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

Customer Release Notes

ExtremeWireless™ Array Operating System

Version 8.5.6-7674
February 2020

INTRODUCTION:

This document provides specific information for version 8.5.6-7674 of software for the ExtremeWireless™ Array Operating System (AOS). This Release Note covers new features and enhancements, resolved issues, known issues and limitations, and hardware and software requirements and is suitable for deployment in production networks.

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

NEW FEATURES AND ENHANCEMENTS:

- Bug fixes

RESOLVED ISSUES:

34052	Wave-1 APs may incorrectly display Tx rates at 6 Mbps where the actual Tx rate is higher.
AOS-165	Radius Accounting: Multi-Session-Id is changing upon Roam to neighbor when Session-Timeout is set.
AOS-199, AOS-331, AOS-423, 34015	Could not change IP of clients once DHCP address was provided. VLAN is now able to change dynamically via an authentication server (Radius).
AOS-301	show running config or diag log does not show LLDP state (enabled/disabled)
AOS-354, 34049	The CLI commands under global-ac-setting for multi-user-mimo and tx-beam-forming were hidden. Now they are displayed.
AOS-355, 33978	On an EasyPass Onboarding Portal, when a user attempts to connect and register more devices than the maximum number allowed, the AP may not display the Max Device Page (the page that notifies the user and allows de-registration of current devices to make room for other devices to be registered).
AOS-357, 34038	With air-cleaner filters enabled on the AP, L2GRE tunnels have trouble working and DHCP packets will not flow to stations.
AOS-361, 33965	Auto-channel at power-on can leave the radio LEDs in a state inconsistent with the configuration.
AOS-365, 34056	TFTP Download Progress Bar Disappeared.
AOS-375, 34058	SSID with WPR Splash defined is displaying the setting, “Web Page HTTPS enable”. This should not be displayed for WPR Splash.

AOS-380, 34069	AOS 8.5.4, 8.5.5 General Process Clean-up (GPC) reboots, which may have WPA authentication engine process restart messages.
AOS-382	On APs running AOS 8.5.4, after a couple of days 1-Click portal clients do not get splash page and have no Internet access.
AOS-386	Enable channels 36-48 for China, for 9144.
AOS-394	When using WPA2/PSK with Internal Splash Page WPR (Web Page Redirect), after a station authenticates, the user sees the Internal Splash page and presses the "proceed" button. After this, if the station's Wi-Fi is turned off and then on again, the station reconnects to the SSID but doesn't get an IP address.
AOS-398	RADIUS MAC not working on APs running AOS 8.5.4/8.5.5. High amount of traffic observed being sent to the RADIUS server.
AOS-400, 34074	(Radius-MAC): If a station authenticates on a 1-Click SSID and then tries to switch to a Radius-MAC SSID, the AP incorrectly uses 0.0.0.0 as the Radius Server IP address. Thus, the station is not authenticated.
AOS-404	Clients cannot reconnect to network after they have left the area. User device would report "Incorrect Password."
AOS-415	(Web Page Redirect): the https setting in "wpr web-page https enable" is now disabled by default. Having this enabled by default (especially for WPR Internal Splash and Login pages) caused the end-user device to show an SSL Error or a blank page.

KNOWN ISSUES:

33141, 33399	Clients associated to 802.11ac Wave1 APs with arp-filter proxy configured are unable to IPv6 ping each other
33398	Wave1 APs with arp-filter set to proxy is rebroadcasting ARP request packets from wireless clients.
33595	(9132) When the RF-Monitor is in Timeshare mode and Dot11g-only is on, beacons are sent at data rate of 1 Mbps rather than 6 Mbps.
33663	On 802.11 Wave 1 APs, stations may get disassociated due to a radio reset. The syslog shows "Low activity condition detected on IAP iap1. Resetting IAP."
33821	EAP stations may stop passing traffic until client re-associates
33827	EAP clients on wave2 APs may stop passing traffic until client re-associates
33828	When there are many stations associated to radio1 on an AP, they are experiencing poor performance, high ping loss and delay and video freezes.
33833	AP may send unnecessary CTS packets when 802.11g devices are present in the environment
33851	Some stations are unable to pass traffic when MU-MIMO is enabled.
33878	Beacon Intervals and RSSI levels on 802.11ac are not consistent in 2.4GHz.
33893	On 802.11ac Wave 2 APs, changing the 802.11k (Radio Resource Management) in global settings doesn't take effect until after a reboot.
33896	802.11r capable iPads are not able to associate to an SSID when 802.11r (fast roaming) and .11w (Protected Management Frames) are enabled.
33924	Stations connected to Wave 2 APs occasionally can't pass traffic. On the station, turning Wi-Fi off and on will fix the problem.
33926	WDS Link recovery is slow on Wave 2 APs after replacing a WDS client or host AP - it takes a long time to re-establish a WDS link. After configuration of the new unit is complete, reboot the APs on both sides of the link to prevent this delay.

AOS-208, AOS-223	Hotspot Shield, Psiphon and Ultrasurf cannot be detected reliably.
AOS-316, 33998	Some clients on wave-1 APs with a bonded channel of 40 MHz may not rate back up past 81.0 Mbps. A de-authentication of the client clears this condition.
AOS-337, 33817	On 802.11 Wave 2 APs, stations may get disassociated due to a radio reset. The syslog shows "Low activity condition detected on IAP iap2. Resetting IAP."
AOS-360, 34053, 34059	Management Engine Restarts occur.
AOS-389	Multiple 9132s (running AOS 8.4.9) are experiencing network connectivity loss. Rebooting fixes this, but it may recur.
AOS-412	9144 shows WDS Link as 11an when both sides are 11anac capable.
AOS-416	GPC on AP running 8.5.5. An identifier string was added to the end of the GPC: "_kmalloc_track_caller.
AOS-419	Watchdog trigger errors on AP after upgrade to AOS 8.5.5, due to processing of large numbers of unassociated stations.
AOS-437	When WDS is configured, a SYSLOG message is generated that should be ignored - the problem it refers to has been fixed in AOS 8.5.6. After an AP reboot, ignore this message: “CTaskMacRcv(3710) taking IapRdLock(7) lock @mib.cpp:getEntry:7369 out of order holding: stationMutex(18)”.

LIMITATIONS AND CONDITIONS:

- **30392** - Bonjour – AppleTV is not able to service a client on SSID with VLAN when AppleTV is on the Bridged wired network. It is not recommended that you place AppleTV on the Bridged Management LAN segment. This will cause a lot of multicast traffic to be processed by the Array on the Management VLAN and can affect performance of the Array. Isolation of Multicast Traffic is recommended to be handled in VLANs that are not part of the Array Management VLAN.
- **34006** – iPad Air (first generation) cannot associate to channels 140 or 144 on 802.11ac Wave 2 platforms. Later generations do not have this problem.
- **AOS-295, 33974** – 802.11u and Hotspot 2.0 are not available on 802.11ac Wave 2 APs, and they cannot be enabled.
- **WDS** – When doing a software upgrade, WDS client (remote) APs must be upgraded before WDS host (network-connected) APs.
- **WDS** - Using WDS between different families of APs (e.g., between Wave 1 and Wave 2 APs) is not recommended. If you must create a link between different radio types, set the most advanced AP type as the host.

UPGRADE NOTES:

None.

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 Via 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.

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