ExtremeCloud IQ Controller v10.17.03.0003 Release Notes

Enhancements, Changes, Supported Devices, and Known Issues

9039547-02
May 08, 2026

ABSTRACT

This release notes document for ExtremeCloud™ IQ Controller version 10.17.03.0003 outlines technical enhancements, supported hardware, installation guidance, and known limitations for IT professionals managing unified access networks. This maintenance release introduces several fixes, the elimination of outdated GUI controls and displays, and enhancements.

INTRODUCTION

The ExtremeCloud IQ Controller is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud IQ 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 CE1000 is an application on the Universal Compute Platform 1130C, replacing the E1120 appliance with similar functionality and limits. It supports up to 250 APs/Defenders and 2,000 users standalone, or 500 APs and 4,000 users in a high-availability setup.
- The CE2000 is an application on the Universal Compute Platform 2130C, replacing the E2120 and E2122 appliances with similar functionality and limits. It supports up to 2000 APs/Defenders and 16,000 users standalone, or 4,000 APs and 32,000 users in a high-availability setup.
- The CE3000 is an application on the Universal Compute Platform 3150C, replacing the E3120 and E3125 appliances with similar functionality and limits. It supports up to 10,000 APs/Defenders and 50,000 users standalone, or 20,000 APs and 100,000 users in a high-availability setup.
- The E1120 is an appliance that meets the needs of entry to mid-level deployments, and is scalable to 250 APs/Defenders, 100 switches, and 4,000 mobility sessions in high-availability mode.
- The E2120 is an appliance that meets the needs of medium-sized, high-density and mission-critical deployments. It supports up to 4,000 APs/Defenders, 800 switches, and 32,000 mobility sessions in high-availability mode. Optionally, a redundant power supply can be ordered separately.
- The E2122 is an appliance that meets the needs of medium-sized, high-density and mission-critical deployments. It supports up to 4,000 APs/Defenders, 800 switches, and 32,000 mobility sessions in high-availability mode. Optionally, a redundant power supply can be ordered separately.
- The E3120 is an appliance that meets the needs of high-density and mission-critical deployments. It supports up to 20,000 APs/Defenders, 2,000 switches, and 100,000 mobility sessions in high-availability mode. Optionally, a redundant power supply can be ordered separately.
- The E3125 is an appliance that meets the needs of high-density and mission-critical deployments. It supports up to 20,000 APs/Defenders, 2,000 switches, and 100,000 mobility sessions in high-availability mode. Optionally, a redundant power supply can be ordered separately.
- 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, VE6120H, and VE6120K offer elastic capacities to cover the full range of offerings as VMWare/MS Hyper-V/Linux KVM, ranging from VE6120/VE6120H/VE6120K-Small to VE6120/VE6120H/VE6120K-Large.
- The VE6125/VE6125K XL are virtual appliances that support up to 4,000 APs/Defenders, up to 400 switches, and 32,000 mobility sessions in high-availability mode, depending on the hosting hardware.

The ExtremeCloud IQ Controller can expand its capacity to meet any growing business needs. The hardware and virtual packages are available for purchase. The customer purchases adoption capacity as a Right-To-Use Subscription model, supporting flexible quantities (per managed device) and term (multiple-year extended term) options.

Changes in 10.17.03.0003	ID
Fixed an issue where policy roles configured with FQDN rule entries appeared blank after saving the configuration, caused by invalid application name references carried over during config import.	CFD-13816
Improved robustness of secure tunnel data traffic from ExtremeCloud IQ Controller to access points (APs).	CFD-14550
Added robustness to AP when 802.11mc is enabled.	CFD-14638
Fixed an issue where configuring WPA3 encryption using the Firefox browser would result in the display of incorrect dual-key options and, after saving, a GUI pop-up with an encryption error warning, preventing configuration completion.	CFD-15109
The Traffic Allocation Framework (TAF) configuration is now managed independently of OFDMA and Beam Forming (MU-MIMO) settings across all AP platforms, ensuring greater flexibility and preventing unintended changes when enabling advanced radio features.	CFD-15756
Improved Fast Transition roaming on Wi-Fi 7 APs to provide more reliable, low-latency client handoffs during movement.	CFD-15854
Fixed an issue under Administration → License → Entitlements and Activations tabs where filtering of logs using **From** and **To** date range was not working, and table columns could not be resized.	CFD-16136
Resolved an issue where some clients were not correctly transitioning from **Unregistered** to **Allow All**. Client roles are now updated as expected.	CFD-16236
Resolved an issue where AP LLDP neighbor advertisements were malformed when the same SSID was mapped to multiple radios, thereby ensuring standards-compliant LLDP packets and correct neighbor visibility on connected switches.	CFD-16296
Enhanced the AP discovery process to more reliably detect and reconnect APs to controllers, resulting in fewer cases where APs stay offline until rebooted.	CFD-16337
Fix provided to prevent AP4020 from sending excessive Pause Frames, resulting in lost connection.	CFD-16358
Improved Live session data structure handling to prevent deadlocks leading to hung task.	CFD-16485
Fixed slow GUI performance and "Exception:null" errors during navigation caused by an issue with memory management and garbage collection.	CFD-16605
Fix provided to detect and restart **radsecproxy** component if it does not restart properly due to race condition.	CFD-16616
Fixed a GUI bug in the Smart Poll Stats widget where expanding a defined poll IP caused subsequent IP addresses to display only their first octet instead of the full address.	CFD-16621

Changes in 10.17.03.0003	ID
Fix provided for the Configure → Networks → WLAN → Default VLAN → Add VLAN page where the **Save** button was not functioning properly when configuring a new VLAN.	CFD-16762

Enhancements in 10.17.03.0003	ID
Introduced the **Traffic Allocation Framework (TAF)** parameter on the Edit Device Group → Edit Profile → Radios → Advanced page and on the Devices → Access Points → Advanced → Overrides page.	XCC-7991

Changes in 10.17.02.0002	ID
Improved the handling of unsolicited Router Advertisements: they are now delivered only to the intended wireless client and are no longer sent back into the network, preventing potential traffic loops.	CFD-14235
Resolved an issue where Dashboard widgets appeared blank and the GUI page returned a 500 response.	CFD-14898
Introduced more robust radio settings to improve reliability and performance on AP5xx, AP4xx, and AP3xx devices.	CFD-15479
Improved policy handling on access points to ensure consistent role assignments and reliable synchronization during client join or leave events.	CFD-15658
Fixed an issue where SmartRF could malfunction in High Availability (HA) environments experiencing role instability, resulting in incorrect power and channel assignments.	CFD-15747
Improved system resilience by addressing conditions that could cause internal services and the management UI to become unresponsive over extended uptime.	CFD-15884
Fixed an issue where deleted multicast rules would reappear in the GUI after saving and reopening the page.	CFD-16034
Fixed a backend calculation issue that could cause 2.4 GHz channel utilization to show a negative “Available” percentage, thus ensuring that the Available value never falls below 0%.	CFD-16039
Resolved an issue in Guest Essentials that prevented users from logging in after registering through the email-passcode splash portal.	CFD-16055
Corrected an issue in ExtremeCloud IQ Controller where AP Ethernet RX byte statistics were not displayed for connected access points, thereby ensuring that complete Ethernet statistics are now shown in the GUI.	CFD-16171
Fixed an issue where a memory leak in the certificate management service could cause ExtremeCloud IQ Controller to run out of memory.	CFD-16224
Improved performance for AP5020-WW access points by adjusting the default Traffic Allocation Framework (TAF) behavior, resolving high client latency experienced by users after upgrading.	CFD-16229
Improved flash reliability on AP40xx and AP50xx by automatically detecting and correcting an incorrect flash format at boot.	WOS-8087

Enhancements in 10.17.01.0016	
Announcing GA for AP4060/X: Wi-Fi 7 2x2 quad-radio AP with dedicated security sensor, MLO support, dual IOT radios, IP67 weatherized design, extended temperature range (-40°C to +60°C), and full 802.3at functionality. Refer to AP4060 Datasheet for more information.	XCC-4182
Enhanced login security: A new back-off mechanism has been implemented across SSH, GUI, and REST API authentication to mitigate brute-force login attacks against ExtremeCloud IQ Controller. The mechanism is based on the originating IP plus username combination and increases the blackout window based on repeated failures.	XCC-5110
Enabled QEMU Guest Agent integration on ExtremeCloud IQ Controller for KVM deployments, allowing graceful shutdown/reboot and retrieval of basic guest details (IP, OS) from the hypervisor.	XCC-5318
Added support for Multi-Link Operation (MLO) for client devices capable of operating in Simultaneous Transmit and Receive (STR), Enhanced Multi-Link Single-Radio (EMLSR), or Multi-Link Single Radio (MLSR) modes.	XCC-5414
Added support for AP4060X-EG SKU for Egypt.	XCC-5810
Updated Password Policy Enforcement: ExtremeCloud IQ Controller now enforces a stronger password policy to enhance system security. The policy includes requirements for minimum length, complexity, password history, and lifetime.	XCC-5989
Added AirDefense Essentials and AirDefense Services Platform (ADSP) support with AP4020/X/FX and AP4060/X dedicated Radio 4 sensor and AP5020 sensor mode software defined radio (SDR). Basic WIPS functionality (Rogue detection and compliance reporting) are also supported.	XCC-6801
Added support for AP5020-IL SKU for Israel.	XCC-6822
Added support for Guest registration using a secure, time-limited passcode sent via email for Guest Essentials integration with ExtremeCloud IQ Controller.	XCC-7027

Changes in 10.17.01.0016	ID
Enhanced system stability by improving map calculation responsiveness and backend performance for large-scale environments.	CFD-13471
Fixed an issue that could cause APs to crash (in the main_HWCcomm process) under certain conditions.	CFD-13889
Fixed an issue where APs could randomly crash during SmartRF scanning due to mis-encoded packets; added enhanced checks to improve stability.	CFD-13889
Fixed an issue where RADIUS accounting data was not sent to the RADIUS server after client authentication, which could result in missing session records, usage statistics, or billing information.	CFD-14229

Changes in 10.17.01.0016	ID
Fixed an issue where the GUI did not support searching or filtering in the License Entitlements and Activation screen.	CFD-14607
Fixed an issue where AP Network port configuration could be lost during initial high availability setup.	CFD-14856
Fixed an issue where neighbor APs were not displayed in the SmartRF neighbor list; corrected handling of Smart-IE data in scan results.	CFD-14918
Corrected the GUI display where Channel Utilization and Channel Occupancy values were shown in the wrong columns.	CFD-14918
Rectified an issue where RF profile parameters were incorrectly switched between 2.4 GHz and 5 GHz radios.	CFD-14918
Fixed an issue where mesh configuration was missing in the AP3935 profile after the number of radios increased from two to three.	CFD-14981
Fixed an issue where the “Tunnel” column was missing from the Monitor → Devices → Access Points screen; the column has been restored.	CFD-14992/CFD-14992
Resolved an issue where 6 GHz APs could remain in AFC Pending state.	CFD-15041
Fixed an issue where assigning a specific AP profile could cause the AP’s eth0 interface to disappear; updated logic to properly initialize filter names and ensure safe string handling.	CFD-15086
Configuring WPA3 in Firefox may cause UI errors, including incorrect key options and encryption failures; this has been fixed to align with expected behavior.	CFD-15109
Fixed an issue where stale SmartRF neighbor entries appeared in the GUI by clearing old records before updating from AP scans.	CFD-15148
Enhanced Probe Request processing for greater stability and accuracy in client discovery, particularly under high-density or noisy RF conditions.	CFD-15194
Resolved multiple crashes related to sensor and WIPS processes by adding additional checks in sensor code.	CFD-15194/CFD-13889
Fixed an issue with LLDP power negotiation between the AP and the PSE, ensuring correct power allocation and stable operation.	CFD-15273
Fixed an issue where AP302W could repeatedly reboot in bootloader when connected to AP5020 in bridge mode and drawing power from its PSE port; updated PSE ON/OFF logic to prevent link and power cycling.	CFD-15273
Fixed an issue where a disabled SSID with radio shown as OFF in the GUI could still emit a 2.4 GHz signal; updated SmartRF logic to exclude that radio from channel updates when no WLAN is configured.	CFD-15290
Fixed an issue where AP5010 could reboot due to a kernel panic; improved memory handling and stack management for greater system stability.	CFD-15364
Improved Tx Max Power Handling for AFC Radios. AFC radios will now retain the user-selected Tx Max Power even when it falls outside the currently allowed range, preventing unintended changes when compliance data is unavailable.	CFD-15650
AFC AP-to-AP FTM ranging clears cached data too slowly, which can prevent persistence of geo-coordinates.	XCC-6512

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.10.17.03.0003	Maintenance Release	May 08, 2026
Previous Version	V.10.17.02.0002	Maintenance Release	March 26, 2026
Previous Version	V.10.17.01.0016	Feature Release	December 15, 2025

SUPPORTED CONTROLLER APPLICATIONS AND APPLIANCES, ACCESS POINTS, AND SWITCHES

Product Name	Image
Applications	
ExtremeCloud IQ Controller CE1000 application for Universal Compute Platform 1130C	XIQC-10.17.03.0003-1.dke
ExtremeCloud IQ Controller CE2000 application for Universal Compute Platform 2130C	XIQC-10.17.03.0003-1.gse
ExtremeCloud IQ Controller CE3000 application for Universal Compute Platform 3150C	XIQC-10.17.03.0003-1.bte
Appliances	
ExtremeCloud IQ Controller VE6120 VMware Min Supported ESXi version 5.1 or later, (tested 8.0)	XIQC-10.17.03.0003-1.dle
ExtremeCloud IQ Controller VE6120H (Windows server 2016 or later)	XIQC-10.17.03.0003-1.spe
ExtremeCloud IQ Controller VE6120K Linux KVM	XIQC-10.17.03.0003-1.dve
ExtremeCloud IQ Controller VE6125 Min Supported ESXi version 5.5 or later, (tested 7.0)	XIQC-10.17.03.0003-1.rse
ExtremeCloud IQ Controller VE6125K Linux KVM	XIQC-10.17.03.0003-1.mfe
ExtremeCloud IQ Controller E1120	XIQC-10.17.03.0003-1.sme
ExtremeCloud IQ Controller E2120	XIQC-10.17.03.0003-1.jse
ExtremeCloud IQ Controller E2122	XIQC-10.17.03.0003-1.wze
ExtremeCloud IQ Controller E3120	XIQC-10.17.03.0003-1.ose
ExtremeCloud IQ Controller E3125	XIQC-10.17.03.0003-1.dze
Access Points	
AP3000-WW	AP3xxx-LEAN-10.17.3.0-005R.img

Product Name	Image
AP3000X-WW	AP3xxx-LEAN-10.17.3.0-005R.img
AP302W-CAN AP302W-FCC AP302W-IL AP302W-WR	AP302W-LEAN-10.17.3.0-005R.img
AP305C-1-CAN AP305C-1-FCC AP305C-1-IL AP305C-1-WR AP305C-CAN AP305C-FCC AP305C-IL AP305C-WR AP305CX-CAN AP305CX-FCC AP305CX-IL AP305CX-WR	AP3xxC-LEAN-10.17.3.0-005R.img
AP310e-1-WR AP310e-CAN AP310e-FCC AP310e-IL AP310e-WR AP310i-1-WR AP310i-CAN AP310i-FCC AP310i-IL AP310i-WR	AP3xx-LEAN-10.17.3.0-005R.img
AP360e-CAN AP360e-FCC AP360e-IL AP360e-WR AP360i-CAN AP360i-FCC AP360i-IL AP360i-WR	AP3xx-LEAN-10.17.3.0-005R.img
AP3912i-FCC AP3912i-ROW	AP391x-10.51.28.0001.img
AP3915e-FCC AP3915e-ROW AP3915i-FCC AP3915i-ROW	AP391x-10.51.28.0001.img
AP3916ic-FCC AP3916ic-ROW	AP391x-10.51.28.0001.img
AP3916-camera	AP3916IC-V1-0-14-1.dlf
AP3917e-FCC AP3917e-ROW AP3917i-FCC AP3917i-ROW	AP391x-10.51.28.0001.img

Product Name	Image
AP3917k-FCC AP3917k-ROW	
AP3935e-FCC AP3935e-ROW AP3935i-FCC AP3935i-IL AP3935i-ROW	AP3935-10.51.28.0001.img
AP3965e-FCC AP3965e-ROW AP3965i-FCC AP3965i-ROW	AP3935-10.51.28.0001.img
AP4000-1-WW AP4000-WW	AP4000x-LEAN-10.17.3.0-005R.img
AP4020-WW	AP40xx-10.17.3.0-005R.img
AP4020FX-WW	AP40xx-10.17.3.0-005R.img
AP4020X-WW	AP40xx-10.17.3.0-005R.img
AP4060-WW	AP40xx-10.17.3.0-005R.img
AP4060X-WW	AP40xx-10.17.3.0-005R.img
AP410C-1-CAN AP410C-1-FCC AP410C-1-IL AP410C-1-WR AP410C-CAN AP410C-FCC AP410C-IL AP410C-WR	AP4xxC- LEAN-10.17.3.0-005R.img
AP410e-CAN AP410e-FCC AP410e-IL AP410e-WR AP410i-1-FCC AP410i-1-WR AP410i-CAN AP410i-FCC AP410i-IL AP410i-WR	AP4xx-LEAN-10.17.3.0-005R.img
AP460C-CAN AP460C-FCC AP460C-IL AP460C-WR AP460S12C-CAN AP460S12C-FCC AP460S12C-IL AP460S12C-WR AP460S6C-CAN AP460S6C-FCC AP460S6C-IL AP460S6C-WR	AP4xxC-LEAN-10.17.3.0-005R.img

Product Name	Image
AP460e-CAN AP460e-FCC AP460e-IL AP460e-WR AP460i-CAN AP460i-FCC AP460i-IL AP460i-WR	AP4xx-LEAN-10.17.3.0-005R.img
AP5010-WW	AP5xxx-LEAN-10.17.3.0-005R.img
AP5020-WW	AP5020-10.17.3.0-005R.img
AP5050D-WW	AP5xxx-LEAN-10.17.3.0-005R.img
AP5050U-WW	AP5xxx-LEAN-10.17.3.0-005R.img
AP505i-FCC AP505i-WR	AP5xx-LEAN-10.17.3.0-005R.img
AP510e-FCC AP510e-WR AP510i-1-FCC AP510i-1-WR AP510i-FCC AP510i-WR	AP5xx-LEAN-10.17.3.0-005R.img
AP560h-FCC AP560h-WR AP560i-FCC AP560i-WR	AP5xx-LEAN-10.17.3.0-005R.img
SA201	AP391x-10.51.28.0001.img
Switches	
210-12p-10GE2 210-24p-10GE2 210-48p-10GE2 210-12p-10GE2 POE 210-24p-10GE2 POE 210-48p-10GE2 POE	210-series_V1.02.05.0013.stk fp-connector-3.3.0.4.pyz (cloud connector)
220-12p-10GE2 220-24p-10GE2 220-48p-10GE2 220-12p-10GE2 POE 220-24p-10GE2 POE 220-48p-10GE2 POE	220-series_V1.02.05.0013.stk fp-connector-3.3.0.4.pyz (cloud connector)
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 X440G2-24t-10G4 X440G2-48t-10G4 X440G2-12t-10G4 POE X440G2-24t-10G4 POE X440G2-48t-10G4 POE	summitX-30.2.1.8-patch2-5.xos summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod (cloud connector)

Product Name	Image
X465_24W X465_48T X465_48P X465_48W X465_24MU X465_24MU_24W	onie-30.2.1.8-patch2-5-vpex_controlling_bridge.lst onie-30.2.1.8-cloud_connector-3.4.1.20.xmod
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	Version
ExtremeControl™	22.3 or higher
ExtremeAnalytics™	22.3 or higher
ExtremeCloud™ A3	4.0
ExtremeCloud™ IQ-Site Engine	22.3 or higher

Air Defense	Version
ExtremeAirDefense™	10.6.2
ExtremeGuest	**Version**
ExtremeGuest™	6.0.1.0-001

Note:

Platform and Access Point Configuration functions are not supported by ExtremeManagement™. ExtremeCloud™ IQ Site Engine v21.9 or greater is required.

Extreme Platform ONE ─ ExtremeCloud IQ Pilot Twin License Provides Backwards Compatibility

Some versions of ExtremeCloud IQ Site Engine and ExtremeCloud IQ Controller do not support Extreme Platform ONE licenses. To provide you with the necessary time to upgrade to later versions, every Extreme Platform ONE Standard subscription includes an ExtremeCloud IQ Pilot Twin license with the same start date, end date, and licensed quantity.

- The Extreme Portal shows both Extreme Platform ONE Standard and ExtremeCloud IQ Pilot Twin licenses.
- ExtremeCloud IQ (Classic) and ExtremeCloud IQ (New) do not show ExtremeCloud IQ Pilot Twin licenses.
- Extreme Platform ONE (that is, Extreme Platform ONE Networking or Extreme Platform ONE Security) does not show ExtremeCloud IQ Pilot Twin licenses.
- ExtremeCloud IQ Site Engine version 25.2 and earlier supports ExtremeCloud IQ Pilot and ExtremeCloud IQ Pilot Twin licenses.

- ExtremeCloud IQ Site Engine version 25.5 and later supports ExtremeCloud IQ Pilot licenses and Extreme Platform ONE subscriptions.
- ExtremeCloud IQ Controller versions support ExtremeCloud IQ Pilot and ExtremeCloud IQ Pilot Twin licenses.

Note:

If you purchased Extreme Platform ONE subscriptions and are running management application versions that are incompatible with Extreme Platform ONE subscriptions, you can use the provided ExtremeCloud IQ Pilot Twin licenses.

INSTALLATION INFORMATION

Application and Appliance Installations	
CE1000, CE2000, CE3000	ExtremeCloud IQ Controller CE1000, CE2000, CE3000 Deployment Guide
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
E3125	Extreme Campus Controller E3125 Installation Guide
VE6120/VE6125	Extreme Campus Controller VE6120/VE6125 Installation Guide
VE6120H	Extreme Campus Controller VE6120H Installation Guide
VE6120K/VE6125K	Extreme Campus Controller VE6120K/VE6125K Installation Guide

KNOWN RESTRICTIONS AND LIMITATIONS

Known Restriction or Limitation	ID
Certain wireless clients (such as Qualcomm Killer Wireless 1535 and Intel 7265D/8260/8265) have been known to not complete the 4-way handshake required to fulfill the association process in networks that have both PMF/MFP (802.11w) and Fast-Transition (802.11r [FT]) enabled. The currently recommended workaround is to not enable PMF/MFP configuration on a service that is also using 802.11r. Such clients have been demonstrated to work correctly on services with just 802.11r (FT) enabled.	nse0003416
AP4020X/FX radios using Operational Mode 2 (2.4/5H/5L GHz) do not support transmit power for 160 MHz channels, unlike other AP models. Note that 5 GHz Low has only one 160 MHz channel; therefore, it is advised that 160 MHz channel not be used in enterprise deployments.	WOS-7664
Using the AP traffic capture feature on version 10.17 may cause an AP crash. This issue is under investigation and will be resolved in a future release.	XCC-8022

Known Restriction or Limitation	ID
Mesh-related instability may occur on Wi-Fi 7 APs in rare corner cases. This issue is under investigation and will be resolved in a future release.	XCC-8024
Release 10.15.01 introduced RADSEC (RADIUS over TLS) support for secure administrator logins using AAA Policies, replacing traditional RADIUS configurations with encrypted authentication. When upgrading from a version without RADSEC support, the system needs to create a new AAA Policy. However, if the maximum number of AAA Policies has already been reached, the upgrade will fail because the new policy cannot be created. To avoid this, ensure there is available capacity for additional AAA Policies before upgrading.	XCC-6686
When configuring attenuation on legacy APs (non-Wi-Fi 7), changing the Radio 1 attenuation value will also update Radio 2 attenuation to the same value. To set different values, users must manually adjust Radio 2 attenuation after changing Radio 1. This behavior does not impact Wi-Fi 7 APs, which intentionally link Radio 1 and Radio 2 attenuation. Users can avoid unintended changes by reviewing and adjusting attenuation values before saving, refreshing the page to restore previous settings if needed, or checking the audit log for earlier values if changes have already been saved.	XCC-7143
After upgrading ExtremeCloud IQ Controller to a new image: • The AFC spectrum is preserved and the 6GHz Standard Power (SP) service is maintained. • The geo coordinates derived by the Geo-Location Agent are **not** preserved, and users have 24H to restore the Geo-Location Agent coordinates for **each floor** by first activating the **Range** button, then the **Derive-Location** button (on the **Subgraph** page under the **Geo Diagnostics** tab). If this action is not taken within 24H, the AFC SP spectrum will expire, and SP service will be revoked. This issue will be addressed in a future release.	XCC-6847
AP4020/X/FX models are unable to save the AFC Fallback channel configuration. This issue will be addressed in a future release.	XCC-6861
AP5020 – Channels 165 (20 MHz) and 106 (80 MHz) are disabled for Isle of Man due to a known issue. This issue will be resolved in a future release.	WOS-7682
Indoor AFC deployment After importing an Ekahau floor map into ExtremeCloud IQ Controller, APs that are not properly associated with existing devices appear as “?” on the map. Using the **Assign to Floor** option to associate these APs may cause inconsistencies. Recommended Workflow: Right-click each “?” AP and manually associate it with the correct device before proceeding with Indoor AFC deployment.	XCC-6603
Language Selection in Internal Captive Portal on iOS Issue Summary: When using the internal captive portal in ExtremeCloud IQ Controller with multiple language options enabled, iOS devices may encounter an error when switching languages.	XCC-6368

Known Restriction or Limitation	ID
Status: This is a known issue under investigation. Updates will be provided in future releases as feasible.	
Controller functions, including internal communications and containerized applications, require the usage of reserved address space. Two subnets are reserved internally to the controller: • 172.17.0.0/24 • 172.31.0.16/28 The user interface prevents assigning IP addresses to local interfaces (physical or virtual) that conflict with these ranges.	XCC-3121
For ExtremeCloud IQ Controller (v5) systems previously onboarded into an ExtremeCloud IQ account for visibility, following an upgrade to ExtremeCloud IQ Controller (v10), you must remove and redeclare the controller to ExtremeCloud IQ. This will facilitate the re-synchronization of the controller with the ExtremeCloud IQ account.	XCC-2463
Before installing a new ExtremeCloud IQ Controller license, you must configure Network Time Protocol (NTP) Server settings. Licensing management is dependent on accurate NTP configuration. Configure NTP via the ExtremeCloud IQ Controller initial Configuration Wizard or go to Admin → System → Network Time to configure and verify the NTP settings.	XCC-2353
For ExtremeCloud IQ Controller configured for authentication of administrators over RADIUS server, the GUI responsiveness may be slow, possibly over 30 seconds if the target server(s) are unavailable or unreachable at login time. If the outage is extensive, the system will eventually timeout to validate against local credentials when provisioned.	XCC-2350
To improve stability of mesh when SmartRF is used with a mesh root AP: • Use fixed channel width. • Set SmartRF sensitivity to "Low" to decrease the time that the AP will abandon the channel for scanning.	XCC-1684
WPA3-Enterprise-192-bit authentication does not work in version 10.17.1.0. It will be addressed in a future release.	WOS-7950
On rare occasions, AP5020 may stop accepting client connections after several days have lapsed and while 802.11mc ranging has been enabled. The issue is under investigation. Workaround: Disable 802.11mc. If AP5020 is operating at standard power, allow 802.11mc to converge, then disable it once the AP5020 units are on standard power.	WOS-7935
In rare cases, AP5010U may experience unexpected instability after upgrading to build 10.17.01. The root cause is under investigation. This behavior was not observed in prior releases. Workaround: Set the OCS scan list to 40 MHz or 20 MHz.	WOS-7930
Beacon Protection (BP) is configured per WLAN. If any 6 GHz network has Beacon Protection enabled, all Multi-Link Operation (MLO) networks must also have BP enabled to ensure proper functionality.	WOS-7908
In certain corner situation enabling MLO may result in reduced uplink throughput. This is end-client driver dependent.	WOS-7879

Known Restriction or Limitation	ID
When Beacon Protection is enabled, wireless clients initiate de-authentication shortly after they get authenticated. Intel BE200 clients consistently de-authenticate, while other clients experience intermittent de-authentication issues. Note, however, that Beacon Protection is disabled by default.	WOS-7872
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
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
Important Note: • 802.11mc is not recommended for use on 2.4 GHz. • Supported AP models for 11mc on 5 GHz: AP5020, AP5010, AP3000, and AP5050. • 6 GHz 11mc support is currently exclusive to AP5020, with expansion to other models planned in future releases.	WOS-5655
For the Access Point Test feature, when using the wireless client option for the 5GHz band, if the Access Point is operating in dual-5GHz mode, and Radio 1 is set to 5GHz low (not 2.4GHz), the AP as a client will operate on the 5GHz low band. This may limit the test client's capability to connect to the infrastructure APs that operate in the 5GHz high band. Recommendation: Only exercise wireless AP Test on devices that are configured for full-band mode.	XCC-3284
AP3900 series requires a minimum firmware revision of 10.41.01 (or later) for onboarding into ExtremeCloud IQ Controller. Customers migrating from ExtremeWireless installations or onboarding new AP3900 inventory to ExtremeCloud IQ Controller must ensure APs are running at least the minimum revision prior to onboarding. Depending on the age of the inventory, this may require a manual upgrade of the unit firmware outside of the management framework.	XCC-3178
AP4020/X/FX and AP4060/X Radio 4 sensor functionality is restricted to basic WIPS and Reporting.	WOS-7913
The AP4020 Radio 4 sensor may fail to detect its own 2.4 GHz and 5 GHz BSS while detecting other BSS. This behavior is under investigation, and no workaround is currently available.	WOS-7802
AP4020/X/FX and AP4060/X Radio 4 detection and sensing capabilities are limited to legacy rates.	WOS-7792
With 11r enabled on an 802.1x network, a Windows 10 PC with an Intel Wi-Fi card (ax200, ax210), running driver version 22.170.0.3 cannot reconnect automatically after an MU is disconnected. The workaround is to toggle the Wi-Fi off and on from the PC.	WOS-4480
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.	Info

Known Restriction or Limitation	ID
For AP deployments in remote locations where APs 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. 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 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 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. During upgrade periods, the Availability link will only re-establish when both the appliance status of availability link and synchronization status can be found. Go to: • “Network Health" widget on the Dashboard, or • Administration → System → Availability	Info ECA-776
Recommendation settings for setup of redundant RADIUS server authentication: • Response Window to 5s [Default: 20s] • Revival Interval to 10s [Default: 60s]	Info ECA-875

SUPPORTED WEB BROWSERS

For ExtremeCloud IQ Controller management GUI, the following Web browsers were tested for interoperability:

Browsers	Version	OS
Chrome	117.0.5938.152	Windows 10 Windows 11
Microsoft Edge	117.0.2045.60	Windows 10 Windows 11
Firefox	118.0.01	Windows 10 Windows 11

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

For Wireless Clients (Captive Portal, AAA), recommended browsers are:

Browsers	Version	OS
Chrome	117.0.5938.152	Windows 10 Windows 11
Microsoft Edge	117.0.2045.60	Windows 10
Firefox	118.0.01	Windows 10 Windows 11
Safari	15.4 (17613.1.17.1.13)	iOS 16.7.1

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.

ExtremeCloud IQ 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
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

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
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
Appliance	Appliance	TCP	Any	6380	REDIS	High Availability (HA) Pair Configuration Synchronization	Yes
Core Back-End Communication							
Appliance	DNS Server	UDP	Any	53	DNS	If using DNS	Optional
Appliance	Syslog Server	UDP	Any	514	Syslog	If Appliance logs to external syslog server	Optional
Appliance	RADIUS Server	UDP	Any	1812	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Appliance	RADIUS Server	UDP	Any	1813	RADIUS Accounting	If enabled RADIUS accounting	Optional
Appliance	RADIUS server	UDP	Any	1814	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Appliance	RADIUS server	UDP	Any	1815	RADIUS Accounting	If enabled RADIUS Accounting	Optional

[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
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

Title	Description
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

Vendor	Model OS	Version
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 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	XIQC connection
Extreme	X440G2-48p-10G4	21.1.1.4	XIQC connectivity
Extreme	Summit 300-48	7.6e1.4	XIQC connection
Extreme	VSP-4850GTS-PWR	(6.0.1.1_B003) (PRIVATE) HW Base: ERS 4850	XIQC connection
Extreme	K6	08.63.02.0004	XIQC connection
Extreme	K6	08.42.03.0006	XIQC connection
Extreme	X440G2-48p-10GE4	21.1.5.2	XIQC connection
Extreme	X440-G2-12p	21.1.1.4	XIQC connection
Extreme	X460-48p	12.5.4.5	XIQC connection
Cisco	Catalyst 3550	12.1(19)EA1c	XIQC 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
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/

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.

LEGAL

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software, or any specifications described or referred to in this document are subject to change without notice.

Trademarks

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.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks