ExtremeCloud™

Software Version 4.31.01.21

Feb 03, 2019

INTRODUCTION

This document provides specific information for ExtremeCloud V4.31.01.21

Extreme Networks recommends that you thoroughly review this document as it contains details on the new version of ExtremeCloud and its associated ExtremeWireless access point firmware. Please remember that to ensure simplicity in operations, your access points will be automatically upgraded by the ExtremeCloud.

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

SOFTWARE SPECIFICATION

Status	Version No.	Type	Release Date
Current Version	4.31.01.21	Maintenance Release	Feb 03, 2019
Previous Version	4.31.01.11	Feature Release	Sep 23, 2018
Previous Version	4.21.01.25	Feature Release	May 13, 2018
Previous Version	4.11.01.19	Feature Release	October 27, 2017
Previous Version	4.01.01.23	Feature Release	July 06, 2017
Previous Version	3.21.05.12	Maintenance Release	May 19, 2017
Previous Version	3.21.04.17	Maintenance Release	March 20, 2017
Previous Version	3.21.03.09	Maintenance Release	January 31, 2017
Previous Version	3.21.02.18	Maintenance Release	December 13, 2016
Previous Version	3.21.01.36	Feature Release	November 10, 2016
Previous Version	3.11.03.18	Maintenance Release	September 28, 2016
Previous Version	3.11.02.25	Maintenance Release	August 24, 2016
Previous Version	3.11.01.43	Feature Release	July 21, 2016
Previous Version	3.01.05.88	Maintenance Release	May 20, 2016
Previous Version	3.01.04.81	Maintenance Release	April 18, 2016
Previous Version	3.01.03.75	Maintenance Release	March 16, 2016
Previous Version	3.01.02.69	Feature Release	Febuary 19, 2016

SUPPORTED DEVICES AND REQUIREMENTS

You must have at least one supported device and meet the additional requirements to use ExtremeCloud.

SUPPORTED WIRELESS ACCESS POINTS

The following wireless access points are supported by this release. (**NOTE** – Access points will be automatically upgraded to the latest image in accordance with the preferences set at the site level.)

Product	Image
Wireless AP3935i-FCC (31012)	AP3935-10.41.10.0017.img
Wireless AP3935i-ROW (31013)	AP3935-10.41.10.0017.img
Wireless AP3935i-IL (31020)	AP3935-10.41.10.0017.img
Wireless AP3965i-FCC (31016)	AP3935-10.41.10.0017.img
Wireless AP3965i-ROW (31017)	AP3935-10.41.10.0017.img
Wireless AP3805i-FCC (30912)	AP3805-10.41.10.0017.img
Wireless AP3805i-ROW (30913)	AP3805-10.41.10.0017.img
Wireless AP3912i-FCC (31025)	AP3912-10.41.10.0017.img
Wireless AP3912i-ROW (31026)	AP3912-10.41.10.0017.img
Wireless AP3915i-FCC (31028)	AP3915-10.41.10.0017.img
Wireless AP3915i-ROW (31029)	AP3915-10.41.10.0017.img
Wireless AP3915e-FCC (31031)	AP3915-10.41.10.0017.img
Wireless AP3915e-ROW (31032)	AP3915-10.41.10.0017.img
Wireless AP3916i-FCC (31034)	AP3916-10.41.10.0017.img
Wireless AP3916i-ROW (31035)	AP3916-10.41.10.0017.img
Wireless AP3917i-FCC (31050)	AP3917-10.41.10.0017.img
Wireless AP3917i-ROW (31051)	AP3917-10.41.10.0017.img
Wireless AP3917e-FCC (31055)	AP3917-10.41.10.0017.img
Wireless AP3917e-ROW (31056)	AP3917-10.41.10.0017.img
Wireless AP-7532-67030-EU(H30788)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67030-IL(H30785)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67030-US(H30787)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67030-WR(H30781)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67040-EU(H30780)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67040-US(H30779)	AP7532-5.9.2.5-001R.img
Wireless AP-7532-67040-WR(H30786)	AP7532-5.9.2.5-001R.img
Wireless AP-7522-67030-EU(H30791)	AP7522-5.9.2.5-001R.img
Wireless AP-7522-67030-US(H30790)	AP7522-5.9.2.5-001R.img
Wireless AP-7522-67030-WR(H30784)	AP7522-5.9.2.5-001R.img
Wireless AP-7522-67040-EU(H30783)	AP7522-5.9.2.5-001R.img
Wireless AP-7522-67040-US(H30782)	AP7522-5.9.2.5-001R.img
Wireless AP-7522-67040-WR(H30789)	AP7522-5.9.2.5-001R.img
Wireless AP-7502-67030-EU(H30877)	AP7502-5.9.2.5-001R.img

Wireless AP-7502-67030-IL(H30875)	AP7502-5.9.2.5-001R.img
Wireless AP-7502-67030-US(H30876)	AP7502-5.9.2.5-001R.img
Wireless AP-7502-67030-WR(H30878)	AP7502-5.9.2.5-001R.img
Wireless AP-7562-670042-EU(H30777)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-670042-IL(H31127)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-670042-US(H30776)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-670042-WR(H30778)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-67040-EU(H30775)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-67040-US(H30773)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-67040-WR(H30774)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-6704M-EU(H30966)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-6704M-US(H30967)	AP7562-5.9.2.5-001R.img
Wireless AP-7562-6704M-WR(H30968)	AP7562-5.9.2.5-001R.img
Wireless AP-7612-680B30-US(37101)	AP7612-5.9.2.5-001R.img
Wireless AP-7612-680B30-WR(37102)	AP7612-5.9.2.5-001R.img
Wireless AP-7632-680B30-US(37111)	AP7632-5.9.2.5-001R.img
Wireless AP-7632-680B30-WR(37112)	AP7632-5.9.2.5-001R.img
Wireless AP-7632-680B40-US(37113)	AP7632-5.9.2.5-001R.img
Wireless AP-7632-680B40-WR(37114)	AP7632-5.9.2.5-001R.img
Wireless AP-7662-680B30-US(37121)	AP7662-5.9.2.5-001R.img
Wireless AP-7662-680B30-WR(37122)	AP7662-5.9.2.5-001R.img
Wireless AP-7662-680B40-US(37123)	AP7662-5.9.2.5-001R.img
Wireless AP-7662-680B40-WR(37124)	AP7662-5.9.2.5-001R.img
Wireless AP-8533-68SB30-US(H30974)	AP8533-5.9.2.5-001R.img
Wireless AP-8533-68SB30-WR(H31348)	AP8533-5.9.2.5-001R.img
Wireless AP-8533-68SB40-US(H30977)	AP8533-5.9.2.5-001R.img
Wireless AP-8533-68SB40-WR(H31349)	AP8533-5.9.2.5-001R.img
Wireless AP-7632-680B30-IL(37117)	AP7632-5.9.2.5-001R.img
Wireless AP-7662-680B30-IL(37130)	AP7662-5.9.2.5-001R.img

SUPPORTED SWITCHES

The following switches are supported by this release. (**NOTE** – Switches will be automatically upgraded to the latest image in accordance with the preferences set at the Site level.)

Product	Firmware	Cloud Connector
X440-G2-12t-10GE4 (16530)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
X440-G2-12p-10GE4 (16531)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
X440-G2-24t-10GE4 (16532)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
X440-G2-24p-10GE4 (16533)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
X440-G2-48t-10GE4 (16534)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
X440-G2-48p-10GE4 (16535)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod

X620-16x-Base (17401)	summitX-22.6.1.4.xos	summitX-cloud_connector-3.0.34.67.xmod
210-12t-GE2 (16566)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
210-12p-GE2 (16567)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
210-24t-GE2 (16568)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
210-24p-GE2 (16569)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
210-48t-GE4 (16570)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
210-48p-GE4 (16571)	210-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-12t-10GE2 (16560)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-12p-10GE2 (16561)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-24t-10GE2 (16562)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-24p-10GE2 (16563)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-48t-10GE4 (16564)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz
220-48p-10GE4 (16565)	220-series_V1.02.04.0007.stk	fp-connector-3.0.34.16.pyz

MOBILE PHONE REQUIREMENTS (APPLICABLE ONLY FOR EXTREMEWIRELESS ACCESS POINTS)

You can rename your access points or assign them to a site through the ExtremeCloud mobile application or the user interface. The following mobile phone software version are supported by the ExtremeCloud mobile application:

- iOS 8+
- Android 4.0.3 and later

NETWORK REQUIREMENTS

A cloud-enabled devices must have NTP, DHCP, DNS, and an Ethernet network port with Internet connectivity.

INSTALLATION AND CONFIGURATION RECOMMENDATIONS

Note:

Please see the full description of requirements and instructions in the *ExtremeCloud Information Center* at: http://documentation.extremenetworks.com/extremecloud/information_center/index.html

1. If you are using a switch, connect it before connecting your access points. Connect one of the Ethernet payload ports of the switch to a network that provides internet access. For an entitled switch to locate and connect to ExtremeCloud, only one port can be connected. Once the connection is established, additional ports can be connected. The switch gets configured automatically.
2. Connect your access points (APs) to a network with an Internet connection. APs can be powered by PoE or a power injector. See the *Installation Guide* for your APs. Each AP discovers ExtremeCloud and then gets configured automatically. If you can see the default SSIDs, the APs have successfully connected to the service.

3. When you log in to your ExtremeCloud account for the first time, you can update the network security key from the *Networks* tab or configure your own network services. Log in to your administrator account at https://ezcloudx.com to review settings and make changes.
4. When you register devices for the first time, default SSIDs and network services are assigned to help you verify that your devices are running successfully with ExtremeCloud. Although the default network services can be used, it is a best practice to configure them to your needs. You can edit or delete services for the default SSIDs, or create new services.

   For example, If you want to allow a completely open SSID, replace the default policy with a policy that allows traffic. You can use the predefined *Allow All* policy or create a more restrictive policy (the latter is recommended). If you want to use the WPA-PSK SSID in production, review the WPA-PSK network service. (We recommend changing the pre-shared key for better security.) Configure the pre-shared key on each device that will be allowed network access through the WPA-PSK SSID.

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS

Enhancements in 4.31.01.21

Hardware

This release introduces the support for the following ExtremeWireless WiNG access point models -

Model	Part Number
AP-7612-680B30-US	(37101)
AP-7612-680B30-WR	(37102)
AP-7632-680B30-US	(37111)
AP-7632-680B30-WR	(37112)
AP-7632-680B40-US	(37113)
AP-7632-680B40-WR	(37114)
AP-7662-680B30-US	(37121)
AP-7662-680B30-WR	(37122)
AP-7662-680B40-US	(37123)
AP-7662-680B40-WR	(37124)
AP-8533-68SB30-US	(H30974)
AP-8533-68SB30-WR	(H31348)
AP-8533-68SB40-US	(H30977)
AP-8533-68SB40-WR	(H31349)
AP-7632-680B30-IL	(37117)
AP-7662-680B30-IL	(37130)

Note: These hardwares need to run 5.9.2 or higher software to connect to ExtremeCloud.

Enhancements in 4.31.01.10

Hardware

Enhancements in 4.31.01.10

This release introduces the support for the following ExtremeWireless WiNG access point models -

Model	Part Number
AP-7612-680B30-US	(37101)
AP-7612-680B30-WR	(37102)
AP-7632-680B30-US	(37111)
AP-7632-680B30-WR	(37112)
AP-7632-680B40-US	(37113)
AP-7632-680B40-WR	(37114)
AP-7662-680B30-US	(37121)
AP-7662-680B30-WR	(37122)
AP-7662-680B40-US	(37123)
AP-7662-680B40-WR	(37124)
AP-8533-68SB30-US	(H30974)
AP-8533-68SB30-WR	(H31348)
AP-8533-68SB40-US	(H30977)
AP-8533-68SB40-WR	(H31349)

Note: These hardwares need to run 5.9.2 or higher software to connect to ExtremeCloud.

Software
Integration of Extreme Location – Allows ExtremeCloud customers to enable ExtremeLocation support. Once ExtremeLocation feature is enabled, APs are configured to report location-related data to ExtremeLocation. This is first step to a tighter integration of ExtremeLocation with ExtremeCloud. In this release, ExtremeLocation behaves as if it is completely separate from ExtremeCloud. **Note –** ExtremeWireless Wing APs should be running 5.9.2.2 or higher and ExtremeWireless APs should be running 10.41.07 or higher software version for this feature to work.
Support for IOT – BLE beacon configuration – Introduces the Support for following IOT modes in ExtremeCloud: **iBeacon Advertisement** – Acts like an Apple iBeacon device that broadcasts an identifier that devices can see and use to report their location. **Eddystone-url Beacon Advertisement** – Broadcasts a URL that can be configured by administrator rather than { UUID, Major, Minor } broadcast by iBeacons. **Thread Gateway** – Thread is another IOT protocol for lightweight communication over 802.15.4 Mesh Wireless. Devices are starting to appear with support for Thread. **Note –** ExtremeWireless Wing APs should be running 5.9.2.2 or higher software and ExtremeWireless APs should be running 10.41.07 or higher software for this feature to work.
Switch Port Manager - Introduces the approach for virtual stacking. The Port Manager feature provides capability to centrally configure ports across multiple switches. The user will be able to retrieve ports based on certain criteria, enter configuration changes and apply to all selected ports.
Port Type Notification - Introduces the capability to show a notification to customer if switch port has an AP connected but port is not configured for the function as “Access Point” in the cloud. The notification would flag it to the customer that the port needs to be reconfigured.
Troubleshooting Enhancement - Introduces support for following troubleshooting tools for ExtremeWrireless WiNG APs – • Remote console – Empowers GTAC with AP CLI access of WiNG AP device from the cloud. • Packet Capture – Provides option to capture the packets on wired/wireless interface. • Ping and Traceroute – Executes ping and traceroute commands on AP for a given address. • Wireless Debug – Provides option to enable and collect wireless packets exchanged between client and WiNG AP.
Deployment pre-requisit tool– Introduces the tool which can be run in the customer environment to assess if the environment meets the deployment requirement for ExtremeCloud devices.

Changes in 4.31.01.10	
wns0020948	[IOT info Message]: We should have a info message that Eddystone-url Beacon will work from build 10.41.05
wns0020754	Resolved an issue - Social Logins require HTTPS for the redirect URI’s
wns0020781	Resolved the request to - Add the MSP and MSP Partner name to the GTAC banner in addition to the customer name that appears now

Enhancements in 4.21.01.25

Hardware

This release introduces the support for the following ExtremeWireless access point models.

Model	Part Number
AP3915i-FCC	31028
AP3915i-ROW	31029
AP3915e-FCC	31031
AP3915e-ROW	31032
AP3916i-FCC	31034
AP3916i-ROW	31035
AP3917i-FCC	31050
AP3917i-ROW	31051
AP3917e-FCC	31055
AP3917e-ROW	31056

Software
PCI Compliance Reports – Introduces PCI compliance reports for vendors who want to process credit card transactions. The reports can be requested or scheduled from each site level or from the tenant level.
User-Customizable Reports – Introduces user-customizable reports, where the report templates are created by dragging and dropping widgets onto a region representing the report document. Once the template is saved, the administrator can schedule reports to be produced from the template periodically and 'on demand'. The report can be requested as a CSV zip file or in PDF format.
Basic WIDS-WIPS Support for WiNG access points – Introduces the ability to configure ExtremeWireless WiNG APs and report following events: • Report on the beacons they detect • Go off channel to discover other APs • Receive 'WIDS-WIPS events and display them in the Event view • Keep track of last time the device was seen • Neighboring/Threatening APs are displayed in a list in a new section • Drill down to a page describing a specific threat AP
TKIP and WEP Support - Adds full support for TKIP and WEP for the retail customers. WEP & TKIP are available as GUI configuration options for both ExtremeWireless and ExtremeWireless WiNG access points.
TAC & OPs GUI enhancement – Introduces the searchability for TAC & OPs based any of the following information: • ExtremeCloud administrator user IDs • Company names • Device serial numbers • Device MAC addresses • Contract numbers
AP Status GUI enhancement –The AP status page was only showing the AP's connection status to the ExtremeCloud). The page was enhanced to show the service status of each AP as follows: • **Green -** All radios that are configured to deliver service are delivering service (Tx power > 0, channel assigned) • **Yellow** - At least one radio that is configured to deliver service is not delivering service (Tx Power = 0 or no channel assigned, or …) • **Red** - None of the radios that are configured to deliver service are delivering service
Reliability and Performance Enhancements – As a part of the infrastructure enhancement, the following changes were made to improve overall reliability and performance: • Autoscaling for Cloud Connector servers • Data migration validation tool • RabbitMq fault tolerance and queue reduction • State manager re-factoring • REST API authentication enhancement

Changes in 4.21.01.25	
wns0017964	Resolved an issue where the AP status is shown as green even when radio 1 is off under certain conditions.
wns0019731	Resolved an GUI issue where Chrome browser sometimes does not display statistics correctly after moving between tabs.

Changes in 4.21.01.25	
wns0019765	Resolved an issue where the Clients tab list will not populate from the device view for AP3935.
wns0019885	Resolved an issue where Smart RF was not working properly on AP3805.
wns0019921	Resolved an GUI issue where the default role was sometimes missing from the network's grid.
wns0019978	Resolved an issue where one network on Radio 2.4GHz is missing if more than two networks are assigned to AP3805.
wns0020032	Resolved an issue where users may encounter issues on saving default VLAN multicast settings.
wns0020158	Resolved an issue where the Device tab may not report assets correctly.
wns0020165	Resolved an GUI issue where AP traces can be generated, but not displayed on the GUI.
wns0020258	Resolved an issue where the network schedule cannot be set to 12:00 AM.
wns0020264	Resolved an issue where RF Domain Manager turns off broadcasting the SSID when tunnel mode is enabled on ExtremeWireless WiNG APs.
wns0020293	Resolved an issue where PoC accounts were not properly deleted after the PoC expired.
wns0020294	Resolved an issue where the device number counts were not correctly reported.

Enhancements in 4.11.01.19
Hardware

Enhancements in 4.11.01.19

This is a convergence release which enables customers to have the ExtremeWireless WiNG access points AP-75XX series (AP-7502/AP-7522/AP-7532/AP-7562) managed from the Extreme Cloud.

The following ExtremeWireless WiNG AP models are supported:

Model	Part Number
AP-7532-67030-EU	H30788
AP-7532-67030-IL	H30785
AP-7532-67030-US	H30787
AP-7532-67030-WR	H30781
AP-7532-67040-EU	H30780
AP-7532-67040-US	H30779
AP-7532-67040-WR	H30786
AP-7522-67030-EU	H30791
AP-7522-67030-US	H30790
AP-7522-67030-WR	H30784
AP-7522-67040-EU	H30783
AP-7522-67040-US	H30782
AP-7522-67040-WR	H30789
AP-7502-67030-EU	H30877
AP-7502-67030-IL	H30875
AP-7502-67030-US	H30876
AP-7502-67030-WR	H30878
AP-7562-670042-EU	H30777
AP-7562-670042-IL	H31127
AP-7562-670042-US	H30776
AP-7562-670042-WR	H30778
AP-7562-67040-EU	H30775
AP-7562-67040-US	H30773
AP-7562-67040-WR	H30774
AP-7562-6704M-EU	H30966
AP-7562-6704M-US	H30967
AP-7562-6704M-WR	H30968

Software
ExtremeWireless WiNG configuration support with Extreme Cloud – With this release, ExtremeWireless WiNG APs (75XX series) are supported from ExtremeCloud. The configuration options** required to configure the ExtremeWireless WiNG APs have been made available in the Extreme Cloud. A Unified Data Model has been introduced to achieve this. A site can hold either all the ExtremeWireless WiNG APs or Extreme Wireless APs. A site configuration is applicable to all the devices which are part of the site. ** For existing Azara customers, this release converges the Azara provided configuration options with ExtremeCloud. Most of the configuration options available in Azara are made available in this release.
ExtremeWireless WiNG stats support with ExtremeCloud – ExtremeCloud stats processing has been augmented to include the ExtremeWireless WiNG supported stats**. A unified stats processing framework has been introduced in this release which now provides most of these stats for both the AP Families (ExtremeWireless & ExtremeWireless WiNG). Many new widgets in the “utilization”, “RF”, “Clients” and “Application Visibility” category have been added. A new category of “Captive Portal” widgets is introduced in this release. This release also supports two new durations – “Last 8 hours” and “Custom range”. ** For existing Azara customers, this release converges the Azara provided stats with ExtremeCloud. Most of the stats supported in Azara are made available in ExtremeCloud in this release.
Troubleshooting – This release introduces the centrized event logs collection framework. This feature enables remote troubleshooting with centralized event logs on a site or on a device. Additionally, flexible filter options are made available for fast issue isolation and resolution.
Introduces support for Smart RF - Optimal self-tuning for RF coverage in dynamic environments.
Flexible Dashboard Manager –Customizable dashboard manager has been enhanced to include the stats included in this release. The customizable dashboard manager allows administrators to select the information they want displayed on their own personal dashboard. Templates and widgets are available for a quick creation of custom dashboards at all levels of the hierarchy, from client, access points and switches, to sites, and across an account’s entire estate. Customer can drag and drop graphs and charts for monitoring, troubleshooting, application visibility, and the captive portal.
Streaming MU events to syslog - Supports sending of captive portal device access log stream to a syslog server.
Security Policy - Enhanced security policy configuration for MSP administrators that empowers “*Power-Admin’* to establish the following security policies: • Maximum failed login attempts before account lockout • Password expiration • Limited reuse of previously used passwords • Minimum password length • Restrict access to specific IP address ranges • Two-factor authentication

Enhancements in 4.01.01.23

Hardware

This release introduces support for the ExtremeSwitching™ 210 Series and ExtremeSwitching 220 Series. The ExtremeSwitching 200 family of switches are an economical, fixed-configuration family of Gigabit Ethernet Layer 2/3 switches designed for enterprises, branch offices and small to medium-sized businesses looking for key features in a flexible, yet easy-to-manage solution.

The following models are supported:

Part Number	Model Number
16566	210-12t-GE2
16567	210-12p-GE2
16568	210-24t-GE2
16569	210-24p-GE2
16570	210-48t-GE4
16571	210-48p-GE4
16560	220-12t-10GE2
16561	220-12p-10GE2
16562	220-24t-10GE2
16563	220-24p-10GE2
16564	220-48t-10GE4
16565	220-48p-10GE4

Supported Capabilities

- Basic LAG (i.e. no support for MLAG)
- PoE (for applicable models)
- LLDP
- Syslog
- Spanning Tree (loopguard and spanguard)
- Standard port throughput statistics & QoS queue utilization statistics

Software	
Introduces support for interactive “heat-maps” or radio frequency (RF) floor maps. Floor plans are easily customized to reflect the exact layout of your building by drawing walls and partitions, and configuring device placement for accurate heat map representation. Floor plans represent your building layouts and the relative location of access points and switches. Users can overlay the floor plan with the following information: heat maps: RSS, channel plan, link speed and RFQI, and augment with configurable statistical badges that reflect devices-specific configuration and status information.	
Introduces an enhanced captive portal which supports: • Social media logins (Facebook, Google and Twitter) • Self-registration via SMS and email • Integrated guest account management • Persistent device registration for a user-defined number of days • Flexible custom login page designer, including pre-defined templates.	
Introduces enhanced security policy configuration for administrators that empowers “*Power-Admin’* to establish the following security policies: • Maximum failed login attempts before account lockout • Password lifetime • Limited reuse of previously used passwords • Minimum password length • Restrict access to specific IP address ranges • Two-factor authentication	
Introduces a customizable dashboard that allows administrators to select the information they want displayed on their own personal dashboard. Templates and widgets are available for a quick creation of custom dashboards at all levels of the hierarchy, from client, access points and switches, to sites, and across an account’s entire estate.	
Introduces multiple look/feel and workflow enhancements throughout the GUI.	
Extended support for the following countries: • AP3805i-ROW (30913): Antigua-Barbuda, Uganda • AP3912i-ROW (31026): Chile, China, Indonesia, Kazakhstan, South Korea, Philippines, Saudi Arabia, Singapore, South Africa, Trinidad&Tobago, UAE	
Changes in 4.01.01.23	
wns0017967	Resolved an issue where the AP may lose the connection to the cloud due to frequently receiving new IP addresses from the DHCP server.

Enhancements in 3.21.05.12	
Reduces the APs and switches check-in time from 5 minutes to 1 minute to accelerate configuration change deployment.	
Changes in 3.21.05.12	
wns0018028	Resolved the issue where an administrator may get incorrectly blocked from provisioning 802.1x authentication and authorization in a network configuration.
wns0018045	Resolved the issue where an administrator may receive an error message when attempting to enable captive portal in a network configuration.

Enhancements in 3.21.04.17	
Hardware	
Introduces support for the AP3912i-FCC (31025) and AP3912i-ROW (31026) - Wall-plate, 802.11ac Wave 2, up to 1.17 Gbps capacity, dual radio, 2×2:2, integrated BTLE/802.15.4 radio.	
Software	
Introduces the ability to define the Minimum Basic Rate (MBR) for better control over radio performance.	
Introduces a new access point Auto-Channel Selection (ACS) algorithm designed to optimally select channels for all selected radio across a designated site.	
Improves rules visibility by displaying both rules custom names (when defined) and administrator-defined content on the same screen.	
Changes in 3.21.04.17	
wns0016100	Addressed issue where PDF Security Report may not be generated when requested.
wns0017373	Addressed scheduled upgrade limitation for switches
wns001559 **wns0017479** **wns0017498**	Addressed multiple issues with SNMP Retry Range, including display of mix/max values, confusing error message
wns0017405	Portals report page now displays the hostname when available.

Enhancements in 3.21.03.09	
Introduces support for a credential-based captive portal authentication using an external RADIUS server.	
Improves visibility by displaying client host-names in all client reports.	
Extended support for the following countries: • AP3935i-ROW (31013): Costa Rica, Dominican Republic, Trinidad & Tobago • AP3805i-ROW (30913): Argentina, Costa Rica, Korea, Philippines, South Africa, Taiwan, Trinidad & Tobago	
Changes in 3.21.03.09	
wns0017201	Resolved the issue where APs, under very specific configurations, may occasionally fail to re-connect to the ExtremeCloud after reboot.
Enhancements in 3.21.02.18	

Enhancements in 3.21.03.09	
Introduces support for configurable event notification using emails. Notification events include all configuration changes, device state changes and scheduled, starting and completing of device upgrade.	
Enhancements for MSPs in 3.21.02.18	
Introduces support for configurable event notification via SNMP traps. Notification events include all configuration changes, device state changes and scheduled, starting and completing of device upgrade.	
Changes in 3.21.02.18	
wns0016861	Resolved the issue where the active web UI session may occasionally time-out prematurely.
wns0017090	Resolved the issue where a switch may fail to re-connect to ExtremeCloud after a power outage or during a firmware upgrade.

Enhancements in 3.21.01.36	
Introduces granular multi-tenancy and rebrandable user interface for Managed Service Providers (MSP). Empowers qualifying organizations to deliver Managed Service practices around ExtremeCloud beyond the initial deployment and provisioning to include day-to-day operations such as move/add/change/delete.	
Introduces a splash screen, firewall friendly captive portal.	
Introduces the ability to enable IGMP snooping on supported Extreme switches.	
Introduces the ability to identify in the user interface the frequency associated with each radio.	
Changes in 3.21.01.36	
wns0016050	Resolved the issue where client statistics may not always get updated as expected.
XOS0064864	Resolved the issue where X440-G2-12p-10GE4 and X440-G2-12t-10GE4 fans may be reported as “fail” when operating at a speed of 0 RPM which lead to the switch inaccurately reporting in “Critical” state in ExtremeCloud.

Enhancements in 3.11.03.18
Hardware
Introduces support for the AP3935i-IL (31020) - Dual Radio 802.11ac/abgn, 4x4:4 MIMO indoor access point with eight internal antenna array for Israel (ROW regulatory domain).
Software
Introduces IPv6 support with IPv6 filter rules.
Introduces support for multi-factor authentication (MFA) for ExtremeCloud administrator logins. Two factor-authentication leverages the Google Authenticator application (time-based only).
Introduces the ability to record a customer's acceptance of the ExtremeCloud Terms & Conditions.
Extended support for the following countries: • AP3935i-ROW (31013): Brazil, Kazakhstan, Korea, Nicaragua • AP3965i-ROW (31017): Brazil, Ecuador, Kazakhstan, Korea, Nicaragua, Russia • AP3805i-ROW (30913): Brazil, Chile, Ecuador, Georgia, Kazakhstan, Mexico, Russia

Changes in 3.11.03.18	
wns0015853	Resolved the issue where MAC-based Authentication (MBA) may not always perform as expected.
wns0015955	Resolved the issue where certain versions of Firefox may show a blank configuration menu on left panel.
wns0015986	Resolved the issue where the CoS profile may not always be successfully deployed to the wireless access points.
wns0016050	Resolved the issue where the client statistics may not consistently be updated.
wns0016095	Resolved the issue where the AP may not always apply the expected role to a client.
wns0016141	Resolved the issue where the deletion of a custom application fingerprint may not always perform as expected.

Enhancements in 3.11.02.25
Introduces the ability to validate all administrators' email addresses to confirm that all accounts created are associated with a valid email address.
Introduces the ability for administrators to select a time and day within two weeks of a new software release to upgrade switches and/or wireless access points, thus minimizing service impact during the upgrade. Note that the upgrade to the ExtremeCloud software is automatic and cannot be scheduled as it is not service impacting.

Changes in 3.11.02.25	
wns0015797	Resolved the issue where the wizard page was presented unnecessarily after upgrade.
wns0015799	Resolved the issue where some information may have been missing from the Role tab.
wns0015868	Resolved the issue where multicast bridging and forwarding may not have performed as expected.
wns0015873	Resolved the issue where the Default VLAN from the Policy > VLAN menu may not have been editable.

Enhancements in 3.11.01.43

Hardware

Introduces support for select ExtremeSwitching™ stackable X440-G2 and X620 switches.

ExtremeSwitching stackable management is primarily targeted at supporting ExtremeWireless AP deployments.

The following ExtremeSwitching stackable are supported:

Part Number	Model Number
16530	X440-G2-12t-10GE4
16531	X440-G2-12p-10GE4
16532	X440-G2-24t-10GE4
16533	X440-G2-24p-10GE4
16534	X440-G2-48t-10GE4
16535	X440-G2-48p-10GE4
17401	X620-16x-Base

Supported Capabilities

- Basic LAG (i.e. no support for MLAG)
- PoE (for applicable models)
- LLDP
- SNMP
- Syslog
- Spanning Tree (loopguard and spanguard)
- Standard port throughput statistics & QoS queue utilization statistics

Software

Introduces application visibility and control.

- Reporting on top application groups is provided globally, and on a per-devices group and client basis.
- Applications-specific rules (including custom-application rules) can be defined to explicitly allow, deny, prioritize or de-prioritize (via CoS re-mapping), contain to a VLAN; and/or rate limit applications with over 3,000 fingerprints covering 2,000+ applications.

Introduces the ability to identify the operating system of a device. The reporting on the operating system of a device is provided globally, on a per devices group and network basis, as well as in the individual devices' report.

Introduces support for redirection to a Firewall Friendly External Captive Portal (FFECP) from the wireless Access Points (AP38xx/39xx). Administrators can define an explicit REDIRECT action within a role to determine when HTTP/HTTPS traffic should be re-directed.

Provides an audit log on all configuration changes to ensure traceability and auditability.

Allows each administrator to configure their own session inactivity timer.

Increases the number of APs that can be associated to a designated site from 50 to 100. Includes support for up to 2,000 active clients per site.

Enhancements in 3.11.01.43
Extended support for the following countries: • AP3935i-ROW (31013): China, Egypt, Hong Kong, India, Indonesia, Jordan, Kuwait, Malaysia, Mexico, Pakistan, Peru, Philippines, Qatar, Saudi Arabia, Singapore, Thailand, United Arab Emirates • AP3965i-ROW (31017): China, Egypt, Hong Kong, India, Indonesia, Jordan, Malaysia, Mexico, Pakistan, Philippines, Saudi Arabia, Singapore, Taiwan, Thailand, United Arab Emirates • AP3805i-FCC (30912): Colombia,Puerto Rico, United States • AP3805i-ROW (30913): Argentina , Australia, Austria, Belgium, Bosnia & Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Malaysia, Malta, Montenegro, Netherlands, New Zealand, Norway, Pakistan, Poland, Portugal, Romania, Saudi Arabia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, Uruguay

Changes in 3.11.01.43	
wns0015590	Resolved the issue that an error could occur when trying to activate a new SSID.

Enhancements in 3.01.05.88
Hardware
Introduced support for the AP3805i-FCC and AP3805i-ROW, a feature rich 802.11ac and 802.11abgn indoor access point that delivers enterprise-grade performance and security. Designed to blend into the office, classroom or hotel environment, the AP3805i-FCC/ROW is ideal for providing secure Wi-Fi connectivity for medium-density environments. It has following country support: • AP3805i-FCC (30912): Puerto Rico, United States • AP3805i-ROW (30913): Australia, Austria, Belgium, Bosnia, Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Malaysia, Malta, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, Uruguay
Software
Extended support for the following countries: • AP3935i-ROW (31013): Hong Kong, Saudi Arabia, Singapore, Thailand, Peru, China, Qatar, Kuwait, Egypt, Jordan, Philippines, Indonesia • AP3965i-ROW (31017): Thailand, Taiwan, Singapore, China, Egypt, Jordan, Philippines, Saudi Arabia, Indonesia

Changes in 3.01.05.88	
wns0014582	Resolved the issue that ExtremeCloud user interface is unreachable using an IE Browser.
wns0014544	Resolved the issue that IOS Safari Browser is not able to log in into the ExtremeCloud user interface.

Changes in 3.01.04.81	
wns0014510	Ensured the browser will always display the page content in English.
wns0014491	Resolved the issue with Deny role is not working to block specific subnet traffic.
wns0014300	Resolved the NTP issue with the access point so you do not need to RESET the Access Points to the factory default after you complete the staging process anymore.

Changes in 3.01.03.75	
wns0014303	Resolved the issue where Site name with more than 16 characters causes the configuration not to load.

KNOWN RESTRICTIONS AND LIMITATIONS

INFO	AP 7662, 7632, 7662 and 8553 should run firmware version 5.9.2 or higher to connect to extremecloud.
wns0019254 – Info	AP(wns17012) -Facebook deny rule of wlan overridden by wlan (CP jumbo templ's whitelist). Identify AP Firmware issue. Set the WLAN with Facebook Deny rules in ExtremeWireless APs. The WLAN is allowing Facebook traffic when the AP has another Guest WLAN with the jumbo captive portal template. Jumbo captive portal sets the Facebook app in the DNS whitelist.

SYSTEM LIMITS

The following table shows the maximum system limits:

Item	Maximum Value
Accounts per customer	1
Sites per account	100/128
Number of APs per Account	10,000
APs per site	100
Users per site	2,000
Roles per AP	64
Rules per role	64
Active Networks per account	8
Administrator accounts per customer	20
Rate limiters per account	16 (8 inbound and 8 outbound)
Rate limiters per Site	16 (8 inbound and 8 outbound)
MAC addresses in customer blacklist	768

LED PATTERN FOR EXTREMECLOUD SUPPORTED ACCESS POINTS

LED Patterns for ExtremeWireless APs Connecting with ExtremeCloud

Radio B/G LED (left)	Radio A LED (right)	Status LED	AP Detailed State
Off	Off	Blink green	Initialization: Power-on Self test (POST)
	Blink green	Blink green	Initialization: Random delay
		Blink red	Initialization: No Ethernet
	Solid green	Blink green	Initialization: Vulnerable period
		Blink red	Reset to factory defaults

Blink green	Off	Blink green / orange	Network discovery: 802.1x authentication
		Blink red	Failed 802.1x authentication
	Blink green	Blink green / orange	Network discovery: DHCP
		Blink red	Default IP address
	Solid green	Blink green / orange	Network discovery: Discovery / connect
		Blink red	Discovery failed
Green - Radio On Off - Radio Off	Green - Radio On Off - Radio Off	Solid green	Connected

LED Patterns for ExtremeWireless WiNG APs Connecting with ExtremeCloud

Task	5 GHz Activity LED (Amber)	2.4 GHz Activity LED (Green)
Unconfigured Radio	On	On
Normal Operation	O If this radio band is enabled: Blinks at 5 second intervals O If this radio band is disabled: Off O If there is activity on this band: Blinks at 1 time per second	O If this radio band is enabled: Blinks at 5 second intervals O If this radio band is disabled: Off O If there is activity on this band: Blinks at 1 time per second
Firmware Update	On	Off
Locate AP Mode	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions.	LEDs blink in an alternating green, red and amber pattern using an irregular blink rate. This LED state in no way resembles normal operating conditions

SUPPORTED WEB BROWSERS

For the ExtremeCloud management GUI, the following web browsers were tested for interoperability:

- Google Chrome 68.0.3440.106
- MS IE Edge 42.17134.1.0
- Firefox 62.0

FIREWALL REQUIREMENTS AND PORT LIST

Modern firewalls can block access to specific Internet application servers. ExtremeCloud-enabled devices need to be able to access several different application servers in order to provide their full functionality. Please ensure that your firewall is allowing ExtremeCloud devices behind it to access to the following domains and ports:

ExtremeWireless TCP/UDP Port Assignment Reference							
Component		Ports for AP/Cloud Communication					
Source	Destination / Domain Name	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall
Admin Console	ezcloudx.com	TCP	Any	443	HTTPS	Access the ExtremeCloud management application.	Required
Admin Console / API integrated systems	api.ezcloudx.com	TCP	Any	443	HTTPS	Application access to the backend services managing ExtremeCloud-enabled devices.	Required
Access Point & Switches	devices.extremenetworks.com	TCP	Any	443	HTTPS	Management Tunnel between AP and ExtremeCloud (configuration, image, statistics, upgrade, traces).	Required
Access Points & Switches	NTP Server	UDP	Any	123	NTP	Clock synchronization.	Required
Access Points	radius.ezcloudx.com	UDP	Any	1812	RADIUS	The integrated captive portal solution requires a cloud RADIUS lookup for each wireless client authentication via the captive portal.	Required if using the built-in captive portal.
Access Points	cp.ezcloudx.com	TCP	Any	443, 80	HTTP HTTPS	The integrated captive portal solution is hosted at cp.ezcloudx.com. Access to the portal is required to ensure wireless clients can authenticate via the captive portal.	Required if using the built-in captive portal.
Access Points & Switches	aptransient-eu-central-1.s3.eu-central-1.amazonaws.com	TCP	Any	443	HTTPS	Used by ExtremeCloud-enabled devices that, on command, may upload tech support files to storage managed by this application.	Required
Access Points & Switches	extremeimages.s3.amazonaws.com	TCP	Any	443	HTTPS	Required to successfully upgrade ExtremeCloud managed devices.	Required
Any	Access Point	TCP	Any	2002, 2003	RCAPD	Collect WireShark traces using AP Real Capture, if enabled.	Optional
Any	Access Point	TCP/UDP	Any	22	SSH	SSH into the AP, if enabled.	Optional
ExtremeWireless WiNG APs	mgmt.devices.extremenetworks.com	TCP	Any	443	HTTPS	Management tunnel between WiNG AP and ExtremeCloud.	Required - Allows outbound Connections from devices to ExtremeCloud over the various ports listed.

RADIUS SERVERS AND SUPPLICANTS

RADIUS SERVERS USED DURING TESTING

Vendor	Model OS	Version
FreeRADIUS	Red Hat Linux release 9 (Shrike)	1.1.6
FreeRADIUS	Red Hat Linux release 8.0 (Psyche)	1.0.1
IAS	Microsoft Server 2003 IAS	5.2.3790.3959
SBR50	SBR Enterprise Edition	6.1.6
NPS	Microsoft Server 2008 NPS	6.0.6002.18005

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)
Wireless Zero	Windows 7, 8, 8.1 Pro, 10 Pro Windows Phone 8.1	Provided with Windows

LAN SWITCHES

Vendor	Model OS	Version	Tested with
Cisco	Catalyst 3550	12.1(19)EA1c	AP 802.1x
Enterasys	G3	01.00.02.0001	For PoE
	G3	06.11.01.0040	
	C20N1	Version 12.1(19)EA1c	No PoE
	B3G124-48P	06.61.03.0004	For AP 802.1x, PoE
	B3	01.02.01.0004	10480068225P
	C5	06.42.06.0008	11511205225K
	B3G124-48P	06.61.03.0004	For AP 802.1x, POE

Vendor	Model OS	Version	Tested with
	Extreme X460-24P	12.5.4.5	For AP 802.1x, POE
	B3	06.61.08.0013	Lab switch - sn 10480062225P
	B3	06.61.08.0013	Veriwave switch - sn 10480075225P
Extreme	Summit 300-24	7.6e.4.4	
	Summit 300-24	System Serial Number: 800138-00-03 0443G-01236 CP: 04	For AP 802.1x, POE
	Summit 300-48	7.6e1.4	AP 802.1x, PoE
	Summit 300-48	7.6e1.4	
	Summit 300	Software Version 7.4e.2.6	Lab switch
H3C	H3C S5600 26C	Bootrom Version is 405	For PoE
HP	ProCurve 4104GL	#G.07.22	Lab switch

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	Cloud Local Server Debian GNU/Linux 8 (jessie)	OpenSSL 1.0.1k 8 Jan. 2015

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

Attribute	RFC Source
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

REST API INTERFACE

Attached is the list of Rest APIs which are getting deprecated in this release. The supported substitute/alternative APIs is mentioned against each deprecated APIs:

Deprecated API		Alternate API	
API	Path & Query parameters	API	Path & Query parameters
DpiSignatureManager		**DpiSignatureManager**	
GET /v1/dpisignatures/custom		GET /v3/dpisignatures/custom	
PUT /v1/dpisignatures		PUT /v3/dpisignatures	
RadioManager		**RadioManager**	
GET /v1/radios/modes	Query Param: country, hardwareType, radioIndex	GET /v3/radios/modes	Query Paramr: country, hardwareType, radioName
GET /v1/radio1/smartrfchannels	Query Param: country, acsChannelSelection1, channelWidth, siteType	GET /v3/radios/smartrfchannels	Query Param: country, channelPlan, channelWidth, radioBand, siteType
GET /v1/radio2/smartrfchannels	Query Param: country, acsChannelSelection2, channelWidth, siteType		
RoleManager		**RoleManager**	
GET /v1/roles		GET /v3/roles	
GET /v1/roles/{roleId}	Path Param : roleId	GET /v3/roles/{roleId}	Path Param : roleId
POST /v1/roles		POST /v3/roles	
PUT /v1/roles/{roleId}	Path Param : roleId	PUT /v3/roles/{roleId}	Path Param : roleId
DELETE /v1/roles/{roleId}	Path Param : roleId	DELETE /v3/roles/{roleId}	Path Param : roleId
GET /v1/roles/default		GET /v3/roles/default	
GET /v1/roles/nametoidmap		GET /v3/roles/nametoidmap	
PUT /v1/roles/appFilters		PUT /v3/roles/appFilters	

TopologyManager		**TopologyManager**	
GET /v1/topologies		GET /v3/topologies	
GET /v1/topologies/{topologyId}	Path Param : topologyId	GET /v3/topologies/{topologyId}	Path Param : topologyId
POST /v1/topologies		POST /v3/topologies	
DELETE /v1/topologies/{topologyId}	Path Param : topologyId	DELETE /v3/topologies/{topologyId}	Path Param : topologyId
PUT /v1/topologies/{topologyId}	Path Param : topologyId	PUT /v3/topologies/{topologyId}	Path Param : topologyId
GET /v1/topologies/default		GET /v3/topologies/default	
GET /v1/topologies/nametoidmap		GET /v3/topologies/nametoidmap	
SiteManager		**SiteManager**	
GET /v2/sites		GET /v3/sites	Query Param: filter, orderBy, page, reset, size
GET /v2/sites/{siteId}	Path Param : siteId	GET /v3/sites/{siteId}	Path Param : siteId
POST /v2/sites		POST /v3/sites	
DELETE /v2/sites/{siteId}	Path Param : siteId	DELETE /v3/sites/{siteId}	Path Param : siteId
PUT /v2/sites/{siteId}	Path Param : siteId	PUT /v3/sites/{siteId}	Path Param : siteId
POST /v2/sites/clone/{siteId}	Path Param : siteId Query Param: newSiteName	POST /v3/sites/clone/{siteId}	Path Param : siteId Query Param: newSiteName
GET /v2/sites/default		GET /v3/sites/default	
GET /v2/sites/nametoidmap		GET /v3/sites/nametoidmap	
GET /v2/snmp/default		GET /v3/snmp/default	
GET /v2/snmp		GET /v3/snmp	

Report Manager REST APIs

Query Params	**Accepted Values**	**Comments**
widgetList	<widgetId> or <widgetId|band> (one or more comma separated widgetIds or widgetBandPairs)	encoded with UTF - 8,band is not supported in case of Switch/Port/Role reports
duration	8H|1|7|31	
starttime	fromTimeInMillis (to be provided in absence of duration along with endTime)	
endtime	toTimeInMillis (to be provided in absence of duration along with startTime)	
band	all|2_4|5	query param used for single widget api

Deprecated API (used to fetch individual report)	Deprecated API Path Params	Deprecated API QueryParams	Mapped alternative API	Alternative API PathParams	Alternative API PathParams	Comments
v1/report/topapsbythroughput/sites		duration	v1/report/sites	-	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds or widgetBand pairs, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/topapsbyusercount/sites			v1/report/sites/widget/{widgetId}	widgetId	band, duration,starttime,endtime	widgetId accepts widgetEnum

v1/report/topswitchesbythroughput/sites						
v1/report/topmanufacturersbydevicecount/sites						
v1/report/topusersbythroughput/sites						
v1/report/toposbyclientcount/sites						
v1/report/topservicesbythroughput/sites						
v1/report/topsitesbyusercount/sites						
v1/report/topsitesbythroughput/sites						
v1/report/uniqueclientcount/sites						
v1/report/topappgroupsbythroughput/sites						
v1/report/topappgroupsbyclientcount/sites						
v1/report/topapsbyusercount/sites/{siteId}	Site Id	duration	v1/report/sites/{siteId}	siteId	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds or widgetBand pairs, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/topapsbythroughput/sites/{siteId}			v1/report/sites/{siteId}/widget/{widgetId}	siteId,widgetId	band, duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/topswitchesbythroughput/sites/{siteId}						
v1/report/topswitchesbythroughput/sites/{siteId}						
v1/report/topmanufacturersbydevicecount/sites/{siteId}						
v1/report/topusersbythroughput/sites/{siteId}						
v1/report/toposbyclientcount/sites/{siteId}						
v1/report/topservicesbythroughput/sites/{siteId}						
v1/report/devicedistribution/sites/{siteId}						
v1/report/uniqueclientcount/sites/{siteId}						
v1/report/usagestats/sites/{siteId}						
v1/report/topappgroupsbythroughput/sites/{siteId}						
v1/report/topappgroupsbyclientcount/sites/{siteId}						

v1/report/toposbyclientcount/aps/{apserial}	apserial	duration	v1/report/aps/{apSerialNumber}	apSerialNumber	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds or widgetBand pairs, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/totaloctetstats/aps/{apserial}			v1/report/aps/{apSerialNumber}/widget/{widgetId}	apSerialNumber,widgetId	band, duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/uniqueclientcount/aps/{apserial}						
v1/report/noiseperradio/aps/{apserial}						
v1/report/channelutilization/aps/{apserial}						
v1/report/currentuserstoband/aps/{apserial}						
v1/report/wiredportsusagestats/aps/{apserial}						
v1/report/wiredportsuniqueclientcount/aps/{apserial}						
v1/report/wiredportsutilizationerrors/aps/{apserial}						
v1/report/wiredportsdiscardedpackets/aps/{apserial}						
v1/report/topappgroupsbythroughput/aps/{apserial}						
v1/report/topappgroupsbyclientcount/aps/{apserial}						
v1/report/devicemanufacturersbyclientcount/services/{serviceId}	serviceId	duration	v1/report/services/{serviceId}	serviceId	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds or widgetBand pairs, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/uniqueusers/services/{serviceId}			v1/report/services/{serviceId}/widget/{widgetId}	serviceId,widgetId	band, duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/topapsbythroughput/services/{serviceId}						
v1/report/topusersbythroughput/services/{serviceId}						
v1/report/topapsbyusercount/services/{serviceId}						
v1/report/toposbyclientcount/services/{serviceId}						

v1/report/usagestats/station/{stationId}	stationId	duration	v1/report/stations/{stationId}	stationId	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds or widgetBand pairs, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/topappgroupsbythroughput/stations/{stationId}			v1/report/stations/{stationId}/widget/{widgetId}	stationId,widgetId	band, duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/topappgroupsbythroughput/roles/{roleId}	roleId	duration	v1/report/roles/{roleId}	roleId	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/topappgroupsbyclientcount/roles/{roleId}			v1/report/roles/{roleId}/widget/{widgetId}	roleId,widgetId	duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/transmittedbytes/switches/{switchSerialNumber}	switchSerialNumber	duration	v1/report/switches/{switchSerialNumber}	switchSerialNumber	widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/receivedbytes/switches/{switchSerialNumber}			v1/report/switches/{switchSerialNumber}/widget/{widgetId}	switchSerialNumber,widgetId	duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/transmittedpackets/switches/{switchSerialNumber}						
v1/report/receivedpackets/switches/{switchSerialNumber}						
v1/report/transmittederrors/switches/{switchSerialNumber}						
v1/report/receivederrors/switches/{switchSerialNumber}						
v1/report/topbusiestports/switches/{switchSerialNumber}						
v1/report/transmittedbytes/ports/{portId}?switchserialno={switchSerialNumber}	PortId	switchSerialNumber,duration	v1/report/ports/{portId}	portId	switchserialno(mandatory),widgetList, duration ,starttime,endtime	widgetList accepts one or more widgetIds, duration for predefined timeRange, starttime and endtime for custom timerange.
v1/report/receivedbytes/ports/{portId}?switchserialno={switchSerialNumber}			v1/report/ports/{portId}/widget/{widgetId}	portId,widgetId	switchserialno(mandatory), duration,starttime,endtime	widgetId accepts widgetEnum
v1/report/transmittedpackets/ports/{portId}?switchserialno={switchSerialNumber}						
v1/report/receivedpackets/ports/{portId}?switchserialno={switchSerialNumber}						

v1/report/transmittedutilization/ports/{portId}?switchserialno={switchSerialNumber}						
v1/report/receivedutilization/ports/{portId}?switchserialno={switchSerialNumber}						
v1/report/transmittederrors/ports/{portId}?switchserialno={switchSerialNumber}						
v1/report/receivederrors/ports/{portId}?switchserialno={switchSerialNumber}						

GLOBAL SUPPORT

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

For the toll-free support number in your country: www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Vía Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.