



# ExtremeCloud IQ Controller v10.14.03.0004 Release Notes

Enhancements, Changes, Supported Devices, and Known Issues

9039276-02  
October 15, 2025

## ABSTRACT

This release notes document for ExtremeCloud™ IQ Controller version 10.14.03.0004 outlines technical enhancements, supported hardware, installation guidance, and known limitations for IT professionals managing unified access networks. This maintenance release introduces changes, such as improved client discovery and AP management operations, as well as corrections to GUI displays and controls.

## 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 2,000 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 10.14.03.0004                                                                                                                                                                                                                                                   | ID        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Enhanced Probe Request processing for greater stability and accuracy in client discovery, particularly under high-density or noisy RF conditions.                                                                                                                          | CFD-15194 |
| Fixed an issue where stale SmartRF neighbor entries appeared in the GUI by clearing old records before updating from AP scans.                                                                                                                                             | CFD-15148 |
| Added more configuration checks to ensure proper AP startup.                                                                                                                                                                                                               | CFD-15086 |
| Removed the deprecated Voice Aware Sensing option from the GUI to align with current feature support and eliminate outdated configuration settings.                                                                                                                        | CFD-15047 |
| Resolved an issue that could cause access points to remain stuck in AFC Pending state.                                                                                                                                                                                     | CFD-15041 |
| Fixed an issue where the "Tunnel" column was missing from the Monitor → Devices → Access Points screen; the column has been restored.                                                                                                                                      | CFD-14992 |
| Addressed an issue where mesh configuration was missing in the AP3935 profile after the number of radios increased from two to three.                                                                                                                                      | CFD-14981 |
| Rectified an issue where RF profile parameters were incorrectly switched between 2.4 GHz and 5 GHz radios.                                                                                                                                                                 | CFD-14918 |
| Resolved an issue where Dashboard widgets appeared blank, and the GUI page returned a 500 response.                                                                                                                                                                        | CFD-14898 |
| Corrected the GUI display where Channel Utilization and Channel Occupancy values were shown in the wrong columns.                                                                                                                                                          | XCC-6879  |
| Corrected AP neighbor report sent to ExtremeCloud IQ Controller.                                                                                                                                                                                                           | WOS-7709  |
| Addressed a problem where APs could not be assigned to a Site using the Access Point configuration option.                                                                                                                                                                 | CFD-14758 |
| Fixed an issue where Docker environment variable values containing equal signs (=) were incorrectly truncated after saving. The parsing logic was updated to preserve all characters in the value field, ensuring accurate configuration of complex environment variables. | CFD-14611 |
| Fixed an issue where the GUI did not support searching or filtering in the License Entitlements and Activation screen.                                                                                                                                                     | CFD-14607 |
| Resolved an issue, where generating tech support on "All" failed, by improving the Redis scanning process.                                                                                                                                                                 | CFD-14587 |
| Addressed an issue where AP3912 and AP302W models may have missing eth1-3/P1-3 ports configuration option under Device Profile Networks. This issue was observed in release 10.14.01, specifically.                                                                        | CFD-14479 |
| Rectified an issue that prevented the ExtremeCloud IQ Controller UI from loading in ExtremeCloud IQ at certain sites, where affected controllers returned an HTTP 503 response.                                                                                            | CFD-14411 |

| Changes in 10.14.03.0004                                                                                                                                                                       | ID        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Addressed skb (socket buffer) corruption, improving packet handling stability and reducing the likelihood of kernel memory inconsistencies under heavy network load.                           | CFD-13856 |
| Optimized Hotspot processing to prevent AP poll timeouts.                                                                                                                                      | CFD-13829 |
| Resolved an issue where ExtremeCloud IQ Controller was unable to decrypt the shared secret configured with the RADIUS server resulting in Disconnect/CoA reauthentication requests timing out. | CFD-13707 |

| Changes in 10.14.02.0002                                                                                                                                         | ID        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Resolved a display issue affecting statistics for 3-hour and 14-hour data collection intervals.                                                                  | CFD-13783 |
| Resolved an issue where the country code changed unexpectedly when switching from ExtremeCloud IQ to ExtremeWireless Wing during the standard OS change process. | CFD-14311 |
| Addressed an issue that caused client connection failures when using OWE transition mode with MAC authentication enabled.                                        | CFD-14493 |
| Fixed an issue where invalid AP coordinates are generated, placing them too far apart and preventing radio initialization.                                       | CFD-14552 |

| Enhancements in 10.14.01.0029                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ID       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| We are pleased to introduce an extension to the current <b>OWE Transition Auto Provisioning</b> mode for the 6 GHz radio. With the existing OWE Transition Auto Provisioning mode, when an open SSID is created on the 2.4 GHz and 5 GHz bands, a hidden companion OWE SSID is also created on the 2.4 and 5 GHz bands. With this new feature, we now support the creation of the same SSID with OWE on the 6 GHz radio. This enhancement facilitates the migration of clients from the 2.4 GHz and 5 GHz bands to the 6 GHz band. | XCC-5194 |
| Added a new L3/L4 Rules panel with controls to specify source and destination addresses and ports when creating ACL rules. Rules created here are listed in tabular form.                                                                                                                                                                                                                                                                                                                                                          | XCC-5818 |
| Added the <b>Type of Place</b> field under Configuration>Sites>Location tab as an update to the RFC 4776 Civic Attributes.                                                                                                                                                                                                                                                                                                                                                                                                         | XCC-5837 |
| Added support for country of Tuvalu for the following Access Points: AP302W-WR, AP460C-WR, and AP305C-WR.                                                                                                                                                                                                                                                                                                                                                                                                                          | XCC-6077 |
| Added support for country of Senegal and Panama for the AP4000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | XCC-6106 |
| Added a country-specific SKU for Israel: AP4020-IL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | XCC-6189 |
| Renewed the captive portal certificate on Access Points to extend validity to June 2026.                                                                                                                                                                                                                                                                                                                                                                                                                                           | WOS-7115 |
| Renewed the captive portal certificate on AP39XX to extend its validity through June 2026. This is final captive portal certificate renewal for AP39XX.                                                                                                                                                                                                                                                                                                                                                                            | WOS-7481 |

| Changes in 10.14.01.0029                                                                                                                                              | ID        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Optimized floor plan upload performance.                                                                                                                              | CFD-12910 |
| Enhanced the reliability of the connection between ExtremeCloud IQ Controller and Access Points to ensure more stable communications.                                 | CFD-13143 |
| Addressed a configuration issue where role bandwidth limits failed to persist.                                                                                        | CFD-13277 |
| Improved Access Point memory usage for large data blocks.                                                                                                             | CFD-13341 |
| Enhanced wireless driver settings with additional configuration validation to ensure correct setup and prevent misconfiguration.                                      | CFD-13590 |
| Support for TLSv1.3 has been added to peer-to-peer communication, enhancing connection stability.                                                                     | CFD-13765 |
| Improved system log parsing to prevent performance issues under certain conditions.                                                                                   | CFD-13906 |
| Since weaker 1024-bit key size certificates are deprecated, the UI is updated to remove 1024-bit key size for generating an Access Point Certificate Signing Request. | CFD-14076 |
| Added workaround Access Point CLI command to disable Application Identification.                                                                                      | WOS-7417  |
| AP4020 USB function is now available under AT power source.                                                                                                           | WOS-7377  |
| Improved data plane packet handling to address potential issues in certain corner cases.                                                                              | WOS-7437  |

**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.10.14.03.0004 | Maintenance Release | October 15, 2025 |
| Previous Version | V.10.14.02.0002 | Maintenance Release | July 24, 2025    |
| Previous Version | V.10.14.01.0029 | Feature Release     | June 20, 2025    |

## SUPPORTED CONTROLLER APPLICATIONS AND APPLIANCES, ACCESS POINTS, AND SWITCHES

| Product Name                                                                                  | Image                          |
|-----------------------------------------------------------------------------------------------|--------------------------------|
| <b>Applications</b>                                                                           |                                |
| ExtremeCloud IQ Controller CE1000 application for Universal Compute Platform 1130C            | XIQC-10.14.03.0004-1.dke       |
| ExtremeCloud IQ Controller CE2000 application for Universal Compute Platform 2130C            | XIQC-10.14.03.0004-1.gse       |
| ExtremeCloud IQ Controller CE3000 application for Universal Compute Platform 3150C            | XIQC-10.14.03.0004-1.bte       |
| <b>Appliances</b>                                                                             |                                |
| ExtremeCloud IQ Controller VE6120 VMware Min Supported Six version 5.1 or later, (tested 8.0) | XIQC-10.14.03.0004-1.dle       |
| ExtremeCloud IQ Controller VE6120H (Windows server 2016 or later)                             | XIQC-10.14.03.0004-1.spe       |
| ExtremeCloud IQ Controller VE6120K Linux KVM                                                  | XIQC-10.14.03.0004-1.dve       |
| ExtremeCloud IQ Controller VE6125 Min Supported Six version 5.5 or later, (tested 7.0)        | XIQC-10.14.03.0004-1.rse       |
| ExtremeCloud IQ Controller VE6125K Linux KVM                                                  | XIQC-10.14.03.0004-1.mfe       |
| ExtremeCloud IQ Controller E1120                                                              | XIQC-10.14.03.0004-1.sme       |
| ExtremeCloud IQ Controller E2120                                                              | XIQC-10.14.03.0004-1.jse       |
| ExtremeCloud IQ Controller E2122                                                              | XIQC-10.14.03.0004-1.wze       |
| ExtremeCloud IQ Controller E3120                                                              | XIQC-10.14.03.0004-1.ose       |
| ExtremeCloud IQ Controller E3125                                                              | XIQC-10.14.03.0004-1.dze       |
| <b>Access Points</b>                                                                          |                                |
| AP3000-WW                                                                                     | AP3xxx-LEAN-10.14.3.0-003R.img |
| AP3000X-WW                                                                                    | AP3xxx-LEAN-10.14.3.0-003R.img |
| AP302W-CAN<br>AP302W-FCC<br>AP302W-IL<br>AP302W-WR                                            | AP302W-LEAN-10.14.3.0-003R.img |
| AP305C-1-CAN<br>AP305C-1-FCC<br>AP305C-1-IL<br>AP305C-1-WR                                    | AP3xxC-LEAN-10.14.3.0-003R.img |

| Product Name                                                                                                                           | Image                         |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| AP305C-CAN<br>AP305C-FCC<br>AP305C-IL<br>AP305C-WR<br>AP305CX-CAN<br>AP305CX-FCC<br>AP305CX-IL<br>AP305CX-WR                           |                               |
| AP310e-1-WR<br>AP310e-CAN<br>AP310e-FCC<br>AP310e-IL<br>AP310e-WR<br>AP310i-1-WR<br>AP310i-CAN<br>AP310i-FCC<br>AP310i-IL<br>AP310i-WR | AP3xx-LEAN-10.14.3.0-003R.img |
| 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-10.14.3.0-003R.img |
| AP3912i-FCC<br>AP3912i-ROW                                                                                                             | AP391x-10.51.27.0001.img      |
| AP3915e-FCC<br>AP3915e-ROW<br>AP3915i-FCC<br>AP3915i-ROW                                                                               | AP391x-10.51.27.0001.img      |
| AP3916ic-FCC<br>AP3916ic-ROW                                                                                                           | AP391x-10.51.27.0001.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-10.51.27.0001.img      |
| AP3935e-FCC<br>AP3935e-ROW<br>AP3935i-FCC<br>AP3935i-IL<br>AP3935i-ROW                                                                 | AP3935-10.51.27.0001.img      |
| AP3965e-FCC<br>AP3965e-ROW                                                                                                             | AP3935-10.51.27.0001.img      |

| Product Name                                                                                                                                                                       | Image                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| AP3965i-FCC<br>AP3965i-ROW                                                                                                                                                         |                                 |
| AP4000-1-WW<br>AP4000-WW                                                                                                                                                           | AP4000x-LEAN-10.14.3.0-003R.img |
| AP4020-WW                                                                                                                                                                          | AP40xx-10.14.1.0-028R.img       |
| AP410C-1-CAN<br>AP410C-1-FCC<br>AP410C-1-IL<br>AP410C-1-WR<br>AP410C-CAN<br>AP410C-FCC<br>AP410C-IL<br>AP410C-WR                                                                   | AP4xxC-LEAN-10.14.3.0-003R.img  |
| AP410e-CAN<br>AP410e-FCC<br>AP410e-IL<br>AP410e-WR<br>AP410i-1-FCC<br>AP410i-1-WR<br>AP410i-CAN<br>AP410i-FCC<br>AP410i-IL<br>AP410i-WR                                            | AP4xx-LEAN-10.14.3.0-003R.img   |
| AP460C-CAN<br>AP460C-FCC<br>AP460C-IL<br>AP460C-WR<br>AP460S12C-CAN<br>AP460S12C-FCC<br>AP460S12C-IL<br>AP460S12C-WR<br>AP460S6C-CAN<br>AP460S6C-FCC<br>AP460S6C-IL<br>AP460S6C-WR | AP4xxC-LEAN-10.14.3.0-003R.img  |
| AP460e-CAN<br>AP460e-FCC<br>AP460e-IL<br>AP460e-WR<br>AP460i-CAN<br>AP460i-FCC<br>AP460i-IL<br>AP460i-WR                                                                           | AP4xx-LEAN-10.14.3.0-003R.img   |
| AP5010-WW                                                                                                                                                                          | AP5xxx-LEAN-10.14.3.0-003R.img  |
| AP5020-WW                                                                                                                                                                          | AP5020-10.14.1.0-028R.img       |
| AP5050D-WW                                                                                                                                                                         | AP5xxx-LEAN-10.14.3.0-003R.img  |
| AP5050U-WW                                                                                                                                                                         | AP5xxx-LEAN-10.14.3.0-003R.img  |

| Product Name                                                                                                               | Image                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| AP505i-FCC<br>AP505i-WR                                                                                                    | AP5xx-LEAN-10.14.3.0-003R.img                                                                       |
| AP510e-FCC<br>AP510e-WR<br>AP510i-1-FCC<br>AP510i-1-WR<br>AP510i-FCC<br>AP510i-WR                                          | AP5xx-LEAN-10.14.3.0-003R.img                                                                       |
| AP560h-FCC<br>AP560h-WR<br>AP560i-FCC<br>AP560i-WR                                                                         | AP5xx-LEAN-10.14.3.0-003R.img                                                                       |
| SA201                                                                                                                      | AP391x-10.51.27.0001.img                                                                            |
| <b>Switches</b>                                                                                                            |                                                                                                     |
| 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<br>fp-connector-3.3.0.4.pyz (cloud connector)                          |
| X435-24P/T-4S                                                                                                              | summitlite_arm-30.7.1.1.xos<br>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-3.4.1.8.xmod<br>(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<br>onie-30.2.1.8-cloud_connector-3.4.1.20.xmod   |
| X620-16x                                                                                                                   | summitX-30.2.1.8-patch2-5.xos<br>summitX-30.2.1.8-cloud_connector-3.4.1.8.xmod<br>(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**

| <b>Application and Appliance Installations</b> |                                                                                    |
|------------------------------------------------|------------------------------------------------------------------------------------|
| CE1000, CE2000, CE3000                         | <a href="#">ExtremeCloud IQ Controller CE1000, CE2000, CE3000 Deployment Guide</a> |
| E1120                                          | <a href="#">Extreme Campus Controller E1120 Installation Guide</a>                 |
| E2120                                          | <a href="#">Extreme Campus Controller E2120 Installation Guide</a>                 |
| E2122                                          | <a href="#">Extreme Campus Controller E2122 Installation Guide</a>                 |
| E3120                                          | <a href="#">Extreme Campus Controller E3120 Installation Guide</a>                 |
| E3125                                          | <a href="#">Extreme Campus Controller E3125 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>               |
| VE6120K/VE6125K                                | <a href="#">Extreme Campus Controller VE6120K/VE6125K Installation Guide</a>       |

**KNOWN RESTRICTIONS AND LIMITATIONS**

| <b>Known Restriction or Limitation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>ID</b>  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| On iOS devices, selecting Polish as the Captive Portal language may not apply correctly.                                                                                                                                                                                                                                                                                                                                                                                                                      | XCC-6368   |
| 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 |
| Starting in 10.14.01, for existing and new AFC deployments, users will not be able to save floor plans unless AP Height Above Floor Uncertainty field has a non-zero value configured. Existing deployments will require a reconfiguration of all floor plans when upgrading from an earlier release.                                                                                                                                                                                                         | XCC-6396   |
| APs used in AFC Indoor configuration (AP5050, AP5010, AP5020, AP3000) must not use 5 GHz radio for MESH connection, since this radio is necessary for performing FTM AP-to-AP ranging.                                                                                                                                                                                                                                                                                                                        | XCC-6464   |
| When heatmaps are enabled for the "Level 2" map, the GUI spins for several minutes before displaying the error: "Failed to calculate floor maps."                                                                                                                                                                                                                                                                                                                                                             | XCC-6202   |
| An issue is being investigated where the local authentication database is queried even when external RADIUS server priority is set higher. This may happen when the same username is                                                                                                                                                                                                                                                                                                                          | XCC-5804   |

| Known Restriction or Limitation                                                                                                                                                                                                                                                                                                                                                                                                     | ID       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| configured both on the external RADIUS server and the local user database.                                                                                                                                                                                                                                                                                                                                                          |          |
| <p>Controller functions, including internal communications and containerized applications, require the usage of reserved address space. Two subnets are reserved internally to the controller:</p> <ul style="list-style-type: none"> <li>• 172.17.0.0/24</li> <li>• 172.31.0.16/28</li> </ul> <p>The user interface prevents assigning IP addresses to local interfaces (physical or virtual) that conflict with these ranges.</p> | 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 |
| When ExtremeCloud IQ Controller is configured for authentication of administrators via RADIUS server, the GUI responsiveness may be slow. It may take over 30 seconds to respond if the target server(s) are unavailable or unreachable at login time. If the outage is extensive, the system will eventually time out to validate against local credentials when provisioned.                                                      | XCC-2350 |
| ExtremeCloud IQ-Site Engine 22.3.10 is the minimum required revision for representation of ExtremeCloud IQ Controller 10.01.01 or later revisions. Extreme Management Center (8.5.x or later) does NOT recognize a controller running ExtremeCloud IQ Controller 10.01.01 or later.                                                                                                                                                 | XCC-2348 |
| <p>To improve stability of mesh when SmartRF is used with a mesh root AP:</p> <ul style="list-style-type: none"> <li>• Use fixed channel width.</li> <li>• Set SmartRF sensitivity to "Low" to decrease the time that the AP will abandon the channel for scanning.</li> </ul>                                                                                                                                                      | XCC-1684 |
| <p>Important Note:</p> <ul style="list-style-type: none"> <li>• 802.11mc is not recommended for use on 2.4 GHz.</li> <li>• Supported AP models for 11mc on 5 GHz: AP5020, AP5010, AP3000, and AP5050.</li> <li>• 6 GHz 11mc support is currently exclusive to AP5020, with expansion to other models planned in future releases.</li> </ul>                                                                                         | WOS-5655 |
| 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  |

| Known Restriction or Limitation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | ID       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 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 |
| 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.<br>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 |
| 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 |
| 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     |
| 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 | Info     |

| Known Restriction or Limitation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ID                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <p>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.</p> <p>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>    |
| <p>WLAN standard 11mc not recommended for 2.4GHz band; it works better with wider channels.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>Info</p>                |

**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<br>Windows 11 |
| Microsoft Edge | 117.0.2045.60  | Windows 10<br>Windows 11 |
| Firefox        | 118.0.01       | Windows 10<br>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<br>Windows 11 |
| Microsoft Edge | 117.0.2045.60          | Windows 10               |
| Firefox        | 118.0.01               | Windows 10<br>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 |
|---------------------------------------------|--------------|--------------------|----------|---------------|----------------|-----------------------------------------------------|---------------------|
| <b>Ports for AP/Appliance Communication</b> |              |                    |          |               |                |                                                     |                     |
| Appliance                                   | Access Point | UDP                | Any      | 13910         | WASSP          | Management and Data Tunnel between AP and Appliance | Yes                 |
| Access Point                                | Appliance    | UDP                | Any      | 13910         | WASSP          | Management and Data Tunnel between AP and Appliance | Yes                 |
| Appliance                                   | Access Point | UDP                | 4500     | Any           | Secured WASSP  | Management Tunnel between AP and Appliance          | Optional            |
| Access Point                                | Appliance    | UDP                | Any      | 4500          | Secured WASSP  | Management Tunnel between AP and Appliance          | Optional            |
| Access Point                                | Appliance    | UDP                | Any      | 13907         | WASSP          | AP Registration to Appliance                        | Yes                 |
| Access Point                                | Appliance    | UDP                | Any      | 67            | DHCP Server    | If Appliance is DHCP Server for AP                  | Optional            |
| Access Point                                | Appliance    | UDP                | Any      | 68            | DHCP Server    | If Appliance is DHCP Server for AP                  | Optional            |
| Access Point                                | Appliance    | UDP                | Any      | 427           | SLP            | AP Registration to Appliance                        | Optional            |
| Appliance                                   | Access Point | TCP/UDP            | Any      | 69            | TFTP           | AP image transfer                                   | Yes                 |
| Access Point                                | Appliance    | TCP/UDP            | Any      | 69            | TFTP           | AP image transfer                                   | Yes                 |
| Appliance                                   | Access Point | TCP/UDP            | Any      | 22            | SCP            | AP traces                                           | Yes                 |
| Any                                         | Access Point | TCP                | Any      | 2002, 2003    | RCAPD          | AP Real Capture (if enabled)                        | Optional            |
| Any                                         | Access Point | TCP/UDP            | Any      | 22            | SSH            | Remote AP login (if enabled)                        | Optional            |
| 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            |

| Comp. Source                                                            | Comp. Dest  | Protocol (TCP/UDP) | Src Port | Dest Port | Service   | Remark                                                    | Open Firewall Req'd |
|-------------------------------------------------------------------------|-------------|--------------------|----------|-----------|-----------|-----------------------------------------------------------|---------------------|
| <b>Ports for Appliance Management</b>                                   |             |                    |          |           |           |                                                           |                     |
| Any                                                                     | Appliance   | TCP/UDP            | Any      | 22        | SSH       | Appliance CLI access                                      | Yes                 |
| Any                                                                     | Appliance   | TCP/UDP            | Any      | 5825      | HTTPS     | Appliance GUI access                                      | Yes                 |
| Any                                                                     | Appliance   | TCP/UDP            | Any      | 161       | SNMP      | Appliance SNMP access                                     | Yes                 |
| Any                                                                     | Appliance   | TCP/UDP            | Any      | 162       | SNMP Trap | Appliance SNMP access                                     | Yes                 |
| Any                                                                     | Appliance   | TCP                | Any      | 80        | HTTP      | Appliance SNMP access ICP Self Registration               | Yes                 |
| Any                                                                     | Appliance   | TCP                | Any      | 443       | HTTPS     | ICP Self Registration                                     | Yes                 |
| Any                                                                     | Appliance   | UDP                | 500      | 500       | IKE       | IKE phase 1                                               | Yes                 |
| Any                                                                     | Appliance   | TCP/UDP            | Any      | 69        | TFTP      | TFTP support                                              | Yes                 |
| Any                                                                     | Appliance   | UDP                | Any      | 4500      | IPSec     | IPSec NAT traversal                                       | Yes                 |
| Any                                                                     | Appliance   | UDP                | Any      | 13907     | Discovery | Used by Discovery                                         | Yes                 |
| Any                                                                     | Appliance   | UDP                | Any      | 13910     | WASSP     | Used by L3 WASSP                                          | Yes                 |
| <b>Ports for Inter Controller Mobility<sup>1</sup> and Availability</b> |             |                    |          |           |           |                                                           |                     |
| Appliance                                                               | Appliance   | UDP                | Any      | 13911     | WASSP     | Mobility and Availability Tunnel                          | Yes                 |
| Appliance                                                               | Appliance   | TCP                | Any      | 427       | SLP       | SLP Directory                                             | Yes                 |
| Appliance                                                               | Appliance   | TCP                | Any      | 20506     | Langley   | Remote Langley Secure                                     | Yes                 |
| Appliance                                                               | Appliance   | TCP                | Any      | 60606     | Mobility  | VN MGR                                                    | Yes                 |
| Appliance                                                               | Appliance   | TCP                | Any      | 123       | NTP       | Availability time sync                                    | Yes                 |
| 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                 |

<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 |
|------------------------------------|------------------|--------------------|----------|-----------|-----------------------------------------|---------------------------------------------------------|---------------------|
| <b>Core Back-End Communication</b> |                  |                    |          |           |                                         |                                                         |                     |
| Appliance                          | DNS Server       | UDP                | Any      | 53        | DNS                                     | If using DNS                                            | Optional            |
| Appliance                          | Syslog Server    | UDP                | Any      | 514       | Syslog                                  | If Appliance logs to external syslog server             | Optional            |
| Appliance                          | RADIUS Server    | UDP                | Any      | 1812      | RADIUS Authentication and Authorization | If using RADIUS AAA                                     | Optional            |
| Appliance                          | RADIUS Server    | UDP                | Any      | 1813      | RADIUS Accounting                       | If enabled RADIUS accounting                            | Optional            |
| Appliance                          | RADIUS server    | UDP                | Any      | 1814      | RADIUS Authentication and Authorization | If using RADIUS AAA                                     | Optional            |
| Appliance                          | RADIUS server    | UDP                | Any      | 1815      | RADIUS Accounting                       | If enabled RADIUS Accounting                            | Optional            |
| Dynamic Auth. Server (NAC)         | Appliance        | UDP                | Any      | 3799      | DAS                                     | Request from DAS client to disconnect a specific client | Optional            |
| Appliance                          | AeroScout Server | UDP                | 1144     | 12092     | Location Based Service Proxy            | Aeroscout Location-Based Service                        | Optional            |
| AeroScout Server                   | Appliance        | UDP                | 12092    | 1144      | Location Based Service Proxy            | Aeroscout Location-Based Service                        | Optional            |
| 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 are 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 |

| RFC No. | Title        | Groups Supported                        |
|---------|--------------|-----------------------------------------|
| 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

Refer to the latest Release Notes for ExtremeWireless™ 10.41.09 or later and/or ExtremeWireless WiNG 5.9.02 or later for the list of compatibility test devices.

## RADIUS SERVERS AND SUPPLICANTS

### RADIUS Servers Used During Testing

| Vendor         | Model OS       | Version                   |
|----------------|----------------|---------------------------|
| FreeRADIUS     | 1.1.6          | FreeRADIUS                |
| FreeRADIUS IAS | 1.0.1          | FreeRADIUS                |
|                | 5.2.3790.3959  | Microsoft Server 2003 IAS |
| SBR50          | 6.1.6          | SBR Enterprise edition    |
| NPS            | 6.0.6002.18005 | Microsoft Server 2008 NPS |

### 802.1x Supplicants Supported

| Vendor                   | Model OS                                                                                                                              | Version                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Juniper Networks® / Funk | Odyssey client                                                                                                                        | Version 5.10.14353.0                                            |
|                          |                                                                                                                                       | Version 5.00.12709.0                                            |
|                          |                                                                                                                                       | Version 4.60.49335.0                                            |
| Microsoft®               | Wireless Zero Configuration                                                                                                           | Version Windows XP-4K-891859-Beta1                              |
|                          | Wireless Network Connection Configuration                                                                                             | Version Microsoft Window Server 2003, Enterprise Edition R2 SP2 |
|                          | Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2 | Version WindowsXP-KB893357-v2-x86-ENU.exe                       |
| Intel®                   | Intel PRO Set/Wireless                                                                                                                | Version 13.0.0.x (with Windows® Intel® driver version 13.0.0.x) |
| Microsoft® Wireless Zero | Windows 7, 8, 8.1 Pro, 10 Pro<br>Windows Phone 8.1, Windows Mobile 10                                                                 | Provided with Windows®                                          |

### Appliance LAN Switch Verification

| Vendor  | Model OS        | Version  | Role              |
|---------|-----------------|----------|-------------------|
| Extreme | X-460-G2        | 12.5.4.5 | XIQC connection   |
| Extreme | X440G2-48p-10G4 | 21.1.1.4 | XIQC connectivity |
| Extreme | Summit 300-48   | 7.6e1.4  | XIQC connection   |

| Vendor  | Model OS         | Version                                       | Role            |
|---------|------------------|-----------------------------------------------|-----------------|
| Extreme | VSP-4850GTS-PWR  | (6.0.1.1_B003)<br>(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 |

| Attribute          | RFC Source                   |
|--------------------|------------------------------|
| NAS-IPv6-Address   | RFC 3162                     |
| NAS-Port           | RFC 2865, RFC 3580           |
| NAS-Port-Id        | RFC 2865, RFC 3580           |
| NAS-Port-Type      | RFC 2865, RFC 3580           |
| Password-Retry     | RFC 2869                     |
| Service-Type       | RFC 2865, RFC 3580           |
| Session-Timeout    | RFC 2865                     |
| State              | RFC 2865                     |
| Termination-Action | RFC 2865, RFC 3580           |
| Tunnel Attributes  | RFC 2867, RFC 2868, RFC 3580 |
| User-Name          | RFC 2865, RFC 3580           |
| Vendor-Specific    | RFC 2865                     |

### RADIUS Accounting Attributes

| Attribute             | RFC Source |
|-----------------------|------------|
| Acct-Authentic        | RFC 2866   |
| Acct-Delay-Time       | RFC 2866   |
| Acct-Input-Octets     | RFC 2866   |
| Acct-Input-Packets    | RFC 2866   |
| Acct-Interim-Interval | RFC 2869   |
| Acct-Output-Octets    | RFC 2866   |
| Acct-Output-Packets   | RFC 2866   |
| Acct-Session-Id       | RFC 2866   |
| Acct-Session-Time     | RFC 2866   |
| Acct-Status-Type      | RFC 2866   |
| Acct-Terminate-Cause  | RFC 2866   |

## GLOBAL SUPPORT

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:  
<https://extremeportal.force.com/>

By Email: [support@extremenetworks.com](mailto:support@extremenetworks.com)

By Web: <https://extremeportal.force.com/>

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](http://www.extremenetworks.com/company/legal/trademarks)

---

© Extreme Networks. 2025. All rights reserved.