| Client Badge in a Floor plan may not show correctly. This issue will be addressed in a subsequent release.  | nse0004565 |
| For Off Channel Scan to work on Distributed APs, 'Smart Monitoring' should be disabled in a Smart-RF profile.   | nse0004568 |
| When configuring system for NTP time assignment, ensure that 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 |
| Multicast rules for Topologies (VLANs) are only enforced on Centralized Site deployments (ExtremeWireless APs). The multicast rules are not enforced by Distributed Sites (ExtremeWirless WiNG APs). Topology assignment in Distributed Sites does not filter multicast. Therefore, traffic is bridged between wireless and wired). AP76xx, AP8432, and AP8533 bridge all multicast traffic from wired to wireless network.   | Info       |
| For service authentication in Distributed Sites (ExtremeWireless WiNG), the Default Unauth Role is applied if the configured RADIUS server can't be reached for authentication. The MBA Timeout Role configured for an MBA network is not applied to an End Client (Mobile Unit [MU]) session.  | Info       |
| <p>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.</p> <p>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.</p>  | nse0003416 |
| Interaction with ExtremeManagement Center – Management of ExtremeCloud Appliance by ExtremeManagement Center will be enhanced over time with the roadmap. ExtremeManagement Center v8.4 is the minimum release base for integration. Version 8.4 provides recognition of an ExtremeCloud Appliance and representation of Wireless Clients and managed Access Points included in the Wireless tab.   | Info       |



| Known Restriction or Limitation   | I.D        |
|---|------------|
| Additional integration will be delivered in upcoming releases. ExtremeManagement Center 8.4 is the current recommended minimum release.   |            |
| 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 reevaluate the rule engines.<br>This situation will be addressed in a future release.  | nse0003279 |
| Wireless capture on Wing APs may return the wrong packet captures containing wired packets and wireless packets only for uplink.<br>This situation will be addressed in a future release.   | nse0002243 |
| 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       |
| Device Level Country override is not supported for WiNG Proxy Mode. Only one country-code assignment per site is supported. All APs at the site must match the same country.  | Info       |
| 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.   | nse0004445 |
| The GUI set action "Retrieve Traces" might fail for the EXOS switches. Repeat setting the "Retrieve Traces" action until the switch uploads the logs and traces the tar file to the ExtremeCloud Appliance.   | nse0004866 |
| Currently fabric attach VLANs are not supported as control VLAN for mesh networks.  | nse0005152 |
| 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.  | nse0005045 |
| Stability improvements for serving 802.1x and 802.11r services are included AP500 Series image WiNG 7.2.1.1-06R. (Default AP image with this package). See Release Notes of 7.2.1.1-06R.  | nse0005125 |
| Upgrade failure will occur when using special characters (escape back slash) in topology.   | nse0004876 |
| An AP crash will occur when starting packet capture from ExtremeCloud Appliance. This problem will be resolved by the 7.3.0 Wing AP release.  | nse0005010 |
| Simultaneous Backup tunnel High-Availability is only enabled for Access Points deployed in Centralized sites.<br>The Network Health widget on the main dashboard, will only count APs in distributed site against their actual connectivity state (Attached to either Primary or Backup controller). The connectivity counters will therefore only reflect (count) the active tunnel. | nse0004956 |
| GUI Mesh Report is missing the information about Root AP with Ethernet connection. This problem will be addressed in a future release.  | nse0005134 |
| In the 3120 Platform, sometimes time series legend for non-empty charts are shown as 'NoData'.  | nse0005137 |
| An issue was observed for AP7632 where the Tunnel-Private-Group-ID value is not used or ignored, and client receives the Default Role.  | nse0005030 |
| Policy rules applied to AP7632 users do not produce expected results. This issue will be resolved in a future release.  | nse0004045 |

| Known Restriction or Limitation   | I.D        |
|---|------------|
| Editing or deleting Control VLAN under the Mesh Network is not possible. This problem will be corrected into a future release.  | nse0005144 |
| After switching from Whitelist mode to Blacklist mode traffic there is the possibility for the traffic from the blacklisted client not to be filtered and be able to connect to different wireless networks and obtain Internet access.<br><br>This problem will be resolved in the next release. | nse0004572 |
| Reboot of the peer ExtremeCloud Appliance 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.                                       | nse0005113 |
| Corrected resource management issue with authentication library that could prevent administrative access to system's graphical user interface.  | nse0005101 |
| 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.   | nse0005065 |
| ExtremeCloud Appliance user accounts created in the pre-registration page do not propagate to the AAA policy.   | nse0005028 |
| Monitor Networks under Distributed Network, Mesh point is missing channel information. This problem will be addressed in a future release.  | nse0005135 |

**SUPPORTED WEB BROWSERS**

For ExtremeCloud Appliance 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                             |
| Safari         | Preinstalled with iOS 12.2  | iOS 12.2                               |
| Safari         | Preinstalled with iOS 9.3.5 | iOS 9.3.5                              |
| Microsoft Edge | 42.17134                    | Windows 10                             |
| Microsoft IE   | 11                          | Windows 7<br>Windows 8.1<br>Windows 10 |
| Chrome         | 75.0.37770.142              | Windows 7<br>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 |
|---|--------------|--------------------|----------|------------|---------------|---|---------------------|
| <b>Ports for AP/Appliance Communication</b> |              |                    |          |            |               |   |                     |
| 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            |

| Comp. Source  | Comp. Dest   | Protocol (TCP/UDP) | Src Port | Dest Port     | Service        | Remark                                      | Open Firewall Req'd |
|---|--------------|--------------------|----------|---------------|----------------|---|---------------------|
| 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            |
| <b>Ports for Appliance Management</b>                                   |              |                    |          |               |                |   |                     |
| 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                 |
| <b>Ports for Inter Controller Mobility<sup>1</sup> and Availability</b> |              |                    |          |               |                |   |                     |
| 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                 |

<sup>1</sup>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                          | 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                 |
| <b>Core Back-End Communication</b> |                  |                    |          |           |   |   |                     |
| 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            |

**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<br>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 | ExtremeCloud Appliance connection |
| Extreme | X440G2-48p-10G4 | 21.1.1.4 | ExtremeCloud Appliance connection |
| Extreme | Summit 300-48   | 7.6e1.4  | ExtremeCloud Appliance connection |

|         |                  |  |                                   |
|---------|------------------|--|-----------------------------------|
| Extreme | VSP-4850GTS-PWR  | (6.0.1.1_B003) (PRIVATE) HW Base: ERS 4850 | ExtremeCloud Appliance connection |
| Extreme | K6               | 08.63.02.0004                              | ExtremeCloud Appliance connection |
| Extreme | K6               | 08.42.03.0006                              | ExtremeCloud Appliance connection |
| Extreme | X440G2-48p-10GE4 | 21.1.5.2                                   | ExtremeCloud Appliance connection |
| Extreme | X440-G2-12p      | 21.1.1.4                                   | ExtremeCloud Appliance connection |
| Extreme | X460-48p         | 12.5.4.5                                   | ExtremeCloud Appliance connection |
| Cisco   | Catalyst 3550    | 12.1(19)EA1c                               | ExtremeCloud Appliance 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 |



| Attribute          | RFC Source                   |
|--------------------|------------------------------|
| 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](mailto: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.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners. Extreme Networks IPS includes software whose copyright is licensed from MySQL AB.

For additional information on Extreme Networks trademarks, please see: [www.extremenetworks.com/company/legal/trademarks/](http://www.extremenetworks.com/company/legal/trademarks/)