

# Customer Release Notes

## ExtremeCloud Appliance

Firmware Version V4.36.03.0006

June 7, 2019

### 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 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.

| <b>Enhancements in 4.36.03.0006</b>  |
|--|
| Extended SmartRF support to AP500 series assigned to Centralized sites. Requires upgrade of AP500 series devices to WiNG 7.1.2 (included) or newer.  |
| Extended support to adoption and management of AP560 series models and bundle variants. Bundle variants (M,T,U) provide AP packaging and mounting options in one convenient package. Adoption is based on the underlying AP model: AP560i/m/u adopt as AP560i; AP560h/t adopt as AP560t. |
| Exposed support for legacy privacy setting networks, such as WEP and WPA2-TKIP.  |
| Introduced support for Client Load Balancing on AP500 Series assigned into Centralized Sites.  |
| Enabled support for IOT transmit functions (iBeacon, Eddystone beacons) for AP500 Series.  |

| <b>Changes in 4.36.03.0006</b>                                   | <b>I.D</b> |
|--|------------|
| Corrected UI issue with alignment of editing function for Roles. | nse0004290 |

**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:**

| <b>Status</b>    | <b>Version No.</b> | <b>Type</b>         | <b>Release Date</b> |
|------------------|--------------------|---------------------|---------------------|
| Current Version  | V.04.36.03.0006    | Maintenance Release | June 7, 2019        |
| Previous Version | V.04.36.02.0014    | Feature Release     | May 03, 2019        |

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

| <b>Product Name</b>  | <b>Image</b>                 |
|--|------------------------------|
| ExtremeCloud Appliance VE6120 VMware<br>(Supported ESXi is 5.1; tested 5.5; 6.0; 6.5)  | ECA-04.36.03.0006-1.dle      |
| ExtremeCloud Appliance E1120   | ECA-04.36.03.0006-1.sme      |
| ExtremeCloud Appliance E2120   | ECA-04.36.03.0006-1.jse      |
| ExtremeCloud Appliance E3120   | ECA-04.36.03.0006-1.ose      |
| <p><b>Note: The minimum release dependency for WiNG APs is ExtremeWireless WiNG v5.9.2.2. WiNG APs must be manually upgraded to v5.9.2.2 or above before being adopted by ExtremeCloud Appliance. After upgrade, reset the WiNG AP to the factory settings. For more information, see GTAC article: <a href="#">ExtremeCloud Appliance - WiNG AP will not connect to ExtremeCloud Appliance</a>.</b></p> |                              |
| AP-7522-67030-US   | AP7522-LEAN-5.9.3.3-004R.img |

| Product Name  | Image                        |
|---|------------------------------|
| AP-7522-67030-WR<br>AP-7522-67030-1-WR<br>AP-7522-67030-EU<br>AP-7522E-67030-US<br>AP-7522E-67030-WR<br>AP-7522E-67030-EU<br>AP-7522-67040-US<br>AP-7522-67040-WR<br>AP-7522-67040-1-WR<br>AP-7522-67040-EU<br>AP-7522E-67040-US<br>AP-7522E-67040-WR<br>AP-7522E-67040-EU  |                              |
| AP-7532-67030-US<br>AP-7532-67030-WR<br>AP-7532-67030-1-WR<br>AP-7532-67030-EU<br>AP-7532-67030-EG<br>AP-7532-67030-IL<br>AP-7532-67040-US<br>AP-7532-67040-WR<br>AP-7532-67040-1-WR<br>AP-7532-67040-EU<br>AP-7532-67040-EG  | AP7532-LEAN-5.9.3.3-004R.img |
| AP-7562-6704M-US<br>AP-7562-6704M-WR<br>AP-7562-6704M-1-WR<br>AP-7562-6704M-EU<br>AP-7562-67040-US<br>AP-7562-67040-WR<br>AP-7562-67040-1-WR<br>AP-7562-67040-EU<br>AP-7562-670042-US<br>AP-7562-670042-WR<br>AP-7562-670042-1-WR<br>AP-7562-670042-EU<br>AP-7562-670042-IL | AP7562-LEAN-5.9.3.3-004R.img |
| AP-7612-680B30-US<br>AP-7612-680B30-WR  | AP7612-LEAN-5.9.3.3-004R.img |
| AP-7632-680B30-US<br>AP-7632-680B30-WR<br>AP-7632-680B40-US<br>AP-7632-680B40-WR  | AP7632-LEAN-5.9.3.3-004R.img |
| AP-7662-680B30-US<br>AP-7662-680B30-WR<br>AP-7662-680B40-US<br>AP-7662-680B40-WR  | AP7662-LEAN-5.9.3.3-004R.img |
| AP-8533-68SB30-US<br>AP-8533-68SB30-WR  | AP8533-LEAN-5.9.3.3-004R.img |

| Product Name  | Image  |
|---|--|
| AP-8533-68SB30-EU<br>AP-8533-68SB40-US<br>AP-8533-68SB40-WR<br>AP-8533-68SB40-EU  | AP8533-LEAN-5.9.3.3-004R.img   |
| AP-8432-680B30-US<br>AP-8432-680B30-WR<br>AP-8432-680B30-EU   | AP8432-LEAN-5.9.3.3-004R.img   |
| <p>NOTE:<br/>All AP75xx family access points use binary image AP7532-LEAN-5.9.x.x-xxxR.img.<br/>AP7632 and AP7662 access points use binary image AP7632-LEAN-5.9.x.x-xxxR.img.<br/>During an image upload, the GUI requires that the name of the binary image matches the name of the AP type.<br/>Therefore, a manual rename of the binary image is necessary.</p> |  |
| AP3912i-FCC<br>AP3912i-ROW  | AP391x-10.51.04.0009.img   |
| SA201   | AP391x-10.51.04.0009.img   |
| AP3915i-FCC<br>AP3915e-FCC<br>AP3915i-ROW<br>AP3915e-ROW  | AP391x-10.51.04.0009.img   |
| AP3916i-FCC<br>AP3916i-ROW  | AP391x-10.51.04.0009.img   |
| AP3916-camera   | AP3916IC-V1-0-14-1.dlf   |
| AP3917i-FCC<br>AP3917e-FCC<br>AP3917i-ROW<br>AP3917e-ROW  | AP391x-10.51.04.0009.img   |
| AP3935i-FCC<br>AP3935e-FCC<br>AP3935i-ROW<br>AP3935e-ROW  | AP3935-10.51.04.0009.img   |
| AP3965i-FCC<br>AP3965e-FCC<br>AP3965i-ROW<br>AP3965e-ROW  | AP3935-10.51.04.0009.img   |
| AP505i-FCC<br>AP505i-WR<br>AP510i-FCC<br>AP510i-WR<br>AP560i-FCC<br>AP510e-FCC<br>AP510e-WR   | AP5xx-LEAN-7.1.2.0-015R.img  |
| Switches  |  |
| 210-12p-10GE2<br>210-24p-10GE2<br>210-48p-10GE2<br>210-12p-10GE2 POE<br>210-24p-10GE2 POE   | 210-series_V1.02.05.0013.stk<br>fp-connector-3.3.0.4.pyz (cloud connector) |

| Product Name   | Image  |
|--|--|
| 210-48p-10GE2 POE  |  |
| 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-22.6.1.4.xos<br>summitX-cloud_connector-3.3.1.9.xmod (cloud connector) |
| X620-16x   | summitX-22.6.1.4.xos<br>summitX-cloud_connector-3.3.1.9.xmod (cloud connector) |

**NETWORK MANAGEMENT SOFTWARE SUPPORT**

| Network Management Suite (NMS) | Version   |
|--------------------------------|---|
| ExtremeManagement™ Center      | 8.1.4.27 or higher<br>8.2.3 required for SA201 and AP75xx visualization<br>8.2.5 recommended for PolicyManager coordination |
| ExtremeControl™                | 8.1.4.27 or higher (per ExtremeManagement Center release)   |
| ExtremeAnalytics™              | 8.1.4.27 or higher (per ExtremeManagement Center release)   |

| Air Defense and Location | Version       |
|--------------------------|---------------|
| ExtremeAirDefense™       | 9.5 or higher |
| ExtremeLocation™         | 1.2 or higher |

**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:**

| Appliance Installations |  |
|-------------------------|--|
| 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                  | <a href="#">ExtremeCloud Appliance VE6120 Installation Guide</a> |
| VE6120                  | <a href="#">ExtremeCloud Appliance VE6120 Installation Video</a> |

**PREVIOUS RELEASES EXTREMECLOUD APPLIANCE**

| Enhancements in 4.36.02.0014  |
|---|
| Change default configuration settings to have 802.11w (Protect Management Frame [PMF]) not enabled by default. Customer can re-enable as required under the Network/SSID's Privacy Settings configuration. Please refer to the Known Restrictions and Limitations: section for possible interoperability issues in combination with 802.11r for several client types.   |
| Introducing support for the E3120, an 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. This release includes validated support for up to 50,000 users in an availability pair. Validation for full 100,000 target capacity will be committed into next minor release. |
| Introducing a set of widgets that provide visibility per Policy/Role on the impact of the defined access rule set (ACL). Available for Centralized sites only.  |
| Introducing support for AP560i and variant (AP560u).  |

| Changes in 4.36.02.0014   | I.D        |
|---|------------|
| Addressed issues with not reporting channel occupancy (WiNG AP only). | nse0003232 |

|  |            |
|--|------------|
| Addressed the situation where GUI packet capture state did not indicate active when the underlying capture was active. | nse0004160 |
| Addressed the situation where GUI could not start a new capture after a packet capture ended.                          | nse0004210 |

| <b>Enhancements in 4.36.01.0097</b>  |  |
|--|--|
| Improves the UI look and feel, separating Monitoring and Configuration functions, and acceleration of Network to Profile assignments.  |  |
| Introduces the configuration Workflow tool, that allows navigation of the system's configuration model in a relational manner. Alternatively, provides a method to directly access any named configuration object in the system.   |  |
| Supports the new WiFi 6 (802.11ax) APs, the AP505i and AP510i models, which introduce also the WiNG 7.1.0 unified AP firmware.   |  |
| Extends ExtremeCloud Appliance as a wireless statistics collector for existing WiNG installations (5.9.1 minimum requirement). Consolidated wireless statistics are leveraged into ExtremeManagement Center's visualization, reporting, and alerting capabilities from ExtremeWireless WiNG installations. This enables deployment of ExtremeManagement Center in holistic and ubiquitous wireless and wired installations. Requires ExtremeManagement Center 8.2.5 or later release.  |  |
| Improves value proposition for directly managed switches by managing the authentication requirements for individual switch ports, providing support for 802.1x or Mac Based Authentication (MBA) against a definable set of site-local reachable RADIUS Servers. RADIUS accounting is similarly configurable.  |  |
| Improves manageability of clients with weak signals or sticky clients. Exposes a per <i>Profile</i> threshold for Received Signal Strength. Can optionally disassociate clients who are moving away from the AP and whose signal has fallen below the defined threshold level. Not responding to and disconnecting weaker clients (aka sticky clients) typically improves the performance of a high-density network. It reduces the burden on the AP that is caused by inherent lower speed links and high error rates associated with those weaker clients. It also improves the chances that the client associates with an AP to which it can establish a stronger bond. Threshold level should be carefully selected in relation to the noise floor and optimal coverage level of the deployment. The threshold level is best determined through a Site survey. |  |
| Enhances support for high-density environments where several APs may be required to cover the same area to address user capacity totals through support for Client Load Balancing. Client Load Balancing is enabled as an advanced <i>Profile</i> setting. Once enabled, member APs of the <i>Device Group</i> essentially form a load balancing group that shares load information and evenly distributes associated user load across the group. Because radio service <i>Profiles</i> are device specific, all APs in a load balancing group ( <i>Device Group</i> ) will be of the same model. Combining different AP models into the same device group is not supported.   |  |
| Enhances flexibility of policy definitions by separating the VLAN assignment from the Policy ( <i>Role</i> ) default action. This adjustment allows for the definition of a catch-all VLAN containment for all traffic allowed by whitelisting within a role, even when the default action is "DENY". This split, provides for easier definition of VLAN segmentation defaults for restrictive roles.  |  |
| Expands Packet Capture diagnostics facility to support up to 10 simultaneous packet captures. Allows the ability to reduce the number of bytes per captured frame, to facilitate longer capture periods and address privacy concerns associated with data payloads.  |  |
| Provides better compatibility options for customers with existing RADIUS authentication server deployments, configured to expect different formats for the end-system's mac address, typically carried in the Calling-Station-ID field in MBA and 802.1x RADIUS authentication requests. Administrator can select which format matches their server's configuration from the <i>MAC Format</i> drop down menu, under the Administration System Settings area. The format setting is global and will apply to any authentication requests performed through the appliance into any of the defined external RADIUS servers.  |  |

| <b>Enhancements in 4.36.01.0097</b>   |
|---|
| Exposes support to directly instantiate and manage general Docker Containers via the Appliance user interface. Allows the user to complement the ExtremeCloud Appliance's native functionality by downloading and installing add-on applications from public repositories, such as Docker Hub. Supports only numerically versioned Containers (alphabetic characters or '.latest' is not supported).  |
| Increases the maximum size of a Distributed mobility site to 256 APs.   |
| Validated interoperability with ExtremeManagement Center™'s Policy Management coordination feature. Required ExtremeManagement Center 8.2.5 or latest revision. Validated and documented integration with ExtremeControl™ for delegated authentication value add or integration into existing environments for dynamic policy assignment or guest onboarding via Captive Portal.<br>Please refer to "ExtremeCloud Appliance Deployment Guide" for more details. |

| <b>Changes in 4.36.01.0097</b>  | <b>I.D</b> |
|---|------------|
| Addressed "Invalid Configuration Request" in ExtremeCloud Appliance log for SA201s in Defender configuration.             | nse0003725 |
| Addressed the problem where WiNG AP did not support duplicate application IDs per role.                                   | nse0003683 |
| Addressed the issue where 200 Series switches did not support redundancy for management connections.                      | nse002870  |
| Addressed an issue where representation of Base channel for bonded operation (40 Mhz or 80Mhz) was displayed incorrectly. | nse0002419 |

**KNOWN RESTRICTIONS AND LIMITATIONS:**

| <b>Known Restriction or Limitation</b>  | <b>I.D</b> |
|---|------------|
| Possible pollution of IPv6 segment for clients on AP500 Series APs. IPv6 RA are transmitted as multicast (all users) therefore can cause incorrect assignment across different networks. Recommend disabling IPv6 until issue is corrected in upcoming release.   | nse0004062 |
| After creating a new floorplan/map, the view panel will refresh to the first floorplan in the site; not necessarily the actual floorplan that was just edited. This issue will be addressed in a subsequent release   | nse0004350 |
| Enabling Appliance as 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 |
| For WiNG Proxied Site configurations the Clients and AP listings, exposes a list of actions, such as Disconnect Client or Upgrade AP. ExtremeCloud Appliance does not enforce control over Proxied information. ExtremeCloud Appliance provides statistics visualization for such deployments. The of available actions has no impact on the represented devices. These superfluous actions that would apply to directly attached/managed devices have no action and will therefore be removed from Proxy-type Sites in a subsequent release. | nse0004284 |
| Operational band labels related widgets are reversed for AP500 series devices, for example Channel utilization on 2.4 and 5.0 GHz. This issue will be addressed in a subsequent release update.   | nse0004503 |



|   |                   |
|---|-------------------|
| In order for AP name to appear as hostname or device prompt it must follow the following rules:<br><ol style="list-style-type: none"> <li>1. Length from 2 to 24 characters</li> <li>2. Starts with letter</li> <li>3. Ends with letter or number</li> <li>4. Contains only letters, numbers '.' or '-'</li> </ol>  | nse0004510        |
| If a network s referenced in a Policy rule (Location constraint) assignment and the Network name is changed the corresponding rules are not updated. Affected rules must be directly adjusted to refer to the new name. This issue will be addressed in a subsequent release.   | nse0004544        |
| Packet captures for APs in Distributed Sites may take up to 1 minute to show results. This issue will be addressed in a subsequent release.   | nse0004545        |
| SNMP settings applicable to managed switches in a Site, will be lost after appliance upgrade or configuration restore. This issue will be addressed in a subsequent release.  | nse0004562        |
| Client Badge in Floorplan may not show correct. This issue will be addressed in a subsequent release.   | nse0004565        |
| Combining RadioShare and Off-Channel-Scanning (OCS) for APs in Distributed Sites is not currently supported. This issue will be addressed in a subsequent release.  | nse0004568        |
| No updates to ExtremeLocation for APs in Distributed Sites, when Profile configuration also includes AirDefense integration. This issue will be addressed in a subsequent release   | nse0004576        |
| U iBeacon/Eddystone listener (remote reporting of iBeacon/Eddystone beacons over UDP) function not supported in this release (4.36.03). Support will be re-introduced in an upcoming release  | nse0004583        |
| Smart RF function for AP500s in Campus mode may stall following a reboot or software upgrade. Issue will be addressed in a subsequent release.<br>Workaround: If stall suspected, toggle the “Smart Monitoring” setting (off-on) under “Profile: Policy Management Policy: Scanning” tab. This issue will be addressed in a subsequent release.   | nse0004584        |
| Voice and Power Save awareness settings not currently supported. Correct settings will not persist correctly. This issue will be fixed in a subsequent release.   | nse0004405        |
| Preservation of system settings may be affected when upgrading the operational category ( such as promoting from Small to Medium to Large capacity levels) of a VE6120. Recommend to always generate and persist off-box a copy of the system configuration before adjusting the resource level in the hypervisor.  | nse0004604        |
| 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.   | Info - 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   | Info              |

|   |                |
|---|----------------|
| <p>authentication. The MBA Timeout Role configured for an MBA network is not applied to an End Client (Mobile Unit [MU]) session.</p>   |                |
| <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>                                      | Info nse003416 |
| <p>Interaction with ExtremeManagement Center – Management of ExtremeCloud Appliance by ExtremeManagement Center will be enhanced over time with the roadmap. ExtremeManagement Center v8.1.4 is the minimum release base for integration. Version 8.1.4 provides recognition of an ExtremeCloud Appliance and representation of Wireless Clients and managed Access Points included in the Wireless tab.</p> <p>Additional integration will be delivered in upcoming releases. ExtremeManagement Center 8.2.5 is the current recommended minimum release.</p> | Info           |
| <p>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.</p> <p>This situation will be addressed in a future release.</p>   | nse0003279     |
| <p>Wireless capture on Wing APs may return the wrong packet captures containing wired packets and wireless packets only for uplink.</p> <p>This situation will be addressed in a future release.</p>  | nse0002243     |
| <p>Wing APs do not yet support Availability failover. In a High-Availability configuration, the WiNG AP will only connect to the appliance instance it discovers. During a service interruption of its primary controller, stats from such APs will not be collected and configuration changes will not be propagated. APs may be reported in a “Down” status by the HA Peer.</p> <p>Once the discovered appliance rejoins the HA pair, all service and state representation is restored.</p> <p>This situation will be addressed in a future release.</p>    | nse0002542     |
| <p>Stats for wired clients connected to a Wing AP7612 wired port are missing in the ExtremeCloud Appliance reports.</p> <p>This situation will be addressed in a future release.</p>  | nse0003316     |
| <p>Distributed Sites, Internal Captive Portal may error out during authentication phase. Clients may be presented with ‘registering’ status even though authentication completed in backend. Engineering is investigating and issue will be addressed in upcoming release.</p>  | nse004457      |
| <p>Several features of WiNG 7 OS are still under-development plan towards full feature parity. Several functions may be available in UI due to common provisioning but are not yet fully supported</p>  | Info           |
| <p>For AirDefense RadioShare Inline mode is not currently supported for Distributed sites. May cause issues with client association. Issue is under investigation and will be addressed in a subsequent release.</p>  | nse0004447     |

|  |                   |
|--|-------------------|
| For WiNG Proxy Mode installations that also have NSight visualization, metrics and status display and representation to ExtremeManagement Center may cease if the ExtremeCloud Appliance is rebooted | Nse004145         |
| Device Level Country override is not supported for WiNG Proxy Mode. Only one country-code assignment per site supported. All APs at the site must match the same country.                            | Info              |
| The Auto-Policy Generator function for revisions of Defender for IOT application of 3.01.19 or lower are not compatible with ExtremeCloud Appliance. Revisions higher than 3.01.19 required.         | nse0004379        |
| Combining MAC Based Authentication and LAG for switch ports is not currently supported. Engineering is investigating and issue will be addressed in upcoming release                                 | Info - nse0004445 |

**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                  |
|--------------|--------------------------|---------------------|
| Chrome       | 46.0.2490.71 dev-m       | Windows server 2012 |
| Chrome       | 47.0.2526.80 m           | Windows 7           |
| Chrome       | 38.0.2125.111m           | Windows server 2012 |
| Firefox      | 41.0.1                   | Windows server 2012 |
| Firefox      | 38.0.5                   | Windows XP          |
| Opera beta   | 34.0.2036.24             | Windows 7           |
| Safari       | Preinstalled with iOS9.1 | iOS9.1              |
| Microsoft IE | 11                       | 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 <sup>1</sup>    |
| Access Point                                | Appliance    | TCP/UDP            | Any      | 69        | TFTP          | AP image transfer                                   | Yes <sup>2</sup>    |
| Appliance                                   | Access Point | TCP/UDP            | Any      | 22        | SCP           | AP traces   | Yes                 |

<sup>1</sup>TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled, TFTP exchanges take place within the secure tunnel and port 69 is not used.

<sup>2</sup>TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled, TFTP exchanges take place within the secure tunnel and port 69 is not used.

| Comp. Source  | Comp. Dest   | Protocol (TCP/UDP) | Src Port | Dest Port     | Service        | Remark  | Open Firewall Req'd |
|---|--------------|--------------------|----------|---------------|----------------|---|---------------------|
| 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            |
| <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<br>ICP<br>Self Registration | Yes                 |
| Any   | Appliance    | TCP                | Any      | 443           | HTTPS          | ICP<br>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>3</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                 |

<sup>3</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                          | 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                 |
| <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 upon request.

**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<br>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                                   | 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 |

| Attribute             | RFC Source                   |
|-----------------------|------------------------------|
| 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](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, 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/)