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

# Customer Release Notes

## Extreme Campus Controller

Firmware Version V05.26.05.0003
July 23, 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 or 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 or Defenders, 800 switches and 32,000 mobility sessions in high-availability mode. An optional redundant power supply is available for ordering separately.

The E2122 is an application appliance meeting the needs of medium sized high-density and mission critical deployments with support for up to 4,000 Aps or 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 or 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 or 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 or Defenders, up to 400 switches and 32,000 mobility sessions in high-availability mode, depending on the hosting hardware.

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

| Changes in 05.26.05.0003 | |
|---|---|
| Relaxed enforcement of Capacity oversubscription after grace period expiration to allow removal of access points under management. Allows customers to match number of devices under management to amount of entitlements available. | CFD-6396 |
| Adjusted file name for AirDefense configuration drop-down menu in UI that could cause AD Blocker plug-in for Chrome browsers to misqualify and prevent the configuration of connection parameters from displaying correctly. | CFD-6444 |
| Changed RADIUS accounting to broadcast updates to all configured Accounting Servers. | CFD-6451 |
| Enhanced client session handling logic on Access Points to assure response from Access Points to Extreme Campus Controller's session management. | CFD-6547 |
| Corrected the condition that prevented editing previously configured floor plans. | CFD-6645 |

| Changes in 05.26.04.0006 | |
|---|---|
| Enhanced device type recognition for Device group rules to match and filter intended devices. | CFD-5973 |
| Corrected detection of Apple devices types running iOS v14. | CFD-6372 |
| Rectified synchronization issue that prevented proper tunnel management within internal components of Extreme Campus Controller. | CFD-6422 |

| Enhancements in 05.26.03.0016 | |
|---|---|
| Enabled BLE/IoT functions for iBeacon/Eddystone (beacon) Send/Receive for Universal APs (AP302W, AP305C/X, AP410C, AP460C and variants). | XCC-703 |
| Adjusted Captive Portal Administration portal to dedicated access port, facilitating better Access policy control on access to Guest-Management portal. Captive Portal user administration portal has been remapped to port 8445. | XCC-897 |
| Provided the option to include Location-Capable attribute, aligned to RFC 5580, for user authorization via RADIUS. | XCC-808 |
| Added vendor-specific attribute (VSA), which includes RSS for client station in RADIUS requests. | XCC-858 |
| Added a new option of "Throughput by Group" widget for custom reports generation. | XCC-1247 |
| Enhanced schedule reports to provide flexible reporting interval. | XCC-1133 |

| Enhancements in 05.26.02.0014 | |
|---|---|
| Added support for adoption of AP302W, the new 2x2 802.11ax wallplate Universal AP. Supported models are:<br>• AP302W-FCC<br>• AP302W-WR<br>• AP302W-CAN | XCC-495 |
| Introduced the Extreme Campus Controller E2122, supporting expandable management for up to 4000 APs (HA). Requires Activation License (XCC-ACT-V5-HW) and device Adoption Capacity Licenses (XCC-ORC-x-xxx).<br>Extreme Campus Controller V5.26.02 or newer installs only. | XCC-664 |

| | |
|---|---|
| Enhanced Reports facility to provide better aggregate reporting representative of large venue installations. Added ability to support reports based on customer-defined user groups, enabling consolidation of metrics from different user categories combined in the same widget.<br>Scheduler for Extreme Campus Controller v1.1.04 recommended in support of automatic report scheduling. | XCC-715 |
| Improved workflow for configuring physical link aggregation (LAG). LAG configuration will automatically remap topologies assigned to member ports to the LAG port. | XCC-775 |
| Improved control over "Locate" LED pattern by providing explicit control for enabling and disabling the pattern. | XCC-825 |
| Introduced new notification event conveying significant changes in the X/Y positioning of an associated device relative to the site's floorplan, providing improved efficiency of external location related applications. Programmable access to this new event is facilitated though the Extreme Campus Controller Python SDK (https://test.pypi.org/project/pyxccsdk/). | XCC-661 |
| Improved utilization metrics widgets to provide customers with better insight as to actual average utilization and the usage contribution from each client. | XCC-844 |
| Improved naming of techsupport files for easier sorting. | XCC-856 |
| (Beta) Added widgets for monitoring of AP connectivity and network link metrics. | XCC-446 |
| Addressed issue with reporting visualization in the User Interface for Mesh Reports of a Root AP with Ethernet connection. | ECA-565 |

| **Enhancements in 05.26.01.0023** | |
|---|---|
| Added support for adoption of Universal AP variants: AP410C and AP460C.<br>Minimum serial number required:<br>- First 410C SN = 04102101280001<br>- First 460C SN = 24602101250001<br>- First 460S6C SN = 34602101250001<br>- First 460S12C SN = 44602101250001 | XCC-562 |
| Added support for adoption of Universal AP variants: AP305C and AP305CX.<br>Minimum serial number required:<br>- First 305C SN = 03052009040001<br>- First 305CX SN = 13052009040001 | XCC-665 |
| Expanded capacity of wired ports on AP5xx/AP4xx and AP410C to 128 clients per port. | XCC-732 |
| Enhanced dashboards to provide top-level and site-level mixed aggregate views for:<br>- Multi-level time chart of users per network (SSID) across all networks<br>- Utilization per Network<br>- Multi-level chart of network utilization across all networks | XCC-716 |
| Extend Central Web Authentication (CWA) capabilities to AP3900 installs, enabling support for redirecting wireless client to HTTP splash page after 802.1x authentication. | XCC-662 |
| Improved configuration of mesh network:<br>- Expose CMCX-ACS parameters on Profile and AP Override<br>- Added configuration for Preferred Neighbor and Preferred Root on Profile and AP Override<br>- Improved Mesh Statistic page, displaying additional details about the mesh connection, including information about the neighboring AP and link quality. | XCC-609 |

| | |
|---|---|
| Added support configuration of Mesh Point operation for Universal AP models, including wireless and wired connectivity extension, for AP types:<br>- AP410C<br>- AP460C/S6/S12<br>- AP305C/CX<br>Note: AP305C/CX does not support a wired Mesh Network extension. | XCC-600 |
| Added support for configurable RSS threshold for client bridge AP to search for new root. | XCC-460 |
| Report Scheduling:<br>New revision 1.1.01 of Scheduler for Extreme Campus Controller application. This revision has been enhanced to support scheduling the generation of customer reports. | XCC-19 |
| (BETA) Introduces new Reports facility that allows administrators to generate custom reports, in PDF format, based on system operational metrics. | XCC-18 |

| Changes in 05.26.03.0016 | I.D |
|---|---|
| Improved accuracy of data collected by RADIUS Accounting. | XCC-1276 |
| Rectified incorrect behaviour of SNMP agent that sent out SNMP traps of all levels, no matter what level was set in the configuration. | XCC-1248 |
| Addressed issue with AP302W defaulting to using TFTP for initial out-of-box upgrade. | XCC-1204 |
| Removed the condition that caused erroneous alarm about bonded channels despite the fact that access points were configured for two different sites. | XCC-1201 |

| Changes in 05.26.01.0023 | I.D |
|---|---|
| Fixed issue where re-ordering of network assignments could result in advertisement of OPEN networks as encrypted. For example, Captive Portal. | XCC-707 |
| An interoperability issue has been resolved with Policy Manager for Extreme Management Center revision 8.5.4. | XCC-684 |

**Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.**

**For the latest firmware versions, visit the download site at:**
www.extremenetworks.com/support/

## FIRMWARE SPECIFICATION:

| Status | Version No. | Type | Release Date |
|---|---|---|---|
| Current Version | V.05.26.05.0003 | Maintenance Release | July 23, 2021 |
| Previous Version | V.05.26.04.0006 | Maintenance Release | June 25, 2021 |
| Previous Version | V.05.26.03.0016 | Feature Release | May 11, 2021 |
| Previous Version | V.05.26.02.0014 | Feature Release | March 26, 2021 |
| Previous Version | V.05.26.01.0023 | Feature Release | March 05, 2021 |

## 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-05.26.05.0003-1.dle |
| Extreme Campus Controller VE6120H<br>(Windows server 2016 or later) | ECA-05.26.05.0003-1.spe |
| Extreme Campus Controller VE6125<br>Min Supported ESXi version 5.5 or later, (tested 6.7) | ECA-05.26.05.0003-1.rse |
| Extreme Campus Controller E1120 | ECA-05.26.05.0003-1.sme |
| Extreme Campus Controller E2120 | ECA-05.26.05.0003-1.jse |
| Extreme Campus Controller E2122 | ECA-05.26.05.0003-1.wze |
| Extreme Campus Controller E3120 | ECA-05.26.05.0003-1.ose |
| SA201 | AP391x-10.51.19.0001.img |
| SA201 | AP391x-10.51.19.0001.img |
| AP302W-CAN<br>AP302W-FCC<br>AP302W-IL<br>AP302W-WR | AP302W-LEAN-7.6.1.2-001R.img |
| AP305C-CAN<br>AP305C-FCC<br>AP305C-IL<br>AP305C-WR<br>AP305CX-CAN<br>AP305CX-FCC<br>AP305CX-IL<br>AP305CX-WR | AP3xxC-LEAN-7.6.1.2-001R.img |
| AP310e-CAN<br>AP310e-FCC<br>AP310e-IL<br>AP310e-WR<br>AP310i-CAN<br>AP310i-FCC<br>AP310i-IL<br>AP310i-WR | AP3xx-LEAN-7.6.1.2-001R.img |
| AP360e-CAN<br>AP360e-FCC<br>AP360e-IL<br>AP360e-WR<br>AP360i-CAN<br>AP360i-FCC<br>AP360i-IL | AP3xx-LEAN-7.6.1.2-001R.img |

| Product Name | Image |
|---|---|
| AP360i-WR | |
| AP3912i-FCC<br>AP3912i-ROW | AP391x-10.51.19.0001.img |
| AP3915e-FCC<br>AP3915e-ROW<br>AP3915i-FCC<br>AP3915i-ROW | AP391x-10.51.19.0001.img |
| AP3916ic-FCC<br>AP3916ic-ROW | AP391x-10.51.19.0001.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-10.51.19.0001.img |
| AP3935e-FCC<br>AP3935e-ROW<br>AP3935i-FCC<br>AP3935i-IL<br>AP3935i-ROW | AP3935-10.51.19.0001.img |
| AP3965e-FCC<br>AP3965e-ROW<br>AP3965i-FCC<br>AP3965i-ROW | AP3935-10.51.19.0001.img |
| AP410C-CAN<br>AP410C-FCC<br>AP410C-IL<br>AP410C-WR<br>AP410e-CAN<br>AP410e-FCC<br>AP410e-IL<br>AP410e-WR<br>AP410i-CAN<br>AP410i-FCC<br>AP410i-IL<br>AP410i-WR | AP4xx-LEAN-7.6.1.2-001R.img |
| AP460C-CAN<br>AP460C-FCC<br>AP460C-IL<br>AP460C-WR | AP4xx-LEAN-7.6.1.2-001R.img |

| Product Name | Image |
|---|---|
| AP460S12C-CAN<br>AP460S12C-FCC<br>AP460S12C-IL<br>AP460S12C-WR<br>AP460S6C-CAN<br>AP460S6C-FCC<br>AP460S6C-IL<br>AP460S6C-WR<br>AP460e-CAN<br>AP460e-FCC<br>AP460e-IL<br>AP460e-WR<br>AP460i-CAN<br>AP460i-FCC<br>AP460i-IL<br>AP460i-WR | |
| AP505i-FCC<br>AP505i-WR | AP5xx-LEAN-7.6.1.2-001R.img |
| AP510e-FCC<br>AP510e-WR<br>AP510i-FCC<br>AP510i-WR | AP5xx-LEAN-7.6.1.2-001R.img |
| AP560h-FCC<br>AP560h-WR<br>AP560i-FCC<br>AP560i-WR | AP5xx-LEAN-7.6.1.2-001R.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 (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 | summitX-30.2.1.8-patch2-5.xos |

| Product Name | Image |
|---|---|
| X440G2-12t-10G4 POE<br>X440G2-24t-10G4 POE<br>X440G2-48t-10G4 POE | summitX-30.2.1.8-cloud_connector-3.4.1.20.xmod (cloud connector) |
| X465_24W<br>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, onie-30.2.1.8-cloud_connector-3.4.1.20.xmod<br>onie-30.2.1.8-patch2-5-vpex_controlling_bridge.lst, onie-30.2.1.8-cloud_connector-3.4.1.20.xmod |
| X620-16x | summitX-30.2.1.8-patch2-5.xos, summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector) |

## NETWORK MANAGEMENT SOFTWARE SUPPORT

| Network Management Suite (NMS) | Version |
|---|---|
| ExtremeManagement™ Center | 8.5.5 or higher |
| ExtremeControl™ | 8.5.5 or higher |
| ExtremeAnalytics™ | 8.5.5 or higher |

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

**Note:**

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

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

## INSTALLATION INFORMATION:

| Appliance Installations | |
|---|---|
| E1120 | Extreme Campus Controller E1120 Installation Guide |
| E2120 | Extreme Campus Controller E2120 Installation Guide |
| E2122 | Extreme Campus Controller E2122 Installation Guide |

| | |
|---|---|
| E3120 | Extreme Campus Controller E3120 Installation Guide |
| VE6120/VE6125 | Extreme Campus Controller VE6120/VE6125 Installation Guide |
| VE6120H | Extreme Campus Controller VE6120H Installation Guide |

## Known Restrictions and Limitations:

| Known Restriction or Limitation | I.D |
|---|---|
| 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.<br>The currently recommended workaround is to not enable PMF/MFP configuration on a service that is also using 802.11r. Such clients have been demonstrated to work correctly on services with just 802.11r (FT) enabled. | nse0003416 |
| Corrected the issue that prevented sending Link Aggregation Group (LAG) configuration from Extreme Campus Appliance to Extreme 220 Series switch. | XCC-1298 |
| When system has one or more scheduled reports, synchronization may fail with error "Duplicate name". The error can be found in the "Network Health" widget and on the Availability configuration page. When this error is observed, synchronization of scheduled reports cannot be completed, and content of reports may be different on each controller in a high availability setup. No other functionality is affected. The workaround is to remove and re-create the scheduled reports. If the error is not observed, there is no need for the workaround. | XCC-1283 |
| Client Bridge is currently not supported for single Port APs (AP305C/CX). It will be added in a future release. | XCC-1045 |
| 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 |

| Known Restriction or Limitation | I.D |
|---|---|
| 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 server(s) are unavailable/unreachable at login time. If outage is extensive, system will eventually timeout to validate against local credentials when provisioned. | ECA-1396 |
| For High-Availability installations, on systems configured with RADIUS Accounting or Smart RF enabled, clients (end-systems) may experience a momentary disconnect during the upgrade process (maintenance window).<br>Users immediately reconnect to the available infrastructure, so impact is negligible. For smoother session availability with fast-failover during a failover event, it is recommended to not run these options. This issue is being investigated and will be addressed in a future release. | ECA-1264 |
| Upgrade failure will occur when using special characters (escape back slash) in topology. | ECA-466 |
| In SmartRF mode, the AP510 power may temporarily drop to 0dBm and returns to 4dBm. | ECA-469 |
| With on-air-busy channel conditions, it is possible for the ACS not to produce the expected results. In this instance, perform manual channel selection. | ECA-528 |
| Widgets do not show tooltips for lower and upper values. This issue will be addressed in a future release. | ECA-567 |
| Firmware for ExtremeWireless AP3900 series access points does not currently support Smart RF. No Smart RF data is displayed. | ECA-1484 |
| Interaction with ExtremeManagement Center – Management of Extreme Campus Controller by ExtremeManagement Center will be enhanced over time with the roadmap. ExtremeManagement Center v8.5.5 is the minimum release base for integration. Version 8.5.5 provides recognition of an Extreme Campus Controller and representation of Wireless Clients and managed Access Points included in the Wireless tab.<br>Additional integration will be delivered in upcoming releases. ExtremeManagement Center 8.5.5 is the current recommended minimum release. | Info |
| Several old Intel clients (i.e. Intel dual band Wireless AC – 7260) if they are using old drivers are NOT seeing BSSID / SSID advertising 11x capability. This is a client issue (forward compatibility). Other older clients may have this issue.<br>See:<br>[https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html\|http://example.com]<br>See KB:<br>[https://gtacknowledge.extremenetworks.com/articles/Solution/AP510-Unable-to-see-the-SSID-on-my-laptop\|http://example.com]<br>NB – The client driver update must be done from Intel\drivers' site because the Windows update reports that the client is running the latest driver.<br>If the client driver cannot be controlled (in a BYOD environment), then the AP radios must be configured on a/n/ac (disable ax) until all clients will upgrade to the latest driver. | Info |
| 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. | Info |

| Known Restriction or Limitation | I.D |
|---|---|
| We recommend setting the default route via data ports, and if necessary, configuring static routes on the Admin port for administration level access. | |
| Before installing a new Extreme Campus Controller license, you must configure Network Time Protocol (NTP) Server settings. Licensing management is dependent on accurate NTP configuration. Configure NTP via the Extreme Campus Controller initial Configuration Wizard, or go to Admin > System > Network Time to configure and verify the NTP settings. | Info |
| For AP deployments in remote locations where access points and controllers may need to be discovered and connected over firewalls, a best practice is to leverage DNS or DHCP Option 60/43 methods for zero-touch-provisioning discovery. These methods provide direct connectivity to the defined IP address. DHCP Option 78, which refers to the controller as a Service Location Protocol – Directory Agent (SLP-DA), requires the exchange of SLP protocol between the AP and the appliance at the core, necessitating that UDP 427 be allowed by any firewall in the path. For such installations, discovery over DHCP Option 78 assist is not recommended.<br>When using SLP, for an AP to establish connection with a controller, it must first exchange SLP Directory Agent registration before IPSEC establishment with the eventual controller. That means that SLP UDP 427 must be open along the path. Further issues can occur if Network Address Translation (NAT) is involved. While this method is popular and widely deployed within a homogenous campus, it may result in inadvertent complications for remote connections. Therefore, it should not be used in favor of an alternate method (DHCP 60/43, DNS, or static override). | Info |
| When configuring system for NTP time assignment, ensure that the NTP server is properly configured. Incorrect time settings (like timestamps far in the future) may adversely affect system operation, such as certificate expiration that may trigger failures in device registration or system instability. | Info<br>nse0003696 |
| Appliances in a High-Availability pair must be of the same model and at the same exact software revision (and time synched) for configuration synchronization to propagate to the peer. During the upgrade process of a High-Availability pair, any configuration changes made while only one appliance has been upgraded (and therefore resulting in a version mismatch) will not be propagated until the peer is correspondingly upgraded to the same revision. We recommend that you NOT perform configuration changes to one of the members of a High-Availability pair while the peer has a different software revision. | Info<br>nse0005086 |
| For High-Availability configurations, during upgrade phases or configuration restore operations, wait until the availability link is established and synchronized before attempting to make any new configuration changes. The Availability status will only re-establish to Synched status when both appliances are running the exact same firmware revision.<br>During upgrade periods, the Availability link will only re-establish when both the appliance status of availability link and synchronization status can be found.<br>Go to:<br>· “Network Health" widget on the Dashboard, or<br>· Administration -> System -> Availability | Info<br>ECA-776 |
| Recommendation settings for setup of redundant RADIUS server authentication:<br>· Response Window to 5s [Default: 20s]<br>· Revival Interval to 10s [Default: 60s] | Info<br>ECA-875 |

## 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 |
|---|---|---|---|---|---|---|---|
| **Ports for AP/Appliance Communication** | | | | | | | |
| Appliance | Access Point | UDP | Any | 13910 | WASSP | Management and Data Tunnel between AP and Appliance | Yes |
| Access Point | Appliance | UDP | Any | 13910 | WASSP | Management and Data Tunnel between AP and Appliance | Yes |
| Appliance | Access Point | UDP | 4500 | Any | Secured WASSP | Management Tunnel between AP and Appliance | Optional |

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|---|---|---|---|---|---|---|---|
| Access Point | Appliance | UDP | Any | 4500 | Secured WASSP | Management Tunnel between AP and Appliance | Optional |
| Access Point | Appliance | UDP | Any | 13907 | WASSP | AP Registration to Appliance | Yes |
| Access Point | Appliance | UDP | Any | 67 | DHCP Server | If Appliance is DHCP Server for AP | Optional |
| Access Point | Appliance | UDP | Any | 68 | DHCP Server | If Appliance is DHCP Server for AP | Optional |
| Access Point | Appliance | UDP | Any | 427 | SLP | AP Registration to Appliance | Optional |
| Appliance | Access Point | TCP/UDP | Any | 69 | TFTP | AP image transfer | Yes |
| Access Point | Appliance | TCP/UDP | Any | 69 | TFTP | AP image transfer | Yes |
| Appliance | Access Point | TCP/UDP | Any | 22 | SCP | AP traces | Yes |
| Any | Access Point | TCP | Any | 2002, 2003 | RCAPD | AP Real Capture (if enabled) | Optional |
| Any | Access Point | TCP/UDP | Any | 22 | SSH | Remote AP login (if enabled) | Optional |
| Any | Access Point | TCP/UDP | Any | 445 | Microsoft CIFS | LDAP support | Optional |
| Any | Access Point | TCP/UDP | Any | 137, 138, 139 | NetBIOS | LDAP support | Optional |
| **Ports for Appliance Management** | | | | | | | |
| Any | Appliance | TCP/UDP | Any | 22 | SSH | Appliance CLI access | Yes |
| Any | Appliance | TCP/UDP | Any | 5825 | HTTPS | Appliance GUI access | Yes |
| Any | Appliance | TCP/UDP | Any | 161 | SNMP | Appliance SNMP access | Yes |
| Any | Appliance | TCP/UDP | Any | 162 | SNMP Trap | Appliance SNMP access | Yes |

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|---|---|---|---|---|---|---|---|
| Any | Appliance | TCP | Any | 80 | HTTP | Appliance SNMP access ICP Self Registration | Yes |
| Any | Appliance | TCP | Any | 443 | HTTPS | ICP Self Registration | Yes |
| Any | Appliance | UDP | 500 | 500 | IKE | IKE phase 1 | Yes |
| Any | Appliance | TCP/UDP | Any | 69 | TFTP | TFTP support | Yes |
| Any | Appliance | UDP | Any | 4500 | IPSec | IPSec NAT traversal | Yes |
| Any | Appliance | UDP | Any | 13907 | Discovery | Used by Discovery | Yes |
| Any | Appliance | UDP | Any | 13910 | WASSP | Used by L3 WASSP | Yes |
| **Ports for Inter Controller Mobility[1] and Availability** | | | | | | | |
| Appliance | Appliance | UDP | Any | 13911 | WASSP | Mobility and Availability Tunnel | Yes |
| Appliance | Appliance | TCP | Any | 427 | SLP | SLP Directory | Yes |
| Appliance | Appliance | TCP | Any | 20506 | Langley | Remote Langley Secure | Yes |
| Appliance | Appliance | TCP | Any | 60606 | Mobility | VN MGR | Yes |
| Appliance | Appliance | TCP | Any | 123 | NTP | Availability time sync | Yes |
| Appliance | DHCP Server | UDP | Any | 67 | SLP | Asking DHCP Server for SLP DA | Yes |
| DHCP Server | Appliance | UDP | Any | 68 | SLP | RespoECA from DHCP Server for SLP DA request | Yes |
| **Core Back-End Communication** | | | | | | | |
| Appliance | DNS Server | UDP | Any | 53 | DNS | If using DNS | Optional |
| Appliance | Syslog Server | UDP | Any | 514 | Syslog | If Appliance logs to external syslog server | Optional |
| Appliance | RADIUS Server | UDP | Any | 1812 | RADIUS Authentication and Authorization | If using RADIUS AAA | Optional |

[1]For extension of ExtremeWireless deployment via Inter Controller Mobility.

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|---|---|---|---|---|---|---|---|
| Appliance | RADIUS Server | UDP | Any | 1813 | RADIUS Accounting | If enabled RADIUS accounting | Optional |
| Appliance | RADIUS server | UDP | Any | 1814 | RADIUS Authentication and Authorization | If using RADIUS AAA | Optional |
| Appliance | RADIUS server | UDP | Any | 1815 | RADIUS Accounting | If enabled RADIUS Accounting | Optional |
| Dynamic Auth. Server (NAC) | Appliance | UDP | Any | 3799 | DAS | Request from DAS client to disconnect a specific client | Optional |
| Appliance | AeroScout Server | UDP | 1144 | 12092 | Location Based Service Proxy | Aeroscout Location-Based Service | Optional |
| AeroScout Server | Appliance | UDP | 12092 | 1144 | Location Based Service Proxy | Aeroscout Location-Based Service | Optional |
| Appliance | Extreme Cloud IQ | TCP | Any | 443 | NSight | Statistics Report into ExtremeCloud IQ | Yes |

## IETF STANDARDS MIB SUPPORT:

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

## EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

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

### Standard MIBs

| Title | Description |
|---|---|
| IEEE802dot11-MIB | Standard MIB for wireless devices |
| RFC1213-MIB.my | Standard MIB for system information |
| IF-MIB | Interface MIB |
| SNMPv2-MIB | Standard MIB for system information |
| BRIDGE-MIB | VLAN configuration information that pertains to EWC |
| P-BRIDGE-MIB | VLAN configuration information that pertains to EWC |
| Q-BRIDGE-MIB | VLAN configuration information that pertains to EWC |

### Siemens Proprietary MIB

| Title | Description |
|---|---|
| HIPATH-WIRELESS-HWC-MIB.my | Configuration and statistics related to EWC and associated objects |
| HIPATH-WIRELESS-PRODUCTS-MIB.my | Defines product classes |
| HIPATH-WIRELESS-DOT11-EXTNS-MIB.my | Extension to IEEE802dot11-MIB that complements standard MIB |
| HIPATH-WIRELESS-SMI.my | Root for Chantry/Siemens MIB |

## 802.11AC AND 802.11N CLIENTS

Please refer to the latest release notes for ExtremeWireless™ 10.41.09 or later and/or ExtremeWireless WiNG 5.9.02 or later for the list of compatibility test devices.

## RADIUS SERVERS AND SUPPLICANTS

### RADIUS Servers Used During Testing

| Vendor | Model OS | Version |
|---|---|---|
| FreeRADIUS | 1.1.6 | FreeRADIUS |
| FreeRADIUS | 1.0.1 | FreeRADIUS |
| IAS | 5.2.3790.3959 | Microsoft Server 2003 IAS |
| 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)Â  HW Base: ERS 4850 | ECA connection |
| Extreme | K6 | Â 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

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.