

# Customer Release Notes

## Extreme Campus Controller

Firmware Version V05.16.05.0012

March 8, 2021

### INTRODUCTION:

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

The E3120 is a large application appliance meeting the needs of high-density and mission critical deployments with support for up to 10,000 APs/Defenders, 2000 switches, and 100,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

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

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

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

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

The VE6125 XL is an virtual appliance that supports up to 4,000 APs/Defenders, up to 400 switches and 32,000 mobility sessions in high-availability mode, depending on the hosting hardware.

The Extreme Campus Controller offers the ability to expand capacity to meet growing business needs. The hardware and virtual packages are available for purchase using a traditional CAPEX model. The customer has the option to purchase adoption capacity via a Perpetual (CAPEX) model or as a Right-To-Use Subscription model, supporting flexible quantities (per managed device) and term (multiple-year extended term) options.

| <b>Changes in 05.16.05.0012</b>  |          |
|--|----------|
| Removed inconsistency in client statistics exchange between XCC and XIQ.   | CFD-5966 |
| Added User Interface warning that enabling 802.11k on Networks/SSIDs can cause radio reset.  | CFD-5969 |
| Addressed issue preventing reference to VLAN 2500  | CFD-6003 |
| Improved logic when adding a Topology/VLAN to a Profile assignment. The fix addresses the condition where assignments from the VLAN creation accelerator could reset existing VLAN assignments in the Profile. | CFD-6007 |
| Introduced restriction for Role names starting with "Unregistered role for" because the phrase conflicts with internally generated references for Captive Portal.  | CFD-6040 |
| Rectified incorrect display of a long Profile name when a Profile is created under a device group.   | CFD-6045 |
| Improved stability of RADIUS Accounting functionality to address issues where bandwidth was reported as very low.  | CFD-6070 |
| Improved license management resilience for better handling of very large entitlement licensed records.   | CFD-6072 |
| Improved exception handling for management of backup files that could prevent deletion of backups once maximum size is reached.  | CFD-6097 |

| <b>Changes in 05.16.04.0004</b>  |         |
|--|---------|
| Fixed issue where re-ordering of network assignments could result in advertisement of OPEN networks (Captive Portal, etc..) as encrypted | XCC-707 |
| Corrected issue where customized dashboards and queries may be lost during upgrade for non-default admin users.                          | XCC-741 |

| <b>Enhancements in 05.16.03.0015</b>   |         |
|--|---------|
| <p>Added support for auto-provisioned enhanced Opportunistic Wireless Encryption (OWE) companion for open WLANs.</p> <p>OWE (aka Enhanced Open) is a Wi-Fi standard which ensures that the communication between each pair of endpoints is protected from other endpoints, when connecting to an "OPEN" network. Unlike conventional Open Wi-Fi, it provides "Individualized Data Protection" such that data traffic between a client and access point is "individualized".</p> <p>Supported for Wi-Fi 6 AP (AP300/AP400/AP500 series) models. Requires client compatibility with feature.</p> | XCC-578 |
| <p>Formalized support for Wireless Mesh for Wi-Fi 6 AP models (AP300, AP400, AP500 i/e/h).</p> <p>Access points can belong to one mesh point at a time, and only one radio of the AP can be used for mesh point (backhaul) connection.</p> <p>Root APs must be statically configured to the same manually assigned non-DFS channel. Non-root (node) APs on the same band will automatically scan for Root APs on the same mesh point.</p> <p>Mesh points managed by Extreme Campus Controller (Campus mode) cannot extend mesh points for AP39xx or ExtremeWireless WiNG installs.</p>         | XCC-543 |

|  |         |
|--|---------|
| Added indication of VxLAN tunnel state between AP and switches.<br>In a High Availability Pair, only one Extreme Campus Controller offers a tunnel state report. Synchronizing the tunnel state to the second Extreme Campus Controller in a High Availability Pair will be supported in a future release. | XCC-240 |
| Added protection from importing configurations that contain distributed or proxied sites.  | XCC-218 |
| Added the ability to dynamically assign a topology to a user without modifying the set of filter rules assigned to a particular end system.  | XCC-23  |
| Added redundancy for internal DHCP server high availability setup.   | XCC-21  |
| Enhanced configuration model to support the definition of Hotspot 2.0 service for AP39xx and Wi-Fi 6 access point models (Campus mode).  | XCC-5   |
| Corrected configuration issue where Off Channel Scanning (OCS) was not enabled when 802.11k was selected.  | XCC-535 |

| <b>Changes in 05.16.03.0015</b>   | <b>I.D</b> |
|---|------------|
| Improved validation of External Captive Portal URL and prevented saving of incorrect configuration entry. | XCC-638    |

| <b>Enhancements in 05.16.02.0020</b>   |         |
|--|---------|
| <p>*(BETA)* Added support for Wireless Mesh for Wi-Fi 6 AP models (AP300, 400, 500 i/e/h models). Mesh connections can be established over APs<br/>Access points can belong to one Meshpoint at a time and only one radio of the AP can be used for meshpoint (backhaul) connection.<br/>Root-APs and Node APs must be statically configured to the same manually assigned non-DFS channel. Off-Channel-Scanning (OCS) not supported for Mesh operations.<br/>MeshPoints managed by Extreme Campus Controller (Campus) cannot extend MeshPoints for AP39xx or ExtremeWireless WiNG installs.<br/>This release is defined as a BETA offering as there are a few enhancements in the works. Enhancements will be delivered in subsequent releases.</p> | XCC-8   |
| Extended adoption for monitoring and basic management for X620-16t-Base switch models  | XCC-320 |
| <p>Opportunistic Wireless Encryption (OWE) (aka Enhanced Open) is a Wi-Fi standard which ensures that the communication between each pair of endpoints is protected from other endpoints, when connecting to an "OPEN" network. Unlike conventional Open Wi-Fi, it provides "Individualized Data Protection" such that data traffic between a client and access point is "individualized".<br/>Supported for Wi-Fi 6 AP (AP300/400/500 series) models. Requires client compatibility with feature.<br/>OWE companion to open WLAN is not supported in 5.16.02. Support for OWE companion to open WLAN will be added in the next release.</p>   | XCC-22  |
| <p>Provide option for enhancing security of connection between AP and Extreme Campus Controller by requiring AP to provide Extreme-signed certificate. When enabled, APs and appliances will use the their Manufacturer (Extreme) Installed Certificate (MIC) as material for cross-authentication. MIC validation is disabled by default but can be enabled at the Profile level or overwritten on a per access point basis.<br/>Manufacturing Installed Certificates are pre-installed on all AP3900, SA201, AP300/400/500 i/e/h series access points. Manufacture Installed Certificates (MIC)</p>  | XCC-16  |

| <b>Enhancements in 05.16.02.0020</b>  |         |
|---|---------|
| are also pre-installed on the physical appliances (E1120, E2120, E3120) and are installed as part of the activation process for virtual appliances (VE6120/H, VE6125).  |         |
| Improved options for enhanced security of Fabric Attach connection to APs by providing support for configurable authentication key.   | XCC-17  |
| Improved usability of channel plan selection in RF Management by providing display of member channel IDs as a hover tip when selecting channel plan in RF management policy.<br>Different channel plans contain different channels (All channels, Non-DFS channels, 3-channel plan, etc). Hover tip now displays the channel numbers included for each selection. | XCC-219 |
| Enabled support for wired client port on AP3965. Client port (GE2) can be used to provide link to wired network for workgroup bridging extension through Meshpoint.   | XCC-213 |
| Improved reporting and integration with ExtremeCloud IQ to better differentiate wired and wireless clients. In ExtremeCloud IQ, wired and wireless clients are represented differently in view of their association capabilities.   | XCC-12  |
| Add support for several external antenna combinations for selected Wi-Fi 6 access points:<br>AP360e:<br>* WS-AO-DQ05120N<br>AP460e<br>* WS-AO-5Q05025N<br>* , WS-AO-5Q040N<br>* WS-AO-DQ05120N<br>AP410e<br>* WS-AI-5Q05025<br>* WS-AI-5Q04060  | XCC-545 |
| Added visibility of Extreme Campus Controller application stats in ExtremeIQ. Statistics are reported by Extreme Campus Controller aggregated per application group.  | XCC-53  |

| <b>Changes in 05.16.02.0020</b>   | <b>I.D</b> |
|---|------------|
| Addressed issue with synchronization of Max Distance settings across the two member appliances of an High Availability pair.  | XCC-532    |
| Improved robustness and bounds checking of certain REST APIs to protect from possible instability when using incorrect enumeration values.  | XCC-472    |
| When defining services for guest access (captive portal) the network name must be shorter than 42 characters. The network name is used in dynamic creation of roles for the un-registered user state. Long network names can cause ambiguity in role identification and possibly result in issues during system upgrades. | XCC-341    |
| Corrected issue with importing of Ekahau floor plan files failing due to a conversion issue with SVG files.   | XCC-269    |

| <b>Enhancements in 05.16.01.0025</b>   |         |
|--|---------|
| Enhanced Client Bridge functionality to allow WLAN service on the same radio that is defined for the Client-Bridge (backhaul) connection. This enables a Client-Bridge AP, when operating as a Wi-Fi extender, to offer dual-band Wi-Fi service. Up to seven services supported on the backhaul radio.   | XCC-94  |
| Enhanced appliance interfaces of Extreme Campus Controller hardware models (E1120, E2120, E3120) and virtual models (VE6120, VE6125) to allow jumbo frames of up to 1800 Bytes. AP tunnels can be extended up to that limit through the AP Profile definition or through an AP override of MTU settings.   | XCC-114 |
| Exposed support for provision of PEAP credentials or X.509 certificates for 802.11ax APs. PEAP credentials can be defined on the AP Profile or defined per individual AP. X.509 certificates can be installed per AP.  | XCC-7   |
| Improved Smart RF operation on DFS channels. When an AP that is operating on a DFS channel is hit by Radar, the AP will switch to a non-DFS or Non-Occupancy List (NOL) channel. Smart RF will not use that DFS channel until the applicable timeout from the NOL.   | XCC-118 |
| <p>Introduced additional options to control operation and performance for Wi-Fi radios, exposing controls of guard interval and wireless cell size. Guard interval can be configured per AP Profile and per individual AP. Supported values:</p> <ul style="list-style-type: none"> <li>- Auto</li> <li>- Short</li> <li>- Long</li> <li>- Quadruple*</li> </ul> <p>Improved option for controlling the effective cell size of an AP. Controlling parameters are available on AP Profile and per individual AP. Cell size can be controlled using parameters:</p> <ul style="list-style-type: none"> <li>- Probe Suppression on Low RSS (existing parameter)</li> <li>- Probe Responses Retry Limit</li> <li>- RX Sensitivity Reduction (dB)*</li> <li>- Airtime Fairness</li> <li>- Maximum Distance</li> </ul> <p>*Wi-Fi 6 models only</p> | XCC-43  |
| <p>Improved System Health widget (Best Practice Assessment) by separating presentation of configuration versus runtime/operational conditions. Additional evaluation conditions:</p> <ul style="list-style-type: none"> <li>* Multicast filters (Validate not excessively open)</li> <li>* RADIUS load balance (Recommend minimum 2)</li> <li>* Co-channel interference (Validation of best practice to use lower channel in bonded channel setting as management)</li> <li>* AP connectivity (Operational assessment that APs are connecting correctly and not experiencing issues with connectivity such as successfully acknowledging configuration)</li> </ul>   | XCC-25  |
| Improved diagnostic tools, such as ping or traceroute, to allow specifying either IP address or host name of target host.  | XCC-24  |
| Added support for X435-24P/T-4S switch models. Eight-port models will be considered for a future release.  | XCC-20  |

| Enhancements in 05.16.01.0025   |        |
|---|--------|
| Improved reporting of AP upgrade status. Report exposes completion status for upgrade group, providing insight into the percentage completed. | XCC-10 |

| Changes in 05.16.01.0025  | I.D     |
|---|---------|
| Corrected the issue where the Client Badge in a Floor plan did not show correctly.  | ECA-369 |
| Addressed an issue where after switching from Whitelist mode to Blacklist mode, there was the possibility for the traffic from the blacklisted client to not be filtered and to be able to connect to different wireless networks, obtaining Internet access. | ECA-373 |

**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.05.16.05.0012 | Maintenance Release | March 8, 2021     |
| Previous Version | V.05.16.04.0004 | Maintenance Release | January 27, 2021  |
| Previous Version | V.05.16.03.0015 | Feature Release     | December 23, 2020 |
| Previous Version | V.05.16.02.0020 | Feature Release     | December 1, 2020  |
| Previous Version | V.05.16.01.0025 | Feature Release     | October 15, 2020  |

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

| Product Name   | Image                       |
|--|-----------------------------|
| Extreme Campus Controller VE6120 VMware<br>Min Supported ESXi version 5.1 or later, (tested 6.7) | ECA-05.16.05.0012-1.dle     |
| Extreme Campus Controller VE6120H<br>(Windows server 2016 or later)                              | ECA-05.16.05.0012-1.spe     |
| Extreme Campus Controller VE6125<br>Min Supported ESXi version 5.5 or later, (tested 6.7)        | ECA-05.16.05.0012-1.rse     |
| Extreme Campus Controller E1120  | ECA-05.16.05.0012-1.sme     |
| Extreme Campus Controller E2120  | ECA-05.16.05.0012-1.jse     |
| Extreme Campus Controller E3120  | ECA-05.16.05.0012-1.ose     |
| SA201  | AP391x-10.51.17.0006.img    |
| AP310e-CAN<br>AP310e-FCC<br>AP310e-IL  | AP3xx-LEAN-7.5.1.3-004R.img |

| Product Name   | Image                       |
|--|-----------------------------|
| AP310e-WR<br>AP310i-CAN<br>AP310i-FCC<br>AP310i-IL<br>AP310i-WR  |                             |
| AP360e-CAN<br>AP360e-FCC<br>AP360e-IL<br>AP360e-WR<br>AP360i-CAN<br>AP360i-FCC<br>AP360i-IL<br>AP360i-WR | AP3xx-LEAN-7.5.1.3-004R.img |
| AP3912i-FCC<br>AP3912i-ROW   | AP391x-10.51.17.0006.img    |
| AP3915e-FCC<br>AP3915e-ROW<br>AP3915i-FCC<br>AP3915i-ROW   | AP391x-10.51.17.0006.img    |
| AP3916ic-FCC<br>AP3916ic-ROW   | AP391x-10.51.17.0006.img    |
| AP3916-camera  | AP3916IC-V1-0-14-1.dlf      |
| AP3917e-FCC<br>AP3917e-ROW<br>AP3917i-FCC<br>AP3917i-ROW<br>AP3917k-FCC<br>AP3917k-ROW                   | AP391x-10.51.17.0006.img    |
| AP3935e-FCC<br>AP3935e-ROW<br>AP3935i-FCC<br>AP3935i-IL<br>AP3935i-ROW                                   | AP3935-10.51.17.0006.img    |
| AP3965e-FCC<br>AP3965e-ROW<br>AP3965i-FCC<br>AP3965i-ROW   | AP3935-10.51.17.0006.img    |
| AP410e-CAN<br>AP410e-FCC<br>AP410e-IL<br>AP410e-WR   | AP4xx-LEAN-7.5.1.3-004R.img |

| Product Name   | Image  |
|--|--|
| AP410i-CAN<br>AP410i-FCC<br>AP410i-IL<br>AP410i-WR   |  |
| 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-7.5.1.3-004R.img  |
| AP505i-FCC<br>AP505i-WR  | AP5xx-LEAN-7.5.1.3-004R.img  |
| AP510e-FCC<br>AP510e-WR<br>AP510i-FCC<br>AP510i-WR   | AP5xx-LEAN-7.5.1.3-004R.img  |
| AP560h-FCC<br>AP560h-WR<br>AP560i-FCC<br>AP560i-WR   | AP5xx-LEAN-7.5.1.3-004R.img  |
| Switches   |  |
| 210-12p-10GE2<br>210-24p-10GE2<br>210-48p-10GE2<br>210-12p-10GE2 POE<br>210-24p-10GE2 POE<br>210-48p-10GE2 POE             | 210-series_V1.02.05.0013.stk<br>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, fp-connector-3.3.0.4.pyz<br>(cloud connector)                          |
| X435-24P/T-4S  | summitlite_arm-30.7.1.1.xos, summitlite_arm-30.5.0.259-cloud_connector-3.4.2.6.xmod                  |
| X440G2-12t-10G4<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-3.4.1.20.xmod<br>(cloud connector) |
| X465_24W   | onie-cloud_connector-3.2.5.16.xmod   |



| Product Name   | Image  |
|--|--|
| X465_48T<br>X465_48P<br>X465_48W<br>X465_24MU<br>X465_24MU_24W | onie-30.2.1.8-patch2-5-vpex_controlling_bridge.lst,<br>onie-30.2.1.8-cloud_connector-3.4.1.20.xmod |
| X620-16x/T   | summitX-30.2.1.8-patch2-5.xos, summitX-30.2.1.8-<br>cloud_connector-3.4.1.8.xmod (cloud connector) |

### NETWORK MANAGEMENT SOFTWARE SUPPORT

| Network Management Suite (NMS) | Version         |
|--------------------------------|-----------------|
| ExtremeManagement™ Center      | 8.5.2 or higher |
| ExtremeControl™                | 8.5.2 or higher |
| ExtremeAnalytics™              | 8.5.2 or higher |

| Air Defense and Location | Version      |
|--------------------------|--------------|
| ExtremeAirDefense™       | 10.4         |
| ExtremeGuest             | Version      |
| ExtremeGuest™            | 6.0.1.0-001R |

#### Note:

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

### INSTALLATION INFORMATION:

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

### Known Restrictions and Limitations:

| Known Restriction or Limitation  | I.D     |
|--|---------|
| Upon upgrading from Extreme Campus Controller version 4 to version 5, the appliance certificates are extended. Firefox browsers may see this validity extension as a | XCC-934 |

| Known Restriction or Limitation  | I.D        |
|--|------------|
| security violation. To resolve, follow FF's procedure for certificate management and remove any certs it may have cached for the appliance(s).   |            |
| <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 |
| An interoperability issue has been discovered with Policy Manager for Extreme Management Center revision 8.5.3.66. Issue is under investigation and will be addressed in a future release.   | None       |
| A reboot of the peer Extreme Campus Controller is required when Availability is configured for the first time to ensure synchronization of the configuration of ONBOARD attributes, such as device groups. This issue will be addressed in a future release.   | ECA-622    |
| GUI Mesh Report is missing the information about the Root AP with Ethernet connection. This problem will be addressed in a future release.   | ECA-565    |
| The switch primary/backup availability is not supported on the EXOS switches running the 3.4.1.8 Cloud Connector. This affects the deployments where two appliances are configured in an Availability Pair. If the primary appliance is going down, then the EXOS switches will not send statistics to the backup appliance and will be marked in red "Critical" state. When the primary appliance is coming up again, the switches will resume sending statistics information to the primary appliance and the state of the switch will be marked with a green "Running" state. | ECA-455    |
| Allow UTF-8 characters in JSON payload for all Rest API so non-ASCII / Unicode characters are accepted in Rest API requests to comply with current Rest API standards.   | ECA-321    |
| If a license violation is corrected, the license violation banner and GUI notification bell are not cleared until the page is refreshed. Similarly, in a new installation, after a license is installed, refresh the page. This issue will be addressed in a future release.   | ECA-1971   |
| MAC-based authentication and WPA3-Compatibility (SAE or WPA2-PSK) and PMF "Required" may not work. This issue will be addressed in a future release.   | ECA-1961   |
| AP310 models are not currently supported by ExtremeLocation™. Do not enable ExtremeLocation settings in the configuration Profile for an AP310 device group. Doing so may have a negative impact on AP performance.  | ECA-1620   |
| For Extreme Campus Controller configured for authentication of administrators over RADIUS server, the GUI responsiveness may be slow, possibly over 30 seconds if target servers are unavailable/unreachable at login time. If outage is extensive, system will eventually timeout to validate against local credentials when provisioned.   | ECA-1396   |
| <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 immediately reconnect to the available infrastructure, so impact is negligible. For smoother session availability with fast-failover during a failover event, it is recommended to not run these options. This issue is being investigated and will be addressed in a future release.</p>   | ECA-1264   |

| Known Restriction or Limitation  | I.D      |
|--|----------|
| Upgrade failure will occur when using special characters (escape back slash) in topology.  | ECA-466  |
| In SmartRF mode, the AP510 power may temporarily drop to 0dBm and return to 4dBm.  | ECA-469  |
| With on-air-busy channel conditions, it is possible for the ACS not to produce the expected results. In this instance, perform manual channel selection.   | ECA-528  |
| Docker requires exclusive use of subnet 172.17.0.0/24 for containers. Customers should not use an IP address in that range for any VLAN or network interface.  | ECA-532  |
| Widgets do not show tooltips for Lower and Upper values. This issue will be addressed in a future release.   | ECA-567  |
| Firmware for ExtremeWireless AP3900 series access points does not currently support Smart RF. No Smart RF data is displayed.   | ECA-1484 |
| <p>Interaction with ExtremeManagement Center – Management of Extreme Campus Controller by ExtremeManagement Center will be enhanced over time with the roadmap. ExtremeManagement Center v8.5.2 is the minimum release base for integration. Version 8.5.2 provides recognition of an Extreme Campus Controller 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 8.5.2 is the current recommended minimum release.</p>  | Info     |
| <p>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.</p> <p>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><a href="http://example.com">[http://example.com]</a></p> <p>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><a href="http://example.com">[http://example.com]</a></p> <p>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.</p> <p>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.</p> | Info     |
| <p>Default router/gateway should be configured with a next-hop associated with one of the physical interfaces. Pointing the default route to the Admin interface will lead to issues because access points will not get the correct services from the data plane. We recommend setting the default route via data ports, and if necessary, configuring static routes on the Admin port for administration level access.</p>  | Info     |
| <p>Before installing a new Extreme Campus Controller license, you must configure Network Time Protocol (NTP) Server settings. Licensing management is dependent on accurate NTP configuration. Configure NTP via the Extreme Campus Controller initial Configuration Wizard, or go to Admin &gt; System &gt; Network Time to configure and verify the NTP settings.</p>  | Info     |
| <p>For AP deployments in remote locations where access points and controllers may need to be discovered and connected over firewalls, a best practice is to leverage DNS or DHCP Option 60/43 methods for zero-touch-provisioning discovery. These methods provide direct connectivity to the defined IP address. DHCP Option 78, which refers to the controller as a Service Location Protocol – Directory Agent (SLP-</p>  | Info     |

| Known Restriction or Limitation  | I.D                        |
|--|----------------------------|
| <p>DA), requires the exchange of SLP protocol between the AP and the appliance at the core, necessitating that UDP 427 be allowed by any firewall in the path. For such installations, discovery over DHCP Option 78 assist is not recommended.</p> <p>When using SLP, for an AP to establish connection with a controller, it must first exchange SLP Directory Agent registration before IPSEC establishment with the eventual controller. That means that SLP UDP 427 must be open along the path. Further issues can occur if Network Address Translation (NAT) is involved. While this method is popular and widely deployed within a homogenous campus, it may result in inadvertent complications for remote connections. Therefore, it should not be used in favor of an alternate method (DHCP 60/43, DNS, or static override).</p> |                            |
| <p>When configuring system for NTP time assignment, ensure that the NTP server is properly configured. Incorrect time settings (like timestamps far in the future) may adversely affect system operation, such as certificate expiration that may trigger failures in device registration or system instability.</p>   | <p>Info<br/>nse0003696</p> |
| <p>Appliances in a High-Availability pair must be of the same model and at the same exact software revision (and time synched) for configuration synchronization to propagate to the peer. During the upgrade process of a High-Availability pair, any configuration changes made while only one appliance has been upgraded (and therefore resulting in a version mismatch) will not be propagated until the peer is correspondingly upgraded to the same revision. We recommend that you NOT perform configuration changes to one of the members of a High-Availability pair while the peer has a different software revision.</p>   | <p>Info<br/>nse0005086</p> |
| <p>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.</p> <p>During upgrade periods, the Availability link will only re-establish when both the appliance status of availability link and synchronization status can be found.</p> <p>Go to:</p> <ul style="list-style-type: none"> <li>· "Network Health" widget on the Dashboard, or</li> <li>· Administration -&gt; System -&gt; Availability</li> </ul>  | <p>Info<br/>ECA-776</p>    |
| <p>Recommendation settings for setup of redundant RADIUS server authentication:</p> <ul style="list-style-type: none"> <li>· Response Window to 5s [Default: 20s]</li> <li>· Revival Interval to 10s [Default: 60s]</li> </ul>   | <p>Info<br/>ECA-875</p>    |

**SUPPORTED WEB BROWSERS**

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

- Firefox 81.0
- Google Chrome 86.0

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

The Wireless Clients (Captive Portal, AAA):

| Browsers       | Version                     | OS                                     |
|----------------|-----------------------------|--|
| Chrome         | 75.0.37770.142              | Windows 7<br>Windows 10                |
| Microsoft IE   | 11                          | Windows 7<br>Windows 8.1<br>Windows 10 |
| Microsoft Edge | 42.17134                    | Windows 10                             |
| Firefox        | 68.0                        | Windows 10                             |
| Safari         | Preinstalled with iOS 12.2  | iOS 12.2                               |
| Safari         | Preinstalled with iOS 9.3.5 | iOS 9.3.5                              |

**PORT LIST**

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

**Extreme Campus Controller TCP/UDP Port Assignment Reference**

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

| Comp. Source                          | Comp. Dest   | Protocol (TCP/UDP) | Src Port | Dest Port     | Service        | Remark                                      | Open Firewall Req'd |
|---------------------------------------|--------------|--------------------|----------|---------------|----------------|---|---------------------|
| Access Point                          | Appliance    | UDP                | Any      | 68            | DHCP Server    | If Appliance is DHCP Server for AP          | Optional            |
| Access Point                          | Appliance    | UDP                | Any      | 427           | SLP            | AP Registration to Appliance                | Optional            |
| Appliance                             | Access Point | TCP/UDP            | Any      | 69            | TFTP           | AP image transfer                           | Yes                 |
| Access Point                          | Appliance    | TCP/UDP            | Any      | 69            | TFTP           | AP image transfer                           | Yes                 |
| Appliance                             | Access Point | TCP/UDP            | Any      | 22            | SCP            | AP traces                                   | Yes                 |
| Any                                   | Access Point | TCP                | Any      | 2002, 2003    | RCAPD          | AP Real Capture (if enabled)                | Optional            |
| Any                                   | Access Point | TCP/UDP            | Any      | 22            | SSH            | Remote AP login (if enabled)                | Optional            |
| Any                                   | Access Point | TCP/UDP            | Any      | 445           | Microsoft CIFS | LDAP support                                | Optional            |
| Any                                   | Access Point | TCP/UDP            | Any      | 137, 138, 139 | NetBIOS        | LDAP support                                | Optional            |
| <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                 |

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

<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 |
|----------------------------|------------------|--------------------|----------|-----------|------------------------------|---|---------------------|
| Dynamic Auth. Server (NAC) | Appliance        | UDP                | Any      | 3799      | DAS                          | Request from DAS client to disconnect a specific client | Optional            |
| Appliance                  | AeroScout Server | UDP                | 1144     | 12092     | Location Based Service Proxy | Aeroscout Location-Based Service                        | Optional            |
| AeroScout Server           | Appliance        | UDP                | 12092    | 1144      | Location Based Service Proxy | Aeroscout Location-Based Service                        | Optional            |
| Appliance                  | Extreme Cloud IQ | TCP                | Any      | 443       | NSight                       | Statistics Report into ExtremeCloud IQ                  | Yes                 |

**IETF STANDARDS MIB SUPPORT:**

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

**EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT**

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

**Standard MIBs**

| Title            | Description                         |
|------------------|-------------------------------------|
| IEEE802dot11-MIB | Standard MIB for wireless devices   |
| RFC1213-MIB.my   | Standard MIB for system information |
| IF-MIB           | Interface MIB                       |



| Title        | Description   |
|--------------|---|
| 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 |

| Vendor                   | Model OS  | Version   |
|--------------------------|---|---|
|                          |   | 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)<br>(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                                  | 1.1.1g        |

**RADIUS ATTRIBUTES SUPPORT****RADIUS Authentication and Authorization Attributes**

| Attribute             | RFC Source                   |
|-----------------------|------------------------------|
| Called-Station-Id     | RFC 2865, RFC 3580           |
| Calling-Station-Id    | RFC 2865, RFC 3580           |
| Class                 | RFC 2865                     |
| EAP-Message           | RFC 3579                     |
| Event-Timestamp       | RFC 2869                     |
| Filter-Id             | RFC 2865, RFC 3580           |
| Framed-IPv6-Pool      | RFC 3162                     |
| Framed-MTU            | RFC 2865, RFC 3580           |
| Framed-Pool           | RFC 2869                     |
| Idle-Timeout          | RFC 2865, RFC 3580           |
| Message-Authenticator | RFC 3579                     |
| NAS-Identifier        | RFC 2865, RFC 3580           |
| NAS-IP-Address        | RFC 2865, RFC 3580           |
| NAS-IPv6-Address      | RFC 3162                     |
| NAS-Port              | RFC 2865, RFC 3580           |
| NAS-Port-Id           | RFC 2865, RFC 3580           |
| NAS-Port-Type         | RFC 2865, RFC 3580           |
| Password-Retry        | RFC 2869                     |
| 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           |

| Attribute       | RFC Source |
|-----------------|------------|
| 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/)